BLOCKCHAIN-BASED DELIVERY ASSURANCE

by

Mehmet Demir

M.B.A. York University, Toronto, ON, Canada, 2007

M.Eng. Bogazici University, Istanbul, Turkey, 2001

B.Eng. Bogazici University, Istanbul, Turkey, 1996

A dissertation

presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

in the program of

Computer Science

Toronto, Ontario, Canada, 2020

AUTHOR'S DECLARATION

FOR ELECTRONIC SUBMISSION OF A DISSERTATION

I hereby declare that I am the sole author of this dissertation. This is a true copy of the dissertation, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this dissertation to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this dissertation by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my dissertation may be made electronically available to the public.

Abstract

BLOCKCHAIN-BASED DELIVERY ASSURANCE

Mehmet Demir

Doctor of Philosophy, Computer Science

Ryerson University, 2020

Climate-related catastrophes and wars are leaving people in need of aid. The main obstacle in providing help to people in need is the lack of trust in aid processes. Donors and charity organizations want to make sure that funds and materials gathered reach the intended destinations. The lack of proof leads to a general sentiment of waste, corruption and misuse, which undermines aid efforts. Blockchain technology injects trust into the business transactions through impeccable record keeping and fulfils the lack of trust problem in aid delivery. However, our review of relevant literature indicates that a delivery assurance framework that covers major aspects of providing a blockchain-based solution to aid delivery is absent.

In this thesis, we propose a novel blockchain-based transparent delivery framework for creating solutions that record and share data on the interaction of business participants involved in a delivery process. This framework is novel as it creates solutions that include handover and monitoring aspects of the delivery business and adds several benefits that come with the blockchain technology. This delivery assurance framework also provides complete guidance as it answers several key questions such as “How can we use blockchain technology to solve problems?” and “How can we make sure the solutions are financially viable and acceptable?”

Our simulation study validates the applicability of our framework and the solution we created using the framework. Further, the validation we received from an industry expert strongly suggests that a solution developed with our framework is applicable in industry. This thesis presents the development of the framework along with details on the design and execution of our simulations, including the raw data, data enhancement processes, tools, data structures, smart contract code, load testing methodology and the eventual analysis of the simulation results.

Acknowledgements

I wish to express my sincere appreciation to my supervisors, Professor Ozgur Turetken and Professor Alexander Ferworn, who guided and encouraged me on my work. Without their persistent help, my work would not have been realized.

Dedication

I dedicate this thesis to my family. To my wife Emily, my daughters Lara, Selin and Aylin, for their support and understanding.

Table of Contents

List of Tables

List of Figures

1. Introduction

Distributed ledger technology (DLT) and blockchain technology are emerging subjects in both academia and industry. These new ways to inject trust to business processes and connect participants without the need for a trusted authority disrupt business processes that connect multiple participants.

The goals of this thesis are to present a framework for blockchain-based delivery assurance and to present cogent arguments for its adoption. Several innovative use cases are developed and used experimentally to demonstrate the utility of this framework.

This thesis document begins with a detailed literature review to define terms, critically evaluate the state of the art, and identify gaps requiring exploration. As will become clear, the literature review indicates, there are no detailed frameworks disclosed related to blockchain technology. Most of the literature is focusing on either network-level technologies, simplistic use cases, cryptocurrencies or solutions with a relatively small blockchain component. Frameworks to guide interested parties towards solutions are not common. Therefore, the research presented in this thesis is essential and fills a significant gap.

1.1. Research Process and Contributions

The objective of this thesis is to design an implementation framework for blockchain-based delivery assurance. Whether it is a classic implementation of parcel delivery or a modern implementation by drone delivery or aid delivery as disaster relief, our implementation framework guides the implementation to inject trust into the business processes using blockchain distributed ledger technology. Finally, our main objective is defined as blockchain-based aid delivery assurance. From the beginning to the point of solving the blockchain-based aid delivery problem, we identified the following research questions:

- How can we use blockchain technology to solve problems?
    - What are the steps that we should follow?
- How can we make sure the solution is financially viable and acceptable?
    - What are the criteria in this assessment?
- How can we automate our operations in a blockchain?

    - How can we make sure about the security aspect of our implementation?
- Is disaster recovery a suitable target area for blockchain implementations?
    - What value does blockchain bring to disaster recovery efforts and services?
- If we decide to use autonomous vehicles in aid delivery, can blockchain add value to the services provided by the autonomous vehicles?
- How can we apply blockchain technology to the delivery industry?
    - What are the techniques to model delivery business as a blockchain and what are steps of this process?
    - What role does blockchain play in providing assurance of delivery?
- Is it possible to deliver aid and use the assurance model of blockchain technology to improve this service?

We have structured our research (Figure 1- Research program) in order to answer our research questions and create a chain of contributions that enable us to tackle the domain issues, solve them, and make contributions as a deliberate strategy to complete this thesis.

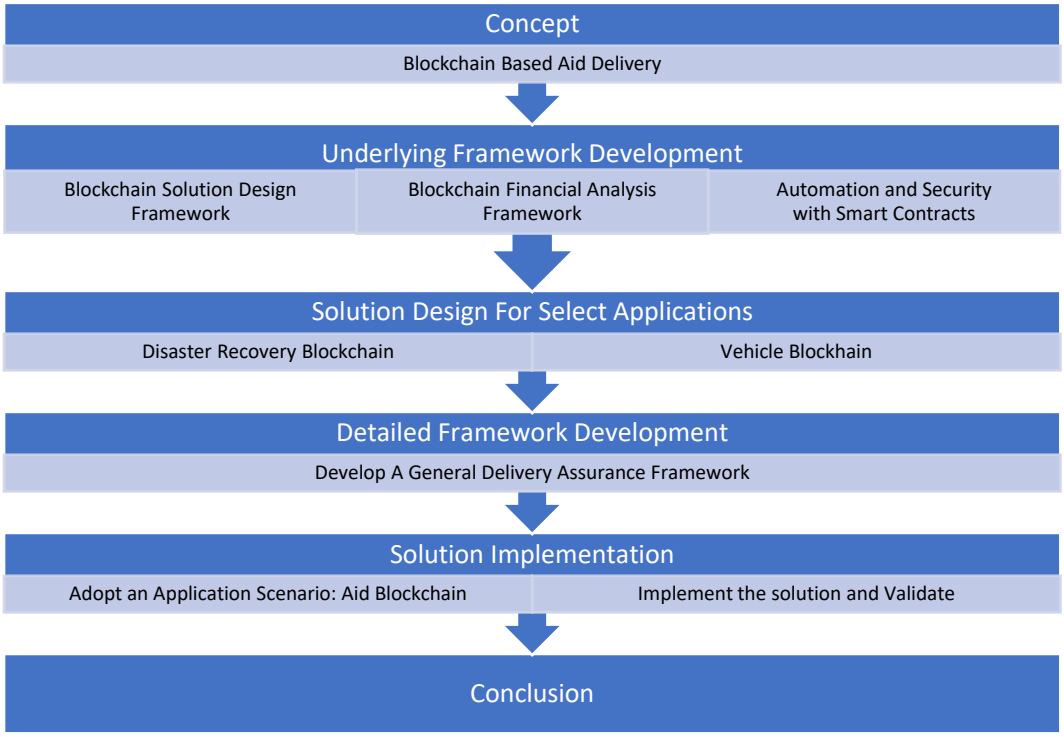


Figure 1- Research program

The first step of our research was to define the subject. We started our investigation on the topic of blockchain-based delivery assurance. After a detailed literature survey which lead to a deep understanding of blockchain technology, we recognized that the top two obstacles confronting blockchain implementations are usability and cost-effectiveness [1]. For a decision-maker to decide on blockchain technology as a solution to a business problem, these two points need to be clear. Two research questions immediately present themselves from this analysis: “How can blockchain actually be used to develop a solution?" and "Is it cost-effective to solve the subject problem with blockchain technology?" We confront these two crucial challenges in our work.

From our research we claim several contributions. Our first contribution is a blockchain-based solution framework called "Blockchain Technology Transformation Framework" (BTTF). BTTF is an enterprise transformation guide for the inevitable disruption caused by blockchain technology. It serves as a guideline for using blockchain technology to solve computational problems. We provide the details of this work in Section 3.1 (Blockchain Technology Transformation Framework). BTTF is essential for our research as we followed this framework to provide a solution to our target problem.

Our second contribution is the creation of a financial evaluation framework to analyze and evaluate the financial fitness of blockchain implementations. Details of this study are presented in Section 3.2 (A Financial Evaluation Framework for Blockchain Implementations). This financial evaluation framework answers the key questions on how we can make sure the solution is financially viable and acceptable. This framework guided us through defending the viability of our solution with a structured set of criteria and complete point of views.

Our solution framework BTTF indicated that blockchain technology solutions could support applications by automating the interactions between participants in a single atomic transaction using smart contracts. While this automation adds several advantages, our research indicated that smart contracts have security issues. We surveyed these issues, categorized them, and indicated the risks introduced by these issues in blockchain implementations. Details of this study are in Chapter 3.3 (Automation and Security with Smart Contracts). This study provides insights and answers the key questions on automation of the aid delivery operations on a blockchain. The findings of this study also greatly influenced our choices in the area of blockchain security.

We used our findings related to these two frameworks, and we evaluate their success using our innovative use cases. Within the Network-Centric Research Team (N-CART) the primary area of interest is Computational Public Safety with an overarching goal of one day creating systems that verifiably save even a single human life. As this is an admirable goal, our first use case is primarily concerned with is the disaster operations. We start with the use case of a limited impact natural disaster situation (severe damage caused by high winds) and implement a solution using blockchain technology. Details of this study are presented in Section 3.4 (Utility Blockchain for Transparent Disaster Recovery). This study provides insights and answers to the key questions on suitability of blockchain technology on providing a reliable information layer to disaster recovery teams. This study helped us start forming our fundamental arguments on the suitability of blockchain implementations at times of emergency conditions where normal systems and processes do not work. Disaster operations and IoT domains converge in the use case where relief efforts are delivered using high technology vehicles. Integrating a variety of vehicles such as Autonomous Unmanned Aerial Vehicles (UAV) to disasters requires the integration of a collection of technologies. Blockchain technology ensures the continuous collection of reliable data from vehicles. With this vital role of blockchain technology in the vehicle domain, we develop two use cases and use them in our research. We conducted a survey of the blockchain implementations and opportunities in the vehicle industry. We concluded that blockchain technology adds value to the services and information provided by autonomous vehicles. Details of this study are presented in Section 3.5 (Blockchain-Based Transparent Vehicle Insurance Management). Our central contribution is a blockchain-based delivery assurance framework. This framework provides guidance to build blockchain solutions to be used in a variety of applications concerning delivery systems to record delivery events. This framework not only records the delivery contact between the delivery service provider and the receiver but also is able to record the events happening to the package along the delivery path. Advances in IoT enable a wide variety of sensors to be utilized to monitor everything from the temperature of their monitoring target to velocity and acceleration that the device is exposed to. All this data can be communicated in near real-time with the anticipated advances in wireless technologies such as 5G. This framework guides the audience to create blockchain systems as a medium to combine conventional techniques and these new technologies. Details of this new framework are in Section 4.1 (Blockchain-Based Delivery Assurance Framework). This study formed the backbone of our work towards blockchain-based

aid delivery and guided us with the steps and principles of applying blockchain technology to the delivery industry. Findings in this study include the techniques to model delivery business as a blockchain implementation and the role blockchain can play in providing proof for the delivery events. We adopted an aid delivery application to validate our delivery assurance framework. This application is a complete reflection of the various findings in previous sections of this thesis. It is a disaster relief application, including vehicle interaction and delivery assurance. This application is developed using with BTTF and designed with the Delivery Assurance Framework. By adopting this application, we demonstrated the possibility to deliver aid and use the assurance model of blockchain technology to improve aid delivery service. Details of this study are in Section 4.2 (Blockchain-Based Transparent Disaster Relief Delivery Assurance). We finally constructed a blockchain system to test the validity of our delivery assurance framework and aid delivery solution. Not only did we construct the system, but we also tested its performance. Details of this experiment are in Section 5.1 (Experiment Implementation).

1.2. Publication List

The following is a list of our publications and the section(s) associated with them. Please note that each application is included in this document with permission from and according to the guidelines of IEEE.

- Section 3.1: M. Demir, O. Turetken and A. Mashatan, "An Enterprise Transformation Guide for the Inevitable Blockchain Disruption," Accepted for *IEEE Computer*. © 2020 IEEE. Reprinted, with permission [2]
- Section 3.2: M. Demir, O. Turetken and A. Ferworn, "A Financial Evaluation Framework for Blockchain Implementations," in *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, 2019. © 2019 IEEE. Reprinted, with permission [3]
- Section 3.3: M. Demir, M. Alalfi, O. Turetken and A. Ferworn, " Security Smells in Smart Contracts," in *IEEE International Conference on Software Security and Reliability (QRS)*, Sofia, Bulgaria, 2019. © 2019 IEEE. Reprinted, with permission [4]
- Section 3.4: M. Demir, A. Mashatan, O. Turetken and A. Ferworn, "Utility Blockchain for Transparent Disaster Recovery," in *IEEE Electrical Power and Energy Conference (EPEC)*, Toronto, ON, 2018. © 2019 IEEE. Reprinted, with permission [5]
- Section 3.5: M. Demir, O. Turetken and A. Ferworn, "Blockchain-Based Transparent Vehicle Insurance Management," in *IEEE International Conference on Software Defined Systems (SDS)*, Rome, Italy, 2019. © 2019 IEEE. Reprinted, with permission [6]
- Section 4.1: M. Demir, O. Turetken and A. Ferworn, " Blockchain and IoT for Delivery Assurance on Supply Chain (BIDAS)," in *IEEE Big Data 2019- IoT Big Data and Blockchain (IoTBB'2019)*, Los Angeles, California, 2019. © 2019 IEEE. Reprinted, with permission [7]
- Section 4.2: M. Demir, O. Turetken and A. Ferworn, " Blockchain-Based Transparent Disaster Relief Delivery Assurance," Accepted for *IEEE SysCon 2020, Montreal, QC*. © 2020 IEEE. Reprinted, with permission [8]

1.3. Contribution of Authors

Mehmet Demir is the first and primary author for all papers included in this dissertation. Mehmet completed primary research, created the design and identified the research undertaking. Mehmet took full responsibility for the research, collected the experimental data, and conducted all analyses included. Mehmet, as the first author, had the first and primary role in preparation of the manuscript.

Co-authors in each paper contributed with supervision of the research process, critical viewpoints, and reviews towards a more concise text.

2. Literature Review

In this section, we present a review that will detail the fundamental aspects of the technology as they are covered in the literature. This literature review will cover the literature starting from the background of blockchain technology. After an extensive background review, we will review the literature focusing in the areas of IoT and supply chain management. Our review will be concluded by an elaborate analysis of the literature where we identify gaps and how our work is similar to / different from what has been done so far.

First section in this review focus on the technology background. We will provide key literature about the cryptography behind blockchain technology starting from hash and signatures. We also review the distributed systems architecture with the advantages that it adds to blockchain solutions. After the technical fundamentals, we continue with the named structures and architectures that needs to be known to better understand blockchain technology. We will continue with the definition of the distributed content delivery networks, distributed ledger technology, which is the superclass of blockchains, and finally the blockchain technology. After a coverage of blockchain technology with its types, significant features and benefits, we widen the review with the review of blockchain technology in IoT. Building on the IoT, we review blockchain technology in supply chain management.

Considering the technology is very new and the implementations are not mature enough to prove the comparative value of the technology in academic mediums, significant portion of the literature are on the blockchain themed web sites, pioneer companies' web sites, consulting companies' reports.

This review section aims to be a base literature review of the technology in general. In each of the following major sections, we have additional reviews that are focusing on the subject area of each section. 3.1.1 reviews blockchain technology as a disruption vehicle, 3.2.2 reviews benefits, 3.2.3 reviews the associated costs, 3.3.3 reviews smart contacts in detail, 3.4.3 reviews blockchain technology in utility industry and 4.1.2/4.1.3 reviews blockchain technology in supply chain management related to delivery.

2.1. Background

2.1.1. Technological Fundamentals

2.1.1.1. What is a cryptographic hash?

Cryptographic hashing is the computational process that calculates a limited size output from arbitrary length data [9]. A cryptographic hashing process typically reads the input (a file or a stream) as a bit sequence, applies a cryptographic algorithm, and outputs the number of bits defined by the chosen hashing algorithm. For example, the SHA-256 hashing algorithm produces 256bit (32byte) hash values [10] regardless of the size of the input, whether it is an eight-character password or a four-hour movie. This process is repeatable; every time the same input is processed, hashing generates the same hash value. Cryptographic hashing is irreversible [11]. It is not possible to take the hash generated and rebuild the input. The generated hash value carries no information about the input. Therefore, it can not be used to extract or guess any features of the input data. Any modification in the input data, even a single bit, changes the hash entirely, and the difference between the two hash values cannot be used to identify what had changed from the first input to the second. The table below demonstrates the changes in input and reflection on the output.

Input	**SHA-256 hash**
A	06f961b802bc46ee168555f066d28f4f0e9afdf3f88174c1ee6f9de004fc30a0
B	c0cde77fa8fef97d476c10aad3d2d54fcc2f336140d073651c2dcccf1e379fd6
a	87428fc522803d31065e7bce3cf03fe475096631e5e07bbd7a0fde60c4cf25c7
Aa	a44cfdd61e71e607b82df307c44b2d6c2914544ccb2482c1049394c092f10e2a
aA	1b3dee655db3e0da56bb88420d8a709d3b7a789a647e467055a14e72784712de

Table 1- Visual display of differences in hashes

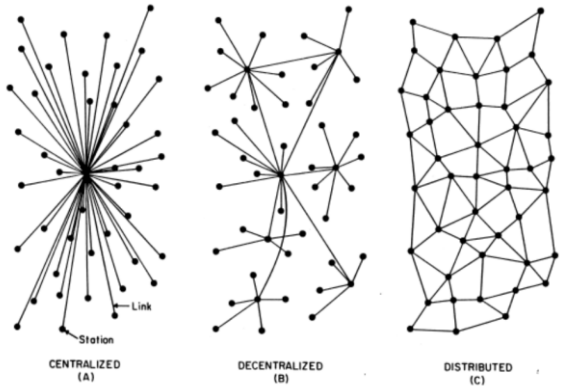
There are several use cases for the cryptographic hashing in the document management. First of all, cryptographic hash identifies the input data [12] with a mathematical certainty. This means that instead of a filename or any other assigned identification token, we can identify a file by its hash. This naming convention works the best for archives as the document does not change therefore the hash of the document does not change [13]. Second scenario is for modification or tamper detection. Since when data changes hash changes as well, we can identify if a document changed by comparing previously known hash value with the current hash value [14].

2.1.1.2. Digital signatures

A digital signature is a cryptographic analog of a hand-printed signature. Digital signatures are one of the by-products of public-key cryptography. They are typically utilized in the academia and industry to enable the verification of authenticity, integrity, and non-repudiation.

With the help of asymmetric (PKI) cryptography, every actor has a public and private key pair [15]. A public key is the one that is added to messages and known by every other actor. Public keys serve as the identity token on communication environments. Network participants can represent themselves on the communication channels with their public key (addresses). The private key is the information only the owners should know. A pair of public and private keys are cryptographically generated to have a mathematical connection so that when one of them encrypts data, the other one can decrypt and therefore verify that the other key had generated the encryption. Typically, when data is transmitted, the sender would create a hash and add the encryption of this hash to the message package [16]. This encrypted hash is called a signature since, by adding this, the sender enables all receivers to verify the originator and authority of the message [17]. With this mechanism, observers can trace which transactions are posted by which participants of the network. Identities can be pseudo identities or real identities. This is dependent on the design of the communication platform. Pseudo anonymity can establish privacy for their participants. Every operation that belongs to a participant is marked with her public key. Every actor with access to the historical records can trace which records have been issued by the owner of this specific public key. However, the real identity of the participant is not known. Some applications enable participants to use real identities. Where real identities are in use, the privileges of each actor are defined based on their identities.

2.1.1.3. Distributed systems architecture



[18]

Figure 2- Systems architectures

From several architectural choices in Figure 2, centralized and distributed models are worth comparison for our topic. Centralized architectures collect the authority and store the most critical information in a central component of the system. Distributed systems architecture allocates computing, authority, and information in multiple places [19]. Both have their own advantages and disadvantages. In different use cases, the recommendation towards which architecture to use can be different.

Centralized architectures are excellent for frequently updated resources such as frequently updated applications and real-time transactional data [20]. Distributed architectures are better choices for infrequently changing resources like documents. When a document is created, sealed and supposed to stay unchanged for a long time, distributed architecture has significant advantages towards providing high availability.

These two approaches differ from the risk and resilience perspective. In a centralized architecture, if the central node is not available for any reason, the resources cannot be accessed anymore. Such an access issue will result in outage and loss of services for the nodes in the centralized architecture [21]. Whereas in the distributed system, if any of the nodes are down, other nodes will pick up the load to minimize the impact on the overall system.

In the centralized architectures, two main performance factors are the performance of the central node and the latency between end nodes and the central node [22]. The latency factor almost always means low performance for the nodes that are the farthest from the central node, whereas the distributed system would minimize the latency since nodes will be most likely to be

served by their neighbors. Neighbor-to-neighbor traffic increases, but since the network distance traveled is reduced in the distributed computing architecture, network utilization decreases, and availability increases [23].

Distributed architectures have a significant advantage against censorship since the only way to disable access to a resource is to take down the entire network [24]. In comparison, when an authority decides to take down a resource in a centralized architecture, they can accomplish it from the centre, more comfortable and faster. Distributed architectures are also empowering users against data control. No system can disable access to an author's book, a music file, a picture, a tweet, or a conversation, because of any reason. Data belongs to the owner, and in a truly distributed system, it is not under control of a private library or social media companies.

2.1.2. Decentralized Content Delivery Networks

Traditionally, when the requirements include accessing static content from a large number of access points on the internet, content delivery networks (CDN) would be the answer. Decentralized and distributed CDNs are also introduced [25] to improve the performance of content delivery and reduce content delivery costs. The key benefit of the distributed CDN is the utilization of the bandwidth when it is advantageous and move the content closer to consumers with the distribution. When a consumer needs a resource, it starts searching from the near neighbors. Having content geographically nearby and utilizing less bandwidth in busy periods of network accomplishes both availability goals and performance goals or a robust CDN infrastructure.

In our literature review, we are not going to focus on the CDNs as they also have service layers that are optimized for millions of users to access a tiny percentage of the available data based on application or URL based identities. We will focus on the file system that enables the distribution of the data and enables hash-based identities. We are also not focusing on all the other varieties of protocols and streaming technologies that a CDN may invest in. Instead, our focus is on a file distribution protocol.

A well-known example of distributed content delivery networks is Inter Planetary File System (IPFS). IPFS appears frequently in blockchain solutions due to its capability to store files outside of the blockchain and with its ability to have a standard size link pointing to any file it

stores. IPFS is a distributed file system based on a hypermedia transport protocol [13]. It is a design based on distributed computing principles where the network of nodes each has resources, and their collaborated ecosystem has a higher aggregate amount of resources. There are subprotocols for finding, naming, bundling, and transferring the data. We will only focus on the features related to the static information where a file does not change with time, such as submitted reports, documents, and images.

Cryptographic hashing adds excellent features to IPFS. Since the resources are assumed to be static in our case, we can also state the hashes are static as well. Hash values identify the originating documents, and IPFS uses hash values as resource identifiers. A requestor needs to present the hash of the resource to request it. IPFS is the proving example that hash values can replace most of the URLs we use today.

Hash-based identification is not limited to a file. A hash can identify a part of a file, a complete file, a directory, or a directory tree such as a web site. Resources related to each other can be represented as a tree of hashes where the end nodes are hash of resources, and the branch nodes are the hash of their child nodes combined (Merkle tree) [13]. Merkle trees help to detect the changes and managing hash values with high performance due to the traverse access methods instead of a sequential access method. This tree structure also allows splitting documents and processing them in chunks.

IPFS has a lot more abilities on the way to represent the next generation internet. Static file access and transfer related features are very similar to the BitTorrent concept static files are shared in a peer to peer file sharing system. Each file should be available to any node in the system. Any node may copy the file into their system and serve it further. Once a file is replicated in this way, a node in need of that file does not need to go to a central repository or an edge server, which may also be down for maintenance at that time. It can just start by asking the neighbors if they have it and start from there. The absence of a central repository improves the resiliency of the network.

IPFS has more than five billion files uploaded [26]. This high number of uploads is an auspicious start for this technology. Each user does not have to have an installation of IPFS at their site. They also do not need to have a vast storage capacity to store all the documents on the Internet. Requesters know that they can request documents with only the hash of the document instead of a

specific server to access for a specific document, they will request the target document using IPFS gateways. The IPFS network will provide the target document.

2.1.3. Distributed Ledger Technology

Record keeping in the form of ledgers has been an important part of large-scale societies [27]. A distributed ledger is a ledger where the records and their relationships are distributed and replicated on a network [28]. Distributed ledger technology (DLT) is a structure to share information between members of a peer-to-peer network continuously. The purpose of DLTs is to have each member of the network retain the same ledger information [29]. The technology described as DLT simply standardizes the data structures, communication, synchronization, and integrity of the shared information [30]. Each DLT defines how its participants store records, how they share the records, how they will synchronize with the rest of the network, and how they will make sure the integrity of the information is intact.

The idea of distributed data or a distributed database is not new. Having data distributed to the members of a network helps reliability and increases the availability of the overall system by removing the single point of failure risk due to database failures [31]. Distributed databases also help performance by reducing latency for geographically dispersed database clients. Thanks to cryptography, today's distributed ledgers are forms of append-only tamper-evident cryptographic distributed databases [32] that provide trust to participants who would not trust each other otherwise.

2.1.3.1. Transactions

Each transaction is a representation of a business activity recorded as a ledger entry in DLT implementations. As the participants conduct business activities, they add transactions to the ledger, and the ledger grows. Attributes of the transactions are defined according to the business transaction details defined in the DLT implementation [33]. An accounting ledger entry is a simple example where a transaction (entry) has the attributes of timestamp, amount, source account, and destination account. As attributes are defined by the underlying business transaction, in a hypothetical car ownership ledger, attributes would be license plate, make, model, vehicle identification number (VIN), previous owner and current owner. Besides the attributes that represent business information, each transaction can have attributes assisting DLT features such

as a transaction identifier and a timestamp. For example, a car ownership ledger may have an attribute in each transaction as a pointer to the last sales record of the same car in order to quickly validate the seller of the car indeed owns the car at the time of sale.

2.1.3.2. Participants

Different types of participants can join the DLT network depending on their business motivations. As per the definition of distributed ledger technology, there is no requirement for participants to be uniform for their motivation to participate though a ledger may focus on specific business activity and has a specific structure to attract participants from a certain common background.

Depending on the technical specification of the DLT, there can be differences in the participation of members. There are DLT implementations identifying participants and practicing role-based access control. Other implementations assume an equal role for each participant and provide privacy to their participants by enabling them to represent themselves with pseudo-anonymity.

2.1.3.3. Decentralization

The baseline of every distributed ledger is the decentralized information architecture. There is no single book-of record, there is no central authority, there is no intermediary service, and there is no single point of failure. There is no dependency on any specific participant in the system. Nodes in the network do not need any permission for their activities [34]. Any node or several different nodes can be down, and the DLT system would continue working as usual with current online participants. When a new participant comes online, it synchronizes with one of its neighbors by downloading the history of the transactions and start receiving new transactions.

Participants of a distributed ledger implementation issue transactions and communicate the transaction to other peers in the network directly or through other peers. The simplest example of a DLT implementation with three nodes would work the same as a DLT implementation with thousands of nodes. When any node issues a transaction, it communicates this information to its neighbors, who then communicate it further on the distributed network, and this goes on until every node of the network eventually gets the message from their neighbors. Each member receives and witnesses the same set of transactions. Each node typically validates and stores the transactions.

There is no restriction on how to use the information. Each node may use the information for its business purpose. A simple example of DLT implementation can be an accounting ledger of a company in a network of accounting software, sales software, bank, and customers. When the bank receives a wire transfer from a customer as a deposit to the company's account, it issues a transaction on the DLT. Every member receives this transaction. The accounting software registers this as an accounting entry of revenue. The sales software assigns commission to the salesperson. The customer records the proof of payment and accounting entry of expense to the customer's accounting ledger.

2.1.3.4. Validation

For each participant, handling DLT transactions can have different complexities depending on the purpose of the DLT application. A complex DLT implementation may require its validation process to include complex business process logic, including interdependencies of transactions. Another DLT may have isolated and straightforward rules solely depending on the existence of some key attributes. In most cases, each member verifies new transactions with old ones in order to prevent inconsistencies. Once accepted, transactions become permanent in the ledger. This process of making the transactions permanent varies between different DLT types. A DLT may persist transactions one by one or as a package of many transactions. Depending on the persistence strategy of a specific DLT, specific data structures contain all validated records.

2.1.3.5. Immutable records

Distributed ledgers are append-only ledgers. Very similar to the classic accounting ledgers, DLT transaction entries are made in sequence. No entries would be inserted in between old entries. Old entries cannot be modified. If there is a need for correction, an adjustment entry would be added to the end instead of modifying any old entry. Since the size of the network and number of participants are not limited, these principles are important for the integrity of the information.

Historical information is vital for the verification of new transactions. This verification is only possible if every node in the network has the same information about past transactions. Immutability is essential as each participant can be sure that the past of the ledger can not change. There is no need to synchronize them further as long as they are obtained once.

2.1.3.6. Integrity protection

In order to accomplish a reliable synchronization of the past transactions, distributed ledgers are built to be tamper-evident. Tamper-evident means that when a transaction or a group of transactions changes in the ledger, it is possible and relatively easy to identify such an event occurred. Cryptographic hashing aids to compare and identify the tampering. DLTs are tamper-resistant as nodes detect tampered transactions, reject them, and preserve original transactions. The mechanism to use cryptographic hashing to maintain integrity varies between DLT implementations.

2.1.3.7. Transparency and traceability

The core element of today's modern society is digitalized information because information is power. In today's world, some authorities do not choose to share information. These authorities may be considering their own business benefits and save the information to themselves. A big part of the world is struggling to protect the truth and freedom of speech from oppression, censorship and the political landscape changes.

The privacy laws and consent considerations are also demotivating the authorities towards collaborating and make them less willing to share. One of the most critical reasons that information sharing is not widely applicable is the difficulty in establishing reliable integration to disseminate data with integrity.

DLT implementations provide business enhancement opportunities to all participants. Impoverished participants, non-affiliated participants, and passive participants can all benefit from the high-quality information flow. Diverse participation in distributed ledger networks is welcomed. Considering that trust is created through sharing the information and collecting the witnesses, the overall system can be stronger and more resilient with diverse participation. Diverse locations of the participants help improve the performance and reach of the overall network. Transparency distributes the authority equally and is a significant step towards preventing corruption. Authorities would be more careful and adamant against offenses when the evidence is public, and their reputation is at stake.

As part of transparency, records are made available to all interested parties. Active and online parties continuously receive transactions. Offline participants have the opportunity to

synchronize by downloading past transactions from neighbors. This level of accessibility to the information enables all participants with the ability to audit and trace information that is communicated on the blockchain. Traceability on a reliable and common platform is beneficial to all industries.

2.1.3.8. Example distributed ledgers

There are several types of DLTs. What data structure to use for packaging the transactions, how to make them tamper-resistant, and how to provide acceptance or consensus in the network differ between various DLT implementations. Tangle is one of the technologies that use direct acyclic graphs (DAG) to provide validity and uniqueness [35]. Several academic projects use DAG for network operations [36]. R3 Corda is a financial services ledger that has a "Notary" infrastructure to validate transactions [37]. Although it is by no means the only ledger technology, due to its pervasiveness and popularity, sometimes the term blockchain is used interchangeably as DLT. Due to its disruptive nature and its role in the birth of first major cryptocurrency, blockchain technology is the most dominant type of DLT.

2.1.4. Blockchain Technology

In this section, we define blockchain technology. We detail the methods, features, and attributes that blockchains add on top of the classic definition of distributed ledger to become the most prevalent distributed ledger.

2.1.4.1. Blockchain from distributed ledger origin

Mainly based on its performance [38] and capacity issues [39] due to the dependence on uninterrupted network access, having a distributed ledger was not considered a robust and dependable integration structure in the technology world. With the introduction of Bitcoin cryptocurrency, the technology world re-evaluated the paradigm and started using newly developed ideas that solved those issues.

The most popular distributed ledger technology today is the blockchain technology [40]. Blockchain is an append-only distributed ledger structured in an immutable chain of blocks of transactions where blocks are linked to each other with the post carrying the hash value of the former block. Blockchain technology enables preidentified or public members to create a

distributed network and share information in a pre-defined format [41]. Members of the blockchain network communicate with each other in a distributed fashion. If a node is down or unavailable, this does not impact the operations in the blockchain network.

2.1.4.2. Transactions and blocks

A transaction in a blockchain network is a unit of information that is added to the blockchain in its predefined format, including several blockchain specific fields and metadata. Each transaction conducted in the network is communicated to every node in the network, which means if any node desires, it can have the complete ledger that consists of every transaction ever conducted in the network.

Each blockchain network collects submitted transactions that are happening in a timeframe and form them into blocks. A block is a data structure that bundles transactions into an atomic unit. The creator of each new block seals the transactions that happened since the last block was created into a block like an envelope and communicates the block to the network peers as an atomic unit. Each block also has additional fields to store blockchain specific information such as a pointer that contains the hash of the previous block. This is where the name blockchain comes from, and the chain structure names this type of DLT a blockchain. Every block in the chain contains the hash of the previous block. When a new block is created, the hash of the last block is added to this new block.

2.1.4.3. Tamper resistance

With the chain structure, when a single block in the middle of the chain is modified, other participants reject the modified block as this modification changes the hash value and make it not match the hash value stored in its succeeding block. When an updated version of any old block ever been communicated in the network, nodes in the network would discard it as this updated block has a different hash than the next block indicates. Therefore, any forgery would be evident. With the same mechanism, a newly forged block cannot be inserted between two blocks. This verification of blocks is performed by every node that receives the blocks every time it receives blocks. Therefore, evidence of forgery would become apparent immediately, and all nodes would reject the proposed state [42]. A malicious attack may happen by forging every node, starting from a specific node. However, in this case, the majority of the participants in the blockchain will see

that the blocks they have are conflicting with the blocks that are communicated. This conflict will also result in rejection.

A block data structure facilitates the features of the blockchain application. The number of transactions and the timestamp are common attributes of a block in blockchains. Blocks can also carry attributes in order to save space and to enable rapid verification of the block. An example of such an attribute is a tree-based combination hash collection of all transactions that is named Merkle-tree hash root [43].

Blockchain technology uses cryptographic hash functions that have specific characteristics, such as collision resistance, and are different from hash algorithms used in other areas of computer science. In order for a malicious attacker to fail, the hashing algorithm must be collision-resistant. Collusion resistant algorithms make it unfeasible to find two blocks that produce the same hash value. By preventing the modification from going unnoticed, cryptographic hashing plays an essential role in tamper-resistance.

2.1.4.4. Types of nodes and retention

In blockchain implementations, all participants do not need to be the same. Typically, there are full nodes that have the entire ledger, lightweight nodes that have important details of the blockchain, and there are other participants that do not have to maintain a complete ledger [44].

Blockchain participants can keep complete details about all transactions. They can also choose to remove some information that they would not need from their own copy. A comprehensive set of information in any blockchain is the transaction details, block hash, and tree of transaction hashes. A full node has to contribute to the functionality of the blockchain therefore it must keep the complete history [45]. For example, if a bitcoin is transferred, a miner must know if the spender of the digital asset owns this asset so that it can judge whether the transaction is valid. The spender's ownership transaction might have happened ten years before the current spending transaction. However, an ordinary member with no intention of validating other people's transactions can keep a shorter history of the chain. Removing old blocks or old transaction data from the node storage is called pruning [46]. Growing blockchains benefit from pruning as the storage responsibility of each node is reduced with pruning. Pruning is optional and does not conflict with the integrity of the blockchain as some nodes always retain the complete set of

records, and the only records that can be pruned are the ones, which no longer contribute to the business process.

2.1.4.5. Benefits of permanent recordkeeping

The ability to retain records permanently without a chance of correction would enable blockchain stored records to be used as evidence in investigations [47]. Conflict resolution with shared information and documents is more straightforward. This permanent evidence layer also adds the ability to conduct investigations without the risk of outdated data. With time, there is a high risk that information will be misremembered, misrepresented, changed, or get lost. With the help of blockchain technology, investigations can be conducted not only in the immediate time frame but also in the future as well [48].

An evidence quality log of information is more like the track record of the events, and knowing the proof of wrongdoing can be revealed in the future would be a significant deterrent in the decision of information related crimes. Any individual that may be tempted with a quick win with information tampering may be discouraged with the chance of facing the accusations any time in the future.

Once the offense is detected, the blockchain will have undeniable details. The evidence would include cryptographic proofs and signatures. When data is entered into the system, it is signed by the originating person or authority. These signature data would undeniably prove the data's origin. This process of finding the origin and history of an item is called provenance tracking in supply chain management. Provenance tracking [49] is one of the biggest advantages of using blockchain.

2.1.4.6. New block creation and consensus

The first block in the blockchain is called a genesis block. This first block is the only one that is not linked to a previous block. A new blockchain starts with the genesis block [50] and continues as blocks get appended after the genesis block.

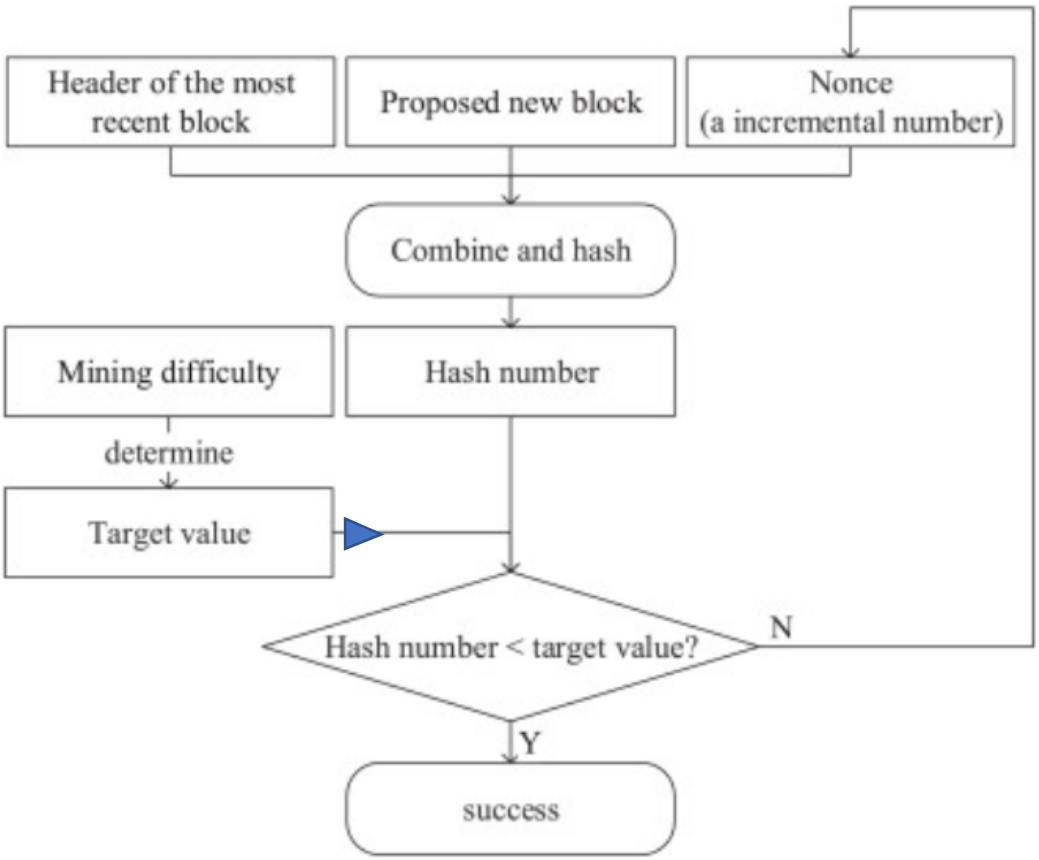
Creating a block is simply packaging all the transactions that happen in a timeframe. A block creator writes the transactions in a block according to the data structure adopted by the blockchain implementation. Creating a block is commonly viewed as a simple task [51]. Communicating this new block to all other participants is also something nodes can do easily.

However, how would all other nodes accept this newly communicated block as the next block? Dependent on the conflict of interest in the system, there can be parties that issue blocks according to their benefits. Therefore, the issuance and acceptance of the new block must be made difficult.

The process of a new block gaining acceptance in the blockchain is called consensus. Blockchain is a chain of blocks that are forged by consensus [44]. There are several ways to organize consensus in a blockchain. In public blockchains, proof-of-work (POW) that Bitcoin [52] uses, proof-of-stake (POS) that Dash [53] uses, or proof-of-capacity (POC) algorithm that Burst [54] uses are well-known consensus algorithms.

With POW, any node can create the next block. Between the nodes that are trying to create the next block, there is a potential that all or most nodes will create the next block at the same time. For deciding which next block would be adopted, a blockchain typically presents a competition through solving a puzzle that requires heavy processing. With this challenge, the node that completes the 'work' first and adds the proof-of-work to the block can successfully broadcast its candidate block. This added challenge stabilizes the block creation activities by making them difficult [55]. Typical blockchains include calculation of a distinctive pattern as a hash, which is also known as hash puzzle [56]. For example, calculating a hash value that starts with a certain number of zeros is a challenging task. It can not be pre-calculated as the block consists of transactions that happen in the timeframe that is just completed. Each candidate block consists of transaction data from a specific time frame. After transactions are collected together in a block, more information is added for each block for structuring the block and hashes. Finally, a small field named nonce is added [57]. Nonce has no information value. Block creator defines the nonce and it can have any value. In POW, in order to calculate the above-mentioned distinctive pattern, block creators work towards finding the right nonce by hashing with different values of the nonce. Finally, a successful nonce becomes the proof of work.

In the cryptocurrency world, the block creator is called a miner. Miners use specialized machines that are advanced in calculating hashes called application-specific integrated circuits (ASICs). These specialized machines' performance gives an advantage to the miner towards successful proof of work faster. The fastest miner to calculate the POW would have the advantage of distributing the new block early and getting accepted. POW blockchains typically reward the miners; therefore, there is a race for the reward [58].



[55]

Figure 3- Proof-of-work

POS assigns the next block creation duty to the contributors with the weight of their stake (or ownership) in the system [59]. It is also argued that participants with high stakes in the wellbeing of the blockchain would not harm the system with malicious activities. In POS consensus, the energy consumption of the overall blockchain is minimal compared to all participants spending energy to calculate the nonce in POW systems [60]. Besides the benefit of low energy consumption, POS-based blockchain systems can perform better since they skip costly calculations.

POC, also known as proof-of-space, assigns block creation privilege in proportion to the disk space allocation of the participant [61]. Proof of Elapsed Time (PoET) requires participants to wait for a random amount of time. A participant would be eligible to create a new block after waiting for a randomly determined amount of time for this participant [62]. There are other variations of the above-mentioned consensus algorithms. We will not go into further detail in this literature review.

2.1.4.7. Public versus private versus consortium blockchains

According to the governance and operating model, the literature identifies three types of blockchains. Public and permissioned blockchains are two main types as they are fundamentally opposed to each other. Consortium blockchains are essentially permissioned blockchains with key functionalities that are handled by selected members of the consortium, where the remaining participants benefit from the blockchain without getting involved in decisions.

Most well-known blockchain implementations are public blockchains. Public blockchains are open to all participants to join and access the blockchain, anonymously issue transactions [63], receive all transaction information, maintain a ledger, and to be considered for creating the next block. Not only the size of the public blockchain is a good indicator of the health of consensus and the integrity of the system, but the amount of communication and computation also increases with size. These extra computational duties may result in performance issues. For example, the block creation process for bitcoin is estimated to be 20,000 times more expensive than the legacy payment systems [64]. The latency of the public blockchain networks is also a problem compared to what the industry needs [65]. With the anonymity of usage, equality of participants, and openness of the network, popular examples of public blockchains are global.

Public blockchains do not identify the participants. They use pseudonymous identities where each participant is identified with an identifier without revealing a full identity [66]. With pseudonymous identities, between two operations, the system can know that if the identifier is the same, these transactions are conducted by the same participant. On the other hand, a participant may have multiple identities. Since pseudonymous identities prevent the system from knowing real identities, there are no defined roles in the operations of the public blockchain. Since public blockchains are entirely open, there is no guaranteed privacy of transaction information. Processes requiring privacy and role definitions cannot use these blockchains. Sharing information may not be acceptable for some businesses.

Permissioned blockchains address some of the privacy and confidentiality issues that are identified with the public blockchains. Permissioned blockchains implement the same underlying blockchain principles as their public counterparts. The difference is that participants are authenticated, and the network has custom rules. Authenticated participants can be assigned roles. Each permissioned blockchain network would have role definitions and corresponding

capabilities. In the permissioned blockchain space, there are two types of blockchains. Consortium blockchains [67] are permissioned blockchains where there is enough distribution of roles so that no one organization manages the blockchain. Fully private blockchains are introduced as blockchains where one organization manages the blockchain.

Permissioned blockchain implementations can handle the privacy of the data as well. Permissioned information between parties, such as details of a business contract, can be hidden from a third party even if they are members of the same network [68]. Public blockchains also are able to implement more complex structures than a simple chain of blocks. Separate modules and networks can be created for a variety of tasks in the blockchain network. Hyperledger Fabric of IBM is an example where there are modules such as membership management, and there are multiple networks separating transactions and consensus communication [69].

A permissioned blockchain is a solution for most businesses that would like to implement their own rules in a blockchain platform. Permissioned blockchains with customization ability make it possible for more businesses to share a blockchain even if they would not like to share data [70]. Partial sharing of data is also possible where public information is communicated. Confidential contracts can be created, and private transactions can be handled on permissioned blockchains. Custom roles also enable different activities, such as business transactions, governance, and audit [71].

Identification of the network members eliminates the risks created by anonymity. Permissioned blockchains define stricter rules around the creation of a new block and that of consensus. Custom rules, such as identifying how the blocks will be created and verified, also help solve performance issues [72] related to the public version of consensus.

Fully private blockchains do not provide the main benefits of the blockchain as the managing organization has the power to make decisions against blockchain principles. This type of fully private blockchain may be useful for proof-of-concept implementations in order to cut development timelines. However, for production implementations, they are far less beneficial compared to consortium blockchains. Fully private chain business scenarios also can be implemented relatively easily using traditional methods such as database-level permissions and database replication.

2.1.4.8. Privacy and security in public blockchains

Since public blockchains are mainly based on pseudonymous identities [66], observers of the transactions may trace the identities and identify all transactions conducted by a pseudonymous identity. By also noticing which other participants are involved in these transactions, it is possible to create a map of relationships. To prevent such information from being derived from the system and violate privacies, there are techniques to hide the trail of transactions.

The first technique is to collect a group of transactions together and mixing them to create another collection of transactions engineering the same outcome while hiding the relationships [73]. Mixcoin is an example of this technique where bitcoin transactions are altered to inject further privacy [74].

The second technique is the anonymous signatures where signing authority belongs to a group instead of a single participant [75]. More than one party in a group can sign a transaction made by any group member. This is generally a very restrictive technique as the formation and operation of a group is complicated. Group signatures [76] and ring signatures [77] are examples of this technique.

In order to prevent access to the data written on the blockchain, encryption can be used. This way, only participants that can decrypt the data can access the information. Common encryption techniques used in blockchain implementations include homomorphic encryption (HE) [78] which is implemented by Ethereum blockchain to hide the custom data injected into the transactions [79], and attribute-based encryption (ABE) [80] which requires all parties eligible for decryption to synchronize on the attributes.

2.1.4.9. Smart contracts

Besides transactions, blockchains contain code blocks that are called a smart contract. Smart contracts are automatically executed when triggered by the events in the blockchain. Since they are on the ledger, they indisputably exist. They cannot be lost as every node in the blockchain has a copy. They are tamper-resistant, just like any other record on the blockchain. They are fast, as there is no manual step or approval in the execution. As a contract, they save cost as it does not need a notary or any other intermediary. The ability to execute a transaction triggered by an event enables a wide variety of business scenarios that can be implemented on blockchains. When

combined with the trust infrastructure of blockchains, smart contracts are candidates for a medium for multi-party business transactions. Burstcoin and Ethereum are blockchains that pioneered smart contract implementations [54].

2.1.4.10. Performance and scalability

Most blockchain technology implementations are experiencing scalability problems [81] [82]. This also is the most significant risk facing the widely accepted blockchain implementations. Traditional frameworks such as Visa has a significant advantage compared to cryptocurrency networks like Bitcoin. There are several research projects and advancements in this area trying to improve the performance of blockchains. The most commonly proposed solution is adopting a structure different than a straight chain. Tangle technology, which uses directed acyclic graphs, provides high performance [83]. Graph technology also helps parallel mining [84], which improves performance. There are blockchain implementations such as Aerum [85] and Stellar [86] targeting higher performance by enhancing parts of existing blockchain protocols. Studies also indicate that the size of information on a blockchain has a significant effect on the performance [87].

Cryptocurrency networks are trying to enhance their scalability by recording the transactions off-the-chain in a private channel between transacting peers. When the transactions are complete or a need for synchronization arise, this private channel is terminated and transactions are persisted [88] using technologies such as the lightning network. Other solutions include segmentation of the transactions such as sharding. Sharding is the term for segregating the network into different channels called shards and use each shard to manage transactions on independent subjects. This parallelization in transactions improves performance [89]. Raiden network is a solution to performance issues by taking the transactions off the blockchain and using the blockchain only to record the results [90]. Lastly, the plasma solution organizes multiple blockchains into a hierarchy and distributes responsibilities in such a way that the shared parent blockchain is not overutilized while child blockchains become segregated ledgers [91].

Transaction speed is a known limitation of the utilization of known blockchain networks. Transaction throughput of Bitcoin is around 7tps, that of Ethereum is around 15, and even the financial system favorite Ripple is around 1500tps. Bitcoin has one more performance measure that indicates low performance, and that is the confirmation time around 55 minutes [92].

2.1.4.11. Common blockchain use cases

There are several use cases of blockchain. Even though the most popular ones are focusing on cryptocurrencies (representation of money) and payments, there are some document processing, and distribution ideas in the literature. These limited research instances are with a narrow focus, and they are serving generic tasks instead of designing a system for custom use cases. On the other hand, Estonian government blockchain [93] and JPMorgan Quorum [94] are institutionalized examples of blockchain technology with more focus on specific business domains.

Bitcoin is the first application that introduced blockchain technology. It is also the most popular application of blockchain technology as the appreciation of cryptocurrencies attracted significant investments. There are many other applications of blockchain technology in several domains, such as IoT, supply-chain, financial institutions [95], healthcare [96], automotive [97] and education [98]. Software vendors are supporting the technology by supplying application infrastructure [99], countries are implementing their own applications such as e-residency [100], and lawmakers are working on regulations to enable blockchains as evidence in the court of law.

Blockchain technology has implementations in every environment, including academia. In order to prevent the fraud and create a trusted platform for a tamper-proof store, multiple solutions are available or as a product [101] or in use by universities. Most repeated scenarios include storing certificates on Ethereum [102] with the aim of creating synergy and collective positive experience.

2.2. Related Work

This section starts with the literature review of the research that connects IoT and blockchain technologies. This connection is important to understand as the cooperation of IoT and blockchain makes both technologies more applicable. Blockchain's traceability and trust injection make IoT data more trustable. IoT systems such as a sensor operated door, or a face recognition vending machine is reliable under normal conditions. If there is an issue, system owners rely on humans to discover and report the issue. In case of a conflict, with the cost in mind, most systems have an adjudication playbook. But when the conflict of interest happens where two IoT systems interact, who can resolve the conflict? If both systems have conflicting information, what would be the conflict resolution playbook. IoT applications need the blockchain-based trust, especially when there is no other trustable non-IoT component in the system. On the other hand, IoT systems have a lot to offer to the blockchain movement. IoT universe has the necessary volume and observations that blockchain applications lack when they are in conventional industries. When supported by the wide variety of IoT devices, blockchain technology is more applicable and more beneficial.

The second part of this related-work section contains the literature review on blockchain technology in supply chain management. Reviewing supply chain management related blockchain literature is important to see the level of adoption and to understand the fit of the industry to the innovative potential of the blockchain technology. While reviewing supply chain management literature, we intentionally exclude the delivery assurance related literature as it is discussed in a separate section later.

We continue our literature review with the criteria to compare the existing literature with our work. We created a list of criteria that we can compare the articles side by side. We group these criteria. We also explain their relevance and importance.

In what follows, we have a detailed and critical review of the literature that has "blockchain-based delivery" theme which is closely related to our topic. We evaluate these articles using the criteria listed in part three, and we compare the key literature with our work. We evaluate what is missing in the current literature and how our work adds on top of the existing work of other researchers.

2.2.1. Blockchain and IoT

Historically, IoT used to be the set of simple and connected devices such as tracking devices for species-at-risk [103]. The size of these devices was a concern and limitation for most applications where the high price, short range, and low capabilities would result in infrequent usage. These devices gathered some data, but the amount was limited to their low capacity. At that low level of utilization, most IoT systems did not require speed or capacity as the data was limited and infrequent. However, in the last decade, new IoT systems designed to include connectable physical objects and people [104]. Addition to that, with the recent advancements in networking technologies, the set of connectable things potentially includes billions of people and many folds of devices. As a result, IoT system requirements are updated to include fast and high volumes of data as well as logic based on interactions [105].

There are two crucial IoT research areas that help us explain the relationship between blockchain and IoT. The first one is smart cities. Smart cities are the service relationships between humans, technology, and organizations [106]. Besides human and organizational involvement, we build Smart Cities by applying technology to the shared services and infrastructure. Advanced utilization of the technology resources and devices towards sharing economy enhances Smart Cities.

People, organizations, and devices in the Smart City concept have sophisticated technical requirements. Technology platforms need to provide automation, democratization, distributed computing, trust-less environments, transparency, privacy, and security. Blockchain is the right solution since it fulfills all these requirements [107]. Blockchains provide an environment where peers collaborate towards building a distributed information management system, and they use smart contacts for automated event-based actions. Most trust issues are handled with transparency and consensus, while the inherent privacy and security protect peers' identity and vulnerabilities.

The second important research area in the IoT world that we would like to introduce is smart homes. Smart homes are the micro blocks of the IoT architecture [108]. In order to reach more sophisticated levels of IoT in a house, one of the most important targets is integrating all sensors and devices. There is a need for data sharing and information integration on a secure platform since privacy is a big concern when data is collected from people's homes [109].

Trust is important to online transactions [110]. Building trust is a time-consuming activity that delays progress. Currently, most payment systems are built around central authorities in order to expedite trust. Credit card companies manage payments and provide trust to both sides of a trade. IoT industry is looking for ways to handle trust in a peer-to-peer network without any central authority. This platform must allow smart city participants or smart home participants to trust each other. Conflicts are inevitable, but an environment that can help to resolve conflicts is invaluable. We believe the solution is the blockchain technology. Blockchain technology enables trustless networks. The blockchain model actually removes the need for trust with full transparency and anonymity. Any node can download and maintain the immutable history of transactions. This makes every detail available to every node in the system transparently. Even though every transaction information is available to all, the identities of the participants are hidden behind their public keys.

Blockchain is an aid to IoT to solve reliability challenges. Decentralization and trust injection of blockchain would benefit "Smart Home," and "Smart City" [111]. Moreover, IoT systems have a high level of dependency on events and their outcomes. Smart contracts offer a solution to this requirement. Automation of outcomes to the expected events enhances the capabilities of IoT systems [112]. Issues such as longevity of devices make them vulnerable. Blockchain support can help eliminate such issues.

Device to device communication is often unsecured due to the lack of identity access management systems. A decentralized access management system for IoT can store and distribute endorsements and identifications as well as permissions [113].

IoT systems need a distributed information sharing mechanism such as blockchains in order to reliably share transaction information and in order to facilitate contractual agreements. This can not be done without addressing several issues. We need new architectures that can carry billions of transactions. This must be done while solving performance, capacity, privacy, exception handling, and legal issues [114]. Providing a solution with low cost is important as well.

Distributed ledgers are great tools to help home devices integrate. The most common blockchains today are not suitable for crowded and high volume IoT architectures. The typical public blockchains are computationally expensive, create high network overhead, and result in delays [115]. This combination is not suitable for most IoT devices situated in a house. Most of

these simple devices do not have the computation power, cryptographic ability, and storage capacity. Most devices also have low adaptation capability for new technologies. Therefore, the blockchain solution for IoT must consider current abilities of the devices [116].

Most current IoT projects focus on providing customized services to people where devices display different behaviours based on the user's profile. Whether it is a smart city or a smart home, this ability of devices accessing personal information puts the users' confidentialities at risk. Privacy is still a big concern while using blockchains. Blockchains are built with the power of transparency [117]. Blockchains can hide personal information, but complete confidentiality is hard to attain. There are breadcrumbs stored in the chain that may lead to precise information. Transactions and contract information can potentially be traced to more information.

Devices have disadvantages compared to the human-to-human interaction. Recognizing and fixing blockchain issues within devices can be time consuming and expensive. Tolerance to exceptions is very low in the IoT interaction scenarios. We can not imagine devices to be very fuzzy and act creatively to handle unexpected issues. Therefore, a potential issue for a human-managed system can turn out to be a big risk for autonomous device environment.

Whether the work is done at the lower or higher levels, whenever security is required on a blockchain, there is a high demand for cryptography. The cost of cryptographic operations in current implementations is high. IoT universe consists of small devices. Giving cryptographic abilities to these devices is not always possible.

There are several emerging examples of IoT and blockchain applications on data collection, crypto currencies for IoT and application use cases which include cryptocurrency Internet of Vehicles, energy trading, electric vehicle charging, smart cities [118] and smart homes [116]. These examples help us understand the emerging trend of using these two technologies together to provide better results.

2.2.2. Blockchain and Supply Chain Management

Supply chain management is a common term for the management of the flow of materials, products, and services [119]. Planning, sourcing, making, delivering (logistics), returning, and enabling are common components of supply chain management. Supply chain management utilizes the technology in every component from AI (artificial intelligence) in planning to BI

(business intelligence) dashboarding and real-time integrations. New technologies find good use cases in supply chain management [120].

Blockchain technology has been a prospective solution platform for supply chain management [121]. Currently, most supply chain management systems are designed as centralized systems. There is a heavy burden on this central authority to collect information, recognize events, and take actions such as billing and payments. Especially the logistics component of supply chain management has several use cases where blockchain technology can change the business. Logistics processes involve several interacting parties. Besides the exchange of goods and services, payments are part of the logistics where the emerging cryptocurrencies are potentially useful.

The supply chain industry is where trading partners interact with each other and experience the difficulties and challenges related to information asymmetry. Where there are parties involved in a trade, and there are continuous conflict of interest situations, blockchain is a natural solution [122]. Business events in the supply chain use cases can be stored in a blockchain utilizing all the features related to a ledger. Moreover, when certain events happen, smart contracts can be executed automatically and manage payments. Companies at distributed locations can conduct business without the need for traditional trust or central management but only with blockchain technology where all events and actions are recorded immutably.

Below are some of the main areas that supply chain management utilizes blockchain technology.

2.2.2.1. Trade finance- Reverse securitization

Companies that take part in international trade are familiar with the challenges of working capital management. Due to the open account trade, which necessitates the delivery of goods before the payment is due, there are risks that exporters take. Reducing this risk would be a great utility to international trade [123]. Blockchain technology is seen to be a good marketplace for the supply chain finance, where trading parties do not know each other enough to trust, and small participants are not well connected enough.

2.2.2.2. Shipping

The shipping industry is a well-known case of global supply chain trade. Due to the high number of trading partners and due to the possible conflict of interest on the containers from the

factories to their destinations through ports, customs, land transportation, and shipping, blockchain-based trust is very valuable [124]. Market leaders already joined forces to digitize the shipping industry on blockchain [125]. TradeLens platform [126] is a good example developed by the technology giant IBM and shipping giant Maersk. Their Chinese counterparts are also developing a similar platform called Maritime Silk Road [127].

2.2.2.3. RFID based systems

RFID systems are in use to identify products from factories to the store shelves and cashiers. Blockchain technology has enabled sophisticated uses of the tracking systems in order to prevent low quality or counterfeit products. By tracing goods from the factory to the store and to the hands of consumers, counterfeit products would be prevented by denying entry to the blockchain. Some valuable products benefit from trustable secondhand markets created on a blockchain as well [128].

Farm to fork processes are a well-covered topic in supply chain management. Transparency is not common in food supply chains. There are several concerns, such as food adulteration. Adulterated oil/honey, mislabeled seafood, contaminated milk, and horse meat in beef are some of the recent events in Canada, China and Europe. Transparency helps consistently finding the cause and path [129], and it is the only way to prevent these incidents. There are several cases that the solution is indicated to be a system tracing items using RFID tags and recording on to a blockchain [130] through the gathering, transferring, processing, warehousing, distribution, and selling.

2.2.2.4. Sourcing and procurement

Blockchain platforms with their ability to automate payments with smart contracts are most useful in the procurement domain of the supply chain management. Record-keeping techniques of blockchain technology can improve supply chain visibility and transparency. It is widely understood that blockchain technology by itself cannot solve any capacity, accessibility, and quality issues. Instead, blockchain technology is an enabler for implementations that encourage such abilities with visibility, transparency, and persistency [131].

Most blockchain projects in supply chain management are about provenance tracking. Provenance tracking is the record-keeping discipline that tracks the lifecycle of a product in order to be used in the future as a trail of quality. Provenance tracking is important for products such as

diamonds [132] and for other high value materials. In order to have a permanent ledger of the materials and tracking the materials' origin, blockchain technology can be a good solution. Procurement activities are closely related to the quality of the materials. For example, a supply chain that procures wood can trace the origin of each material using blockchain [133]. Another blockchain is designed for tracking the lifecycle of cardboard boxes [134]. Blockchain adoption in the procurement processes is highly likely and would be the norm when some of the early adopters take action. These early adapter actions are expected to put pressure on the rest of the suppliers.

Blockchain-based communication brings a transparency that solves the current issues with wholesale price contract management. Currently, these contracts create a case of double marginalization leading to supply insufficiencies.

2.2.2.5. Governments and insurance companies

Governments benefit from the openness of the companies operating in their countries. Collecting tax, issuing permits, and managing customs operations can be easier and reliable on the blockchain type of ledger. All the distributed architecture benefits would help operations to continue reliably where forgery can be prevented actively.

Insurance companies are the next largest group of indirect beneficiaries of the blockchain in supply chain [6]. Insurance companies are taking the risk of forgery, loss, and fraud. They are the victims of the information asymmetry [135]. Blockchain-based operations will provide them the most excellent tool to fight fraud and forgery while collecting great information to calculate risks and realize responsibilities.

2.2.3. Literature Comparison Criteria

Our work is targeting a complicated topic and multiple aspects of supply chain management. Before we list the literature comparable to our work, detail coverage of each article, analyze shortcomings and compare with our work, we created a set of criteria to represent every success factor that makes the candidates a good solution in our topic. In this section, we introduce the criteria. We also group them into subject areas in order to organize the analysis.

The first subject area is about introducing a framework to guide followers to solve business issues. The second subject area is focusing on physical delivery use cases in supply chain

management. We continue with the IoT subject area where we check the variety of data. A subject area on blockchain technology follows with criteria that analyze the adequate and quality usage of technology. The last subject area is focusing on the development project comparing the project artefacts.

2.2.3.1. Framework coverage and quality

Considering the hype, there is a possibility of misusing blockchain technology. Developing a general business solution framework or at least validating included use cases with a general solution framework proves an advanced maturity level. We check whether each article includes a solution framework aiding its followers to solve a business problem with blockchain technology.

Providing a solution to a specific problem in the supply chain domain is valuable. However, a more significant research target is providing a framework for a supply chain domain that is to be applied to multiple problems. We check whether each article provides a solution framework to followers that can solve a supply chain problem with blockchain technology.

The hype stage of the blockchain technology motivated applying the technology without adequate assessment. Especially an evaluation of the financial feasibility of the blockchain-based project or any cost-benefit analysis is a factor of maturity. Without a financial analysis exercise, projects may be conducted towards an expensive implementation that does not benefit the system towards a feasible solution.

Proposing an open framework that is able to include new and diverse participants is a positive value. In order to test this, we ask whether the proposed framework or the solution is suitable for crowdsourcing. Crowdsourcing is an innovation trigger that enables a high volume of new participants while strengthening the system.

Finally, this category of framework quality is tested by checking whether the proposed architecture is independent of a specific vendor with its platform, components, or blockchain implementation. Independence of the framework provides high adaptability and opportunity to advance with the emerging platforms. The majority of the early articles describe projects working on platforms that have high impact on the solution design. For example, Ethereum and smart contract-based solutions have restrictions on the data size, they are frequently advocating only to store the hash values, and they have capacity issues inherited from the named blockchain platform.

2.2.3.2. Delivery and supply chain

Our focus in the supply chain industry is on the physical product distribution and logistics. There are several research studies on other aspects of the supply chain. Significant examples are reviewed in our literature review on supply chain management above. However, if the supply chain related study is not on the distribution of the physical assets, it will not be a good comparison with our work.

In the logistics related research, our focus is on the issues related with the last-mile. Our framework is guiding the implementation of solutions to last-mile issues. We compare any other study with these criteria, whether it is also a possible solution to the last-mile issues.

Within the supply chain, and within delivery, we work on a possible solution to disaster recovery. Our use case is on delivery assurance in disaster recovery scenarios. Therefore, we compare the existing work and check if the solution is applicable to disaster recovery.

2.2.3.3. IoT

Our literature review on the IoT technology indicates the momentum of research on this topic. We believe that sensors and condition monitoring will enrich delivery business. Niche businesses of delivering perishable or condition sensitive assets present an excellent opportunity to start blockchain adoption. We compare if the related work in the literature has any sensors and condition monitoring. IoT data enriches the systems from capabilities and data perspective.

Usual events in the IoT universe are simple such as entry, exit, pickup and delivery. We look for a flexible solution that can accommodate a variety of events. A variety of events also means a variety of data sizes and a variety of data structures.

Some projects include the simplest of events in their scope, such as geolocation. GPS coordinates are small in size and can be collected with minimum technological challenge. We are checking whether the proposed solution extends beyond this minimum.

One of the important tools in emerging technologies is autonomous vehicles. These vehicles, which also include popular example named drones, are adding extensive capabilities to the supply chain, delivery, and disaster recovery. Therefore, we are checking whether the proposed solution includes or discusses autonomous vehicles.

2.2.3.4. Blockchain utilization/dependency

We first differentiate whether the solution is genuinely distributed or not. There are many research articles introducing a solution with key components in a centralized architecture. They describe the solution as a decentralized solution since there is a blockchain component involved. If there is a single point of failure or a similar vulnerability due to centralized components, we categorize the solution accordingly.

Earlier articles in blockchain technology related literature are mainly concentrated on the pioneers of technologies such as Bitcoin and Ethereum. With the influence of the hype and with the lack of business blockchains, dated implementations usually include a public blockchain. We test whether the existing work in literature is used or can be used with private blockchains.

Blockchain technology is only useful with quality participation. Well known risks like 51% attacks can be mitigated only with very high numbers of participation. Also, in business blockchains, even though the number of participants is not expected to be high, the scope of involvement is important. We find out whether all participants in the delivery ecosystem is thought about.

In the overall solution, the typical role of the blockchain technology is data collection. Blockchain technology provides integrity and trust. These features are enforced by the communication patterns that broadcast transactions to all participants. With these abilities, blockchain technology brings a trustable distributed database to the big picture. Comparable studies at least need to have this role for the blockchain technology.

There are several implementations of blockchain technology where the implementers use a relational database system as their primary data store, and the blockchain technology is only used as a medium of communication. This pattern of implementation is misusing the blockchain technology for capturing the prestige of using this new technology while using it more like an accessory in the overall solution. Some solutions present a blockchain as part of their ecosystem but not keeping the business-valuable data on it. Mostly guided by the privacy concerns, only a hash of the data is on the blockchain while the body of data is kept in alternative sources. Adaptation to the privacy restrictions is an essential feature of the blockchain solution, but the introduction of parallel data storage solutions usually brings the value of the blockchain down and

creates issues such as a single point of failure. Therefore, we check whether the data is kept primarily on the blockchain or in other systems.

2.2.3.5. Project and validation

In the existing literature, there are many articles related to ideas and use cases without any validation. Realistic validation is one of the criteria we have in our comparison. We check whether the articles report on an actual implementation.

Description of the implementation is not enough to understand the technical details. The first indicator of the technical quality and level of blockchain utilization is the code. When provided, we review the code and confirm some of the claims. The second question to every implementation is the existing metrics. Code without metrics is usually an indication of a validation in a test environment. Meanwhile, metrics are accepted as an indication of analysis and improvement efforts.

Finally, we check whether the implementation is still alive and active. An unreachable or out-of-order website is considered to be an indication of an unsuccessful project. Not having a way to access the project also can be interpreted that the implementation is no longer maintained. For successful commercial implementations, a professional website is almost always reachable. For the academic examples, we emailed the authors to ask for the status of the implementation project.

2.2.4. Existing Work in Blockchain-based Delivery

In this section, we review research and commercial projects in the field of delivery assurance using blockchain technology. We list the significant publications and compare them to this document with the criteria provided in the previous section.

2.2.4.1. HP3D – Wu et al.

Hybrid peer-to-peer physical distribution (HP3D) is a ledger architecture for supply chain distribution visibility [136]. This ledger architecture models the information flow between supplier, distribution centre, customer, and carrier. Even though the subject area is quite close to our work, analysis, framework, and implementation is quite different.

HP3D is not a framework for solving business problems for blockchain. It does not provide guidance on whether to use blockchain or not. It has a specific solution that authors promote for a specific problem. HP3D does not promote broad participation, such as crowdsourcing.

HP3D is not genuinely decentralized. It models an index server for the registration of the participants. It also specifies that an index server is a central component with a traditional database. This centralized design creates a single point of failure and makes this system vulnerable.

Data sharing methodology of HP3D is based on groups. Each group that conduct trades has a dedicated private ledger and adds anchor hash values to the designated public ledger. Even though this model of sub-chains is an applicable model for some use cases, there are several drawbacks to this model. HP3D suggests using the public ledger for monitoring and storing the hash values of the other events which are stored in the private ledgers. There will be participants opposing this indicating the location of the shipment is private. Malicious parties such as thieves would find location information useful, especially when it indicates a truck full of merchandise. There is also a significant limitation in the type of monitoring events where only GPS locations are monitorable.

The proposed architecture suggests creating blockchains of blockchains in this proposal in order to hide the information. Since the financial and operational costs are not discussed, the cost of every business contract having its own ledger is not calculated. Therefore, if the information is not transparent to more contributors, the additional benefit of blockchain is limited. The cost may exceed the benefits.

Finally, other publications [137] of the same author suggests that the provided article is a proposed architecture only, and the implementation does not include a blockchain. Instead, blockchain functionality is simulated with a no-SQL database (MongoDB). In the documentation, this persistence layer is called the database layer. The article indicates a set of distributed databases are used for blockchain technology scope. The author of the article also confirmed in an e-mail that the artifacts of the implementation are missing.

2.2.4.2. Modum

Modum is a company that has a solution implementation storing the sensor data for pharmacy products. Even though the blockchain implementation is added to the system, it is

backed with traditional systems due to the sensitive nature of the data. This dependence on traditional systems makes it a centralized solution that does not benefit from a decentralized architecture.

Sensors communicate with mobile devices that talk to HTTP servers, which store data in the relational database layer. Meanwhile, data is added to a blockchain [138]. Even though this solution uses blockchain technology, it is not decentralized. It has several single points of failure.

Modum lacks several features compared to our work. It is not a framework to help solve different problems. It targets a specific problem and provides a specific service. This is a commercial project that is bound to a specific vendor. Its limitations also include a lack of participation. The provided solution only serves the distributor company. Receivers and other stakeholders are not considered in sequence of business process events, interaction analysis, or data management strategy. There is also no shared metrics on this commercial implementation.

2.2.4.3. IBM TYS

IBM released its own blockchain environment as a verification network in the summer of 2019. A supply chain blockchain named Trust Your Supplier (TYS) comes with the promise of creating frictionless integration across supply chains while reducing costs. Cost reduction by elimination friction is a useful purpose for modernization on a blockchain if the cost of the reduction can be quantified. TYS is a background check blockchain [139] that enables the discovery, qualification, validation, and onboarding of suppliers [140]. In the TYS system, suppliers have digital identities. Suppliers fill questionnaires and load their business, geographic, industrial, and shared information onto the blockchain.

TYS is a blockchain solution for a specific problem. It is not a general framework to solve problems with blockchain technology. It is also not a general framework to solve a variety of supply chain problems. The TYS implementation is an IBM implementation and is a service provided by IBM. It is not a solution for delivery assurance. We included TYS in our review due to the solution it provides to the logistics business-related issues. However, it is not a delivery assurance solution to be compared to our work.

2.2.4.4. IBM TradeLens

The TradeLens platform [126] is another blockchain platform by IBM, which focuses on shipping. TradeLens manages conventional paper shipping processes through blockchain events. TradeLens manages the process, including all intermediary steps at factories, land transports, ports, ships, ports, customs, and warehouses. There is a lot of room for improvements in global trade. TradeLens targets to improve these points. Blockchain is a good platform for some of these functions. This product focuses on international trade and shipping more than delivery. It is built on Hyperledger Fabric. Costs and integration challenges to this blockchain had been significant issues for participants. Its claims on productivity, and benefits for the shippers are questionable [141]. Participants of this blockchain are shippers, and the competitive environment in the shipping industry limits the involvement of the shippers.

TradeLens is a solution implementation for the shipping industry. It is not a framework for the solution to guide implementers to take advantage of the blockchain technology innovatively to solve their problems. It is exclusively for shippers. It does not focus on the last mile. The solution is implemented, and dependent, on the IBM platform. It does not consider crowdsourcing or autonomous vehicles. TradeLens does not have the ability to be customized for disaster recovery. Main solution scenarios are all related to the shipping related supply chain such as customs-related documents, inspection certificates, dangerous goods declaration, and export declarations.

2.2.4.5. IBM Developer Community

IBM Developer community [142] has one of the most descriptive blockchain architectures related to disaster recovery. This blockchain solution is fundamentally modeled as a use case on IBM platforms. It is a general architecture that describes a complicated solution for a very focused problem. It is not a blockchain framework focusing on solving business problems with blockchain technology. It is not a supply chain framework that targets supply chain platforms.

Blockchain is only a piece of the overall solution. Most of the implementation is dependent on the IBM cloud platform to solve issues. The overall solution is not a distributed solution. The implementation stores its data on a NoSQL database. This shows the low reliance on blockchain technology. It is not an implemented project. It is merely an architectural model for any project to adopt to involve blockchain. Without implementation, the use case seems to be unrealistic since it includes videos recorded by users during a crisis and medical records. It also does not record the

IoT device data. Instead, it values the start and destination points in the order, which often can be wrong, or has to be altered due to disaster conditions.

2.2.4.6. H. Hasan & K. Salah

The academic study described in [143] presents a good summary of the benefits of blockchain. It mainly focus on the decentralized marketplaces where sellers and buyers meet, and payments are conducted in Ethereum cryptocurrency tokens.

This work is bound to the Ethereum blockchain and modeled with the capabilities of that. For example, it does not have a flexible model to store data on the blockchain, but it relies on the side systems such as IPFS to store the data while the blockchain only stores the hash of the information. The seller and the buyer are signing an agreement (not clear how), and the contract is stored in IPFS. The privacy concerns related to IPFS are not addressed. All transactions are stored and managed by smart contracts as Ethereum requires this. We review all the issues related to Ethereum and its smart contracts in a later section in this document. The smart contract code for this article is available online. However, a blockchain system is more than a collection of smart contracts. The main disadvantage of the smart contract is the inflexibility of the business model.

The proposed design has an arbitrator, and it is described as a ‘trusted entity.' The main reason that blockchain technology is required in business is to eliminate the need for intermediaries and trusted entities. It is controversial that this article proposes an arbitrator that adjudicates the transactions. It states that the arbitrator is an in-case role, which is not a fundamental component of the blockchain.

This model only focuses on delivery events and payment. It does not focus on any monitoring events. It does not consider that IoT sensor events will be recorded on the blockchain as part of the delivery cycle.

2.2.4.7. Drone Chain

The study in [144] is an article that connects the drones to blockchain infrastructure and lists the benefits gained from the enhanced data integrity. Even though the Blockchain technology has the promise of decentralization, this article presents a design that is a fusion of centralized drone system technology, centralized database technology, and blockchain technology. The result is a system with several single points of failure.

Even though the implementation is called as a blockchain-based drone communication architecture, the drawings in the article clearly indicate a drone system using a blockchain as an enhanced database. This architecture target can be accomplished by much simpler components in conventional methods. The need and benefits of the blockchain addition in this article do not have a convincing use case. All the validation and performance evaluation work provided is based on a private adapter named Tierion and is not realistic enough due to the encapsulation of the data and operations in that layer.

Since there is a third-party product that is used as the interface between the drone's logic and the blockchain, the value of the related code is minimal. Most business logic is in the control system and the cloud server whose application code is not provided.

2.2.4.8. Other studies with similar titles

There are some articles that have titles that suggests a similarity to our work. Despite the titles of [145] and [146], they mainly focus on the delivery of digital assets and identification of related fraud.

The research in [147] focuses on the delivery business domain. This article acknowledges the innovations in the delivery industry and the role of blockchain technology. It describes the business scenario of drone-based delivery. This article mainly focuses on two topics. The first topic is DeliveryCoin, which is a new blockchain template. This article gives low-level details on how to create a block, update a block, forward information in the blockchain, and internal economics of a coin based blockchain (similar to Ethereum and Ether). The second topic is the intrusion detection of the blockchain with machine learning algorithms. This article evaluates the consensus process of the blockchain with a large intrusion detection dataset. We are not directly comparing this article with our work as this article does not provide a blockchain-based solution framework to delivery business issues. It provides a framework for vehicle-to-vehicle secure communications.

2.2.4.9. Side-by-side comparison

Below is the table to compare all the papers that are considered to be the related work and have sufficient contribution to the field that we can compare to our work.

Table 2- Literature comparison

	Framework					Delivery S.C.			IoT				Blockchain Utilization/Dependency						Project/ Validation			
	A general blockchain solution framework	A solution framework for supply chain	Covers financial suitability	Suitable for crowdsourcing	Independent from a specific vendor	Ability to focus on disaster recovery	Physical product distribution and logistics	Focus on last-mile	Monitoring with IoT Sensors	Unlimited type of events	Monitoring other than the geolocation	Autonomous vehicles involved	Truly Distributed	A private blockchain	Involve every particpant, sender/receiver	A data collection platform	Data on the blockchain	Data primarily on the blockchain	An implemented project	Shared code	Collected/shared metrics	Still active
Our Work	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
HP3D – Wu et al.	-	Y	-	-	Y	-	Y	Y	Y	-	-	-	-	Y	Y	Y	-	- MongoDB	-	-	-	-
Modum	-	-	-	-	-	-	Y	Y	Y	-	Y	-	-	-	-	Y	-	- PostGreSQL	Y	-	-	Y
IBM TYS	-	-	-	-	-	-	-	-	-	-		-	Y	Y	Y	Y	Y	Y		-	-	Y
IBM TradeLens	-	-	-	-	-	-	Y	-	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	-	-	Y
IBM Dev Community	-	-	Y	-	-	Y	Y	Y	-	-	-	-	-	Y	Y	Y	Y	- Couch DB	-	-	-	?
H. Hasan & K. Salah	-	Y	Y	-	-	-	Y	Y	-	-	-	-	-	-	Y	Y	-	- IPFS	-	Y	-	-
DroneChain	-	-	-	-	Y	-	-	-	Y	Y	Y	Y	-	-	-	Y	Y	-	-	-	-	-

2.2.5. Summary, Research Gaps and Our Work

The literature validates the value of our topic. There is a need for a reliable and permanent tracking system for the resources deployed in the distribution domain, such as vehicles. It is also suggested that as long as such a reliable system is available, technologies such as GPS will be integrated as an input source of information [148]. There is a great desire for analytics aspects of data, and the only way to collect reliable data seems to be with a trustable technology such as blockchain [131]. Despite these acknowledgments of the need for the utilization of blockchain technology in the supply chain industry, especially in the delivery field, the amount of research is very limited.

In the literature, there are no frameworks for guiding new IoT implementations using blockchain technology. There are some tests related to suitability, but the guidance for the business leaders on appropriate usage of blockchain technology is missing. There is no framework matching the maturity of our Blockchain Technology Transformation Framework that we review in the following sections.

In the supply chain management literature, there are sufficient examples indicating high level of interest in the blockchain technology. The above-mentioned supply chain management research all includes examples of this interest. However, there are not enough studies and knowledge on "Where to start?" and "What to Adopt?" [149]. There are several studies that focus on technology. Several more studies are conducted for criticizing technology readiness. In order for the supply chain management to adopt blockchain, they need to understand benefits, compatibility with current practices, complexity of the usage, easiness of testing, and the provision of visible results [150]. Our use cases and experiments presented in this dissertation enable this deep understanding.

There are plenty of ideas on what to do with blockchain technology in all industries. The supply chain industry also has many blockchain use cases that are mentioned in the literature review. However, the ideas are stuck in the conceptual modeling, and many do not reach any validation phase. Most do not get implemented due to the missing business stakeholder support. One reason for this missing business stakeholder support is the lack of financial analysis. There is no financial framework that project owners can use to comprehensively explain their blockchain project. We review our financial evaluation framework in the following sections.

Blockchain technology is fundamental for systems trying to reach distributed trust. However, several implementations of the blockchain technology projects create a system that actually is not entirely decentralized. Our projects are entirely decentralized with the idea of identifying the issues with decentralization and find solutions to them instead of avoiding those issues with workarounds.

We believe decentralization opens the way to crowdsourcing related innovations. Current crowdsourcing projects still require a trusted entity. For example, there is still a company named Uber that provides trust to users of its service. We are not intentionally removing these trust organizations from the solutions. However, our framework for supply chain delivery makes sure that the system is flexible for including an unlimited number of partners without central management.

As a framework developer, a significant difference we have with the majority of the literature is the independence from a specific vendor or a specific blockchain. Projects that are bound to use, for instance, Ethereum, inherit all the limitations of this blockchain. In order to reach the flexibility of the data model and agility, we avoid such vendor dependency. There are products that IBM provides. These products are well integrated into the rest of the IBM Cloud. However, this product mentality and integration reduces the flexibility of these solutions. We provide frameworks to enable the ability to be implemented to any blockchain of choice.

Within the Network-Centric Research Team (N-CART), the primary area of interest is Computational Public Safety, with an overarching goal of one day creating systems that verifiably save even a single human life. As this is an admirable goal, our work targets to use blockchain technology in disaster recovery. Therefore, our frameworks have the flexibility to be used in disaster relief scenarios, and our uses cases that we validate include disaster recovery.

One of the main gaps in the literature is the lack of IoT blockchain integration. Frameworks that model the delivery business with IoT monitoring events are very rare. Where they exist, they are limited to one type of attributes such as GPS or Temperature. Our model is not limiting the type of events and keeping the data model open for more monitoring, which is vital for sensitive deliveries that need the blockchain provided trust more than uncomplicated deliveries. Another critical point that is not covered in the literature is the autonomous vehicles and other autonomous

agents. The model for these vehicles is different since they lack the human factor. Our framework specifically focuses on drone delivery to show the difference.

Our data model is flexible for the followers to choose between keeping all the data in the blockchain or linking it to other data sources. This flexibility gives us the ability to avoid choosing a data store and getting stuck with the privacy issues related to it. With our model, if the data is public, then it can be kept in the blockchain. If the data is large or private, it can be saved in JSON based lightweight linked json object standard (JSON-LD). This methodology also allows encryption that can be used in the data store or on the blockchain hosted data. Among all data hosting options, one option that we avoid is the central database that most applications seem to be based on. Instead of having a central database to speed up the system, we prefer to focus on the performance bottlenecks of the blockchain and provide a solution to those.

Although several articles in the literature provide only designs, we implement a solution using our frameworks, share the code, share the metrics, and keep the project active for further research.

3. Underlying Framework Development

After a detailed literature survey which led to a deep understanding of blockchain technology, we recognized that in order to design an implementation framework for blockchain-based delivery assurance, we need to define how to create successful blockchain solutions. In this section, we go through our work that provides guidance on how blockchain implementations can be successful, cost-effective and secure. Contributions of this section to our overall research program is circled in red in the figure below.

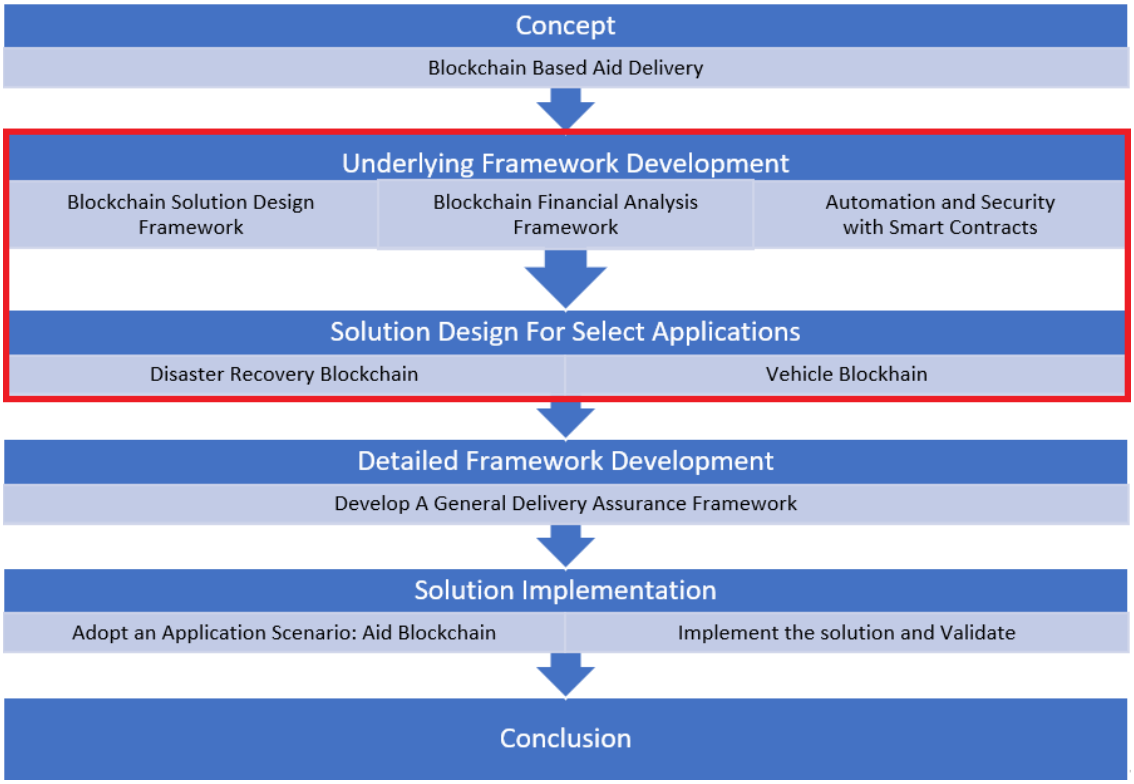


Figure 4- Research program - Underlying framework development

The first topic in this section is a blockchain-based solution framework called "Blockchain Technology Transformation Framework" (BTTF). BTTF is an enterprise transformation guide for the inevitable disruption caused by blockchain technology. It serves as a guideline for using blockchain technology to solve business problems. While creating a solution for Blockchain-Based Delivery Assurance, we use BTTF to make sure our solution is structured and complete. By following the structured process steps of BTTF listed in Figure 5, we could ensure all aspects of our solution is validated and detailed.

Question	Action
Who? Participation	Identify independent collaborators in the process. Decide if anonymous participation is allowed. Decide who can approve or govern this process. Identify how participants can benefit from a trustable distributed ledger and transparency
What? Tokenization	Identify digital assets used in the transactions. Find out how these assets are currently represented and stored by each participant. List the sensitivity of the attributes towards transparency. Find out the book-of-record process dependencies. Find out what information current intermediaries request and provide.
Where? Network & Interaction	Identify how participants interact with each other and how this would change with peer-to-peer networking Identify which interactions utilize which tokens. Identify each participant's role for each token
Why? Trust -injection	Identify current trust issues. Find out quality issues with current service Decide how to provide trust (select from below) • Extended communication • Data sharing, process tracking, • Tamper-resistant transaction history, logs, audit trails, • Fraud prevention, • Transparency, and censor resistance.
When? Events & Automation	Identify events in the system. Identify which events can trigger transactions that can be conducted automatically Identify which interactions have a contractual nature.

Figure 5- BTTF framework process

The second topic in this section is a financial evaluation framework to analyze and evaluate the financial fitness of blockchain implementations. We use this framework to make sure our solution is financially viable. This framework answers the key questions on how to make sure the solution is financially viable and acceptable. This framework guide us on defending the viability of our solution with a structured set of criteria and complete point of views shown in Figure 6.

$$V_{financial}\,(u) = \sum_{focus\ area=1}^{5} (v_{area}(focus\ area))$$

$$focus\ area\ = \{solution, features, costs,$$
$$other\ factors, implementation\ and\ operations\}$$

Figure 6- Value statement of a blockchain implementation

The third topic in this section is the analysis of business logic automation methods in blockchain applications. While the automation adds several advantages, our research indicated that smart contracts have security issues. We surveyed these issues, categorized them, and indicated the risks introduced by these issues in blockchain implementations. While we are creating a solution for Blockchain-Based Delivery Assurance, we use findings of this work to design the automation and prevent possible security issues. The findings of this study also greatly influenced our choices in the subject of blockchain security.

We continue with our innovative use cases in order to apply previously defined frameworks. We start with the use case of a limited impact natural disaster situation (severe damage caused by high winds) and implement a solution using blockchain technology. Our blockchain-based transparent disaster recovery study provides insights and answers to the key questions on suitability of blockchain technology on providing a reliable information layer to disaster recovery teams. This study helped us start forming our fundamental arguments on the suitability of blockchain implementations at times of emergency where normal systems and processes do not work.

Disaster operations and IoT domains converge in the use case where relief efforts are delivered using high technology vehicles. Integrating a variety of vehicles such as Autonomous Unmanned Aerial Vehicles (UAV) to disaster aid requires the integration of a collection of technologies. Blockchain technology ensures the continuous collection of reliable data from the vehicles. With this vital role of blockchain technology in the vehicle domain, we develop two use cases and use them in our research. First, we conducted a survey of blockchain implementations and opportunities in the vehicle industry. We concluded with an implementation related to storing vehicle and ownership information.

In this section, the following research questions are addressed.

Research Question	**Addressed by**
How can we use blockchain technology to solve problems? What steps should we follow?	BTTF
How can we make sure the solution is financially viable and acceptable? What are the criteria and point of views in this assessment?	Financial Analysis Framework
How can we automate our operations in a blockchain? How can we ensure the security aspect of our implementation?	Automation and Security with Smart Contracts
Is disaster recovery a suitable target area for blockchain implementations? What value does blockchain bring to disaster recovery efforts and services?	Blockchain-based Transparent Disaster Recovery
If we decide to use autonomous vehicles in aid delivery, can blockchain add value to the services provided by the autonomous vehicles?	Blockchain-based Transparent Vehicle Insurance Management

Figure 7- Research questions addressed in Chapter 3

3.1. Blockchain Technology Transformation Framework

In order to provide a solution to delivery assurance with blockchain technology, two research questions immediately present themselves from this analysis: “How can we use blockchain technology to solve problems?” and “What steps should we follow?”

Our first contribution is a blockchain-based solution framework that answers these research questions. We designed this framework as an enterprise transformation guide for the inevitable disruption caused by blockchain technology. It serves as a guideline for using blockchain technology to solve computational problems. This framework guides us throughout our research by providing a solution to our target problem.

This chapter is submitted and accepted for publication [2]. It is not yet completed and published at the time of this thesis preparation. M. Demir, O. Turetken and A. Mashatan, "An Enterprise Transformation Guide for the Inevitable Blockchain Disruption," Accepted for *IEEE Computer*.

Blockchain technology offers great potential to disrupt and revolutionize businesses. Industry is taking notice of this potential as evidenced by numerous bootcamps, courses and seminars about this technology. However, executives have been caught in a position where they are informed about the concept but not equipped with the right questions to ask to leverage the potential of blockchains. Technology professionals are knowledgeable about the technology, yet not many substantial business problems have been solved with blockchains. Unorganized effort is spent on getting involved in practice projects on sandbox environments. However, there is not a lot to learn from the cumulative experience of the community of blockchain adopters as what is available is a collection of stories about projects without convincing evidence of their business benefits. This, combined with the concerns about the technology due to privacy, security, performance and capacity issues, makes it imperative to organize the thinking on blockchain-based innovation. We believe a good start to this is the identification of a comprehensive set of questions to decide whether and how a blockchain-based solution could work for a particular organization. Reluctance to adopt disruptive technologies may be a significant competitive disadvantage for an organization whereas proactive planning can be a significant advantage. Understanding where and how blockchain technology will disrupt existing processes will benefit business executives.

We propose a framework through which enterprises can determine if and how they can viably and cost-effectively transform their business processes to be supported by blockchain technology. We provide key questions in order to provide insight into how using blockchain technology might be helpful.

New blockchain-based business models should present collective benefits for all involved stakeholders. Increasing involvement generally enhances the reliability and resistance of these systems. Marketing of this paradigm to classically trained individuals is a managerial challenge.

Due to the nascence of this technology, widely accepted industry standards have not yet been formed and organizations are defining their own access rights, data structures and allowable transactions [151]. This lack of standards has been identified as a managerial challenge which BTTF can help alleviate. BTTF provides a guideline for standard defining activities, which will help organizations form a complete set of definitions in their blockchain solution. By following BTTF, executives can also find out whether blockchain is the right solution for their business challenges. A well-designed blockchain solution based on BTTF increases understandability for stakeholders and demonstrates business benefits to decision makers limiting speculations.

3.1.1. Blockchain Technology as a Disruption Vehicle

3.1.1.1. Business impacts

Without any compelling reason, businesses would not just switch to blockchain technology. To evaluate potential benefits, the following features of blockchain implementations need to be analyzed for their impacts on the particular organization and a specific business scenario as some of these features may be positive for some organizations and negative for others. For example, transparency may concern stakeholders of a certain organization due to its impact on privacy and liabilities whereas another organization may consider it an asset.

Auditability and Traceability: Auditing is essential and very manually intensive. In the absence of trust, auditors spend a lot of time and resources to cross-check the validity of data. Blockchains solve this problem by keeping the complete history of transactions and by providing traceability guaranteed by cryptographic methods. An auditor can easily verify the veracity of transactions based on the events on the blockchain.

Transparency: Having the state and outcome of a business process transparent to the stakeholders increases their trust in the system and improves service experience. It assures all participants of the integrity of the system and the processes. Blockchains can deliver this when the transactions are occurring on a network open to all participants. The value proposition is at its highest when it brings transparency to lengthy processes such as supply-chain management.

Provision of Trust: When processes involve applications owned by different parties, disputes arise over what exactly has caused an incident to occur. When parties rely on their own copy of the records, reconciliation becomes a major part of a resolution. Blockchain technology can enable the participants to have the same copy of the records, leading to a quick and cost-effective resolution that also increases confidence.

Permanency: Information is power and there may be intentions to not share it or only share what supports a specific cause. In business-to-business communication, omission can be used for the purpose of hiding mistakes or failures. Communication platforms migrated to blockchains have the advantage of maintaining the original truth through this tamper-evident mode of communication. Blockchains enforce availability, integrity, and permanency of the complete truth.

Eliminating System Dependencies and Intermediaries: Blockchains can remove the need for a separately maintained book-of record, a central authority or an intermediary through its decentralized architecture, which also removes the risk of a single point of failure. New blockchain-based systems can effectively complete transactions such as cross border money transfer in minutes without any intermediaries.

Event-driven Automation: Smart contracts have made event-driven automation possible. Coupled with the trust provided by blockchain technology, smart contracts can simplify complex business processes by alleviating the need for manual interventions without compromising the integrity or quality of the overall process.

3.1.1.2. Blockchain enabled features

Below is a list of features that blockchain technology helps to improve. When one considers a benefit such as transparency, they should question whether it would add value, eliminate a weakness, provide an advantage or whether it is a threat if competitors have this feature. An

alternative approach would be investigating whether the corresponding question is a common question in the business process.

Process Tracking – Who does What? Blockchains are very good at recording business events and communicating those to all participants. Such event communication and persistence make blockchains ideal for process tracking.

Sensitive Records – Who can Access What? Sensitive records can be protected by means of cryptography. Ownership of records can be transferred on digitally signed transactions. Encryption can protect the necessary authorization tokens while access and permissions can be traced and audited on the blockchain.

Identity Management – Who is Who? Trading partners can share identity related information on blockchains, e.g., verifying the information about a customer and placing the public credentials of the customer on the blockchain with a flag indicating that this is a verified customer.

Digital Asset Ownership – Who Has What? Cryptocurrencies showed that ownership transfer can securely occur on blockchains without an intermediary.

Voting – Who Approves What? Voting is very similar to digital assets from an ownership perspective. The ownership of the vote, i.e., ability to send or assign the vote, would be given to the user at the beginning of the process. Businesses can model complex processes with smart contracts combined with voting.

Product Traceability – Where is What? Tracing the order, transportation and subsequent delivery of the products in a supply chain can be handled on blockchains. Blockchains would inform partners of the events, and the status would be shared on the ledger. Order, payment, transportation and delivery events can be managed by smart contracts.

Intermediary and Settlement Agencies – Why the Middleman? When there is a distributed ledger and all participants trust the accuracy of the data, there will not be need for a middleman.

3.1.1.3. Challenges ahead of mainstream implementations

Some challenges with widespread implementation of blockchain technology are easier to resolve while others may take considerable amount of time and coordination among industry stakeholders. Some of these roadblocks are of technical nature while others are business related.

3.1.1.3.1. Technology challenges: A promising technology at its infancy

Unlike many others that were first developed and matured in academia, blockchain technology has not gone through academic due diligence, which makes it susceptible to a variety of issues.

Software Issues: Each active participant in the blockchain network needs the blockchain network specific software for issuing transactions with consensus. Such software is developed in open-source platforms, and encapsulates the rules of the network that may change as the network matures. There can be small changes updating some of the rules slowly [152] or material changes where the network should be upgraded to a new version [153] or even emergency changes [154] to prevent a high-risk issue. In order to publish the updated software and manipulate the behavior of the blockchain network there are two well-known choices: soft and hard forks.

Technical Integration Challenges: Introducing blockchain technology in an established enterprise requires adopters and connectors between legacy systems and processes and the blockchain. The architectural differences may make the integration near impossible [155]. In some cases, blockchain adoption could mean a major revamp or a total construction from scratch due to incompatibility.

Scalability and Performance: Due to the decentralized architecture and consensus mechanisms, transaction verification takes some time on a blockchain. This can be easily tolerated in many cases such as a supply chain, where it may be a major roadblock in others such as stock trading [156].

Cybersecurity: There are several ways blockchains are protected from malicious activities. Cryptographic methods protect the interactions by preventing forgery of blocks or preventing nodes trying to tip the consensus. The system is strong and solid as a whole, but is vulnerable at its nodes. If participants do not have adequate security at their ends, blockchains are open to malicious activity through impersonated clients. If hackers access the private key of a participant, they can issue bogus transactions. The anonymity provided by the blockchain empowers hackers in this case. For example, BitCoin had reputational problems when one of the exchanges got hacked and bitcoins got stolen [157]. This exchange went bankrupt and public trust towards blockchains got a hit.

3.1.1.3.2. Business challenges

The nascent nature of blockchain technology will be more concerning to business executives who look at technology merely as a business enabler.

Talent Shortage: The industry does not yet have a sizable pool of solid talent who can implement robust blockchain implementations. Besides cryptocurrencies, blockchain instances are mostly Proof-of-Concept (PoC) implementations with only 5% to 10% moving to production [158]. The lack of blockchain technical experts prevents organizations from moving faster beyond PoCs. Blockchain focused technical skills are not yet taught in standard higher education curricula therefore solid blockchain skills are rare.

Cost-Benefit Analysis: Upfront cost of blockchain implementation is high. It includes new infrastructure and a capable team so existing revenues can be negatively impacted. A big initial investment and loss of existing revenues are justifiable in the presence of sizable benefits; however, some costs or benefits are not easily measurable hence making the adoption decision difficult. Unlike operational efficiency, it is not easy to assign a dollar value to trust or reputational risks.

Governance: Health and sustainability of business interactions are guaranteed through defined rules and responsibilities. An intermediary system can manage interactions and maintain service level agreements. An authority can define rules and enforce accountability of participants. In a decentralized architecture, however, we lose intermediaries and authorities, and have to opt for decentralized governance in the form of consensus mechanisms or a regulatory body [151], which does not define a single owner for the governing rules and can result in volatility and uncertainty.

Uncertain Regulatory Status: Laws tend to catch up slowly with new technology such as blockchains [151]. Current major players such as banks, insurance companies, government agencies and lawyers who are highly regulated are waiting for clear rules for widespread adoption hence there is considerable effort towards legislation. Most concerns are about users and their possible relation to money laundering or similar illegal activities. For governments and revenue agencies, money flow and related tax implications are still a concern.

Cultural Adaption: Business owners are used to solving their problems with systems by sharing minimum information, and concentrating on divided responsibilities. In blockchains, sharing the information makes it more secure. This change, which not only distributes power, but also reduces the control of former authorities, would likely threaten some potential participants. Attracting participants is important for the success of the blockchain [151]. Trusting a system with a greater number of participants rather than one with centralized authority is a new concept, which requires a culture change.

Reluctance to Change: Fear of unknown technology and its possible shortcomings can cause concern. 'If not broken, why fix it?' has been the motto of many business executives. Meanwhile, resistance from third parties such as trusted intermediaries who may lose their relevance adds to the overall reluctance.

3.1.2. Blockchain Technology Transformation Framework (BTTF)

Many blockchain research initiatives focus on applying blockchain technology to a specific scenario or industry. It is common to see research describe the use-cases for an industry and decide suitability with the end state, i.e. the final solution by following a flowchart [159]. While helping with the decision of whether to use blockchain or not, these frameworks can be more narrowly focused on the current technologies and problem, instead of transformation of business and discovery of opportunities.

This end state focus also ignores which methodology is followed. For research purposes, focusing on a specific aspect of the problem is natural, but in the industry, lack of a methodology can end with cookie-cutter applications of the technology, which can lead to unsuitable applications or clone applications such as the creation of hundreds of digital coins after one or two successful ones. Unnatural applications of blockchain cannot provide the desired benefits.

We propose a structured solution (transformation) framework for organizations to redesign their processes or identify opportunities for using smart contracts. The introduction of a new trust model influences the number of collaborators. With the help of our framework most current business processes designed to communicate with a minimum number of external systems or partners can be redesigned to have many more collaboration partners.

BTTF presents five key questions to analyze the participation, tokenization, interaction, trust-injection and events/automation characteristics of the target business process. Detailed analysis of these characteristics reveals whether the business process is suitable for improvement with blockchain technology. Each characteristic is analyzed with further questions. While answering analysis questions in each area, organizations learn about the suitability of the blockchain technology for their business process.

There are two types of questions in this framework. The first type is a question that requires identification of one or more items. For these questions, the number of identified items is an indication of better suitability. For example, while answering the question of "Who?" one identifies independent collaborators. Existence of several independent collaborators, the ability to add more, or the expectation of having more, increase the ability of a blockchain solution to improve the business process. On the other hand, if there is only one collaborator, or there is a cluster of collaborators all managed by one entity thus removing any independent decisions, a blockchain solution may not bring much value. The second type of question focuses on decisions which enables the future direction or an existing constraint to become an input to the blockchain-based transformation. Having discussions to provide these decisions helps process owners understand what alternatives they have with blockchain technology and what the consequences of using blockchain are. The ability to have a clear decision shows the strong possibility of improvement while not being able to decide shows the possibility of future issues. For example, whether anonymous participation is allowed or not is necessary to decide the type of blockchain. The ability to decide on these items indicates a clear direction. If there are challenges to make such decisions, this could be an indication of the problem domain being too large for a single solution.

Figure 8 shows the five key questions in BTTF. In order to understand the suitability of a potential blockchain solution, analysis is necessary in all these five areas. Below are the descriptions of each question and their analysis process to guide the business process owners while using BTTF. We start with understanding "Who" (participants), continue with "What" (tokenization of assets and information), then "Where?", which reveal the details of the interaction network in order to understand how "Who" and "What?" are interacting. "Why?" is a question to discover the issues to solve and the benefits to gain. "When?" helps to understand events in the system that helps us to use blockchain technology with its smart contracts and automation tools.

Question	Action
Who? Participation	Identify independent collaborators in the process. Decide if anonymous participation is allowed. Decide who can approve or govern this process. Identify how participants can benefit from a trustable distributed ledger and transparency
What? Tokenization	Identify digital assets used in the transactions. Find out how these assets are currently represented and stored by each participant. List the sensitivity of the attributes towards transparency. Find out the book-of-record process dependencies. Find out what information current intermediaries request and provide.
Where? Network & Interaction	Identify how participants interact with each other and how this would change with peer-to-peer networking Identify which interactions utilize which tokens. Identify each participant's role for each token
Why? Trust -injection	Identify current trust issues. Find out quality issues with current service Decide how to provide trust (select from below) • Extended communication • Data sharing, process tracking, • Tamper-resistant transaction history, logs, audit trails, • Fraud prevention, • Transparency, and censor resistance.
When? Events & Automation	Identify events in the system. Identify which events can trigger transactions that can be conducted automatically Identify which interactions have a contractual nature.

Figure 8- List of framework questions

Who? – Participants: The re-design process starts with the analysis of existing actors to identify the participants involved in the process. Introducing blockchains will revolutionize the communication, interaction, and collaboration of these participants. Participants in the old process may have new roles in the new process. Depending on the overall business goals, there may be new participants to fulfill desired process outcomes. Existing participants can remain only if they are independent collaborators in the network. For the participants in the new blockchain led design, the next step is to decide whether every participant in the process can approve and govern. Accordingly, designers can decide about the type of blockchain design. A higher number of participants justifies the use of blockchains.

What? – Tokenization: What goes into an entry in the ledger is fundamental to the usage and benefit of the blockchain. It is possible to place various types of tokens into the blockchain. One of the most common types of tokens are digital assets. Therefore, identifying digital assets with their attributes such as ownership information and identifiers should be the starting point for tokenization. If tokens do not emerge as a result of this analysis, the next step can be to find out whether there are entities in the process that multiple systems are interested in. A token can be created from such an entity that multiple systems are interested in. If the process benefits from all transactions related to this entity to be on the distributed ledger, it can be marked as a token. If there are existing book-of-record systems or intermediaries, they can be excluded in favor of similar functionalities over the blockchain. Analyzing the request and response structure may reveal the detail of the peer-to-peer communication over the intermediary and this communication structure can be used to define new tokens.

Where? - Interaction Network: In order to operate on the peer-to-peer distributed network structure of blockchains, each participant needs to have the ability to connect with several other participants. An important design target is to eliminate any dependencies on a specific group of nodes and removing any single point of failure.

Why? - Trust Injection: The most valuable feature of blockchains is the trust provided to normally untrusting participants conducting a transaction. At this point in the process design, all previous findings should be validated considering trust requirements. Existing trust issues should be listed and prioritized. If a process with the identified participants, tokens and interactions requires trust, the use of blockchains would be justified. Each trust requirement should be matched with a particular blockchain feature.

When? – Automation-Events: This step reveals the events that can be detected in the redesigned process for previously identified participants, tokens, and interactions. For each event, actions would be identified. If an action would automatically trigger a transaction, smart contracts are relevant. Smart contracts would initiate new transactions when predefined events are realized in blockchains. Many legacy processes do not have an event-based approach to automated transaction execution. Therefore, identifying automated transaction sources can be an extended discovery effort. Automation may lead to cost savings. Identification of these savings is important as it helps justify the new blockchain implementation.

3.1.3. Use Case 1: Supply Chain – Global Trade

Most international supply chains are difficult to track. Products and goods change several hands from manufacturers to consumers. Building a foundation of trust is hard considering the variety of trading partners. The current need for such trust is mostly filled with intermediaries and by filing several copies of legal contracts. The additional costs of acquiring trust and process traceability are very significant. For example, documentation and follow-up costs for a container shipment are more than double the cost of real physical shipment work [160]. We present a simplified use case of an international supply chain process to demonstrate the concept, steps and value of BTTF in this context.

The analysis in Figure 9 shows that the target supply chain use case is a good candidate for improvement with blockchain technology. There are plenty of independent collaborators. Participants have motives and benefits from the implementation. There are several well-defined tokens present in the process. There are a lot of ways that the collaborators will benefit from the new token model and the new interaction model. The current trust issues and quality issues are well listed. Almost all possible ways of injecting blockchain related trust into the new process model are confirmed. Several smart contract opportunities are identified including a partial payment automation. Our framework has been followed well in the above example and the process is a good candidate to be improved by blockchain technology.

3.1.4. Use Case 2: Real Estate Sale Process

Multi party agreements such as a real estate sale process require information to be shared between the seller, the buyer, their lawyers, their banks, their spouses, insurance companies, the power utility, the gas company, city utilities, land registry and government revenue taxation agencies, which are traditionally done by sharing information between two parties at a time. Smart contracts can execute the sale, transfer responsibilities, change the ownership, and transfer the money. Such a system under close monitoring of so many stakeholders would be more trustable than one where each stakeholder keeps their own records with partial information.

The analysis in Figure 10 shows that the target real estate use case is a good candidate for improvement with blockchain technology as well. There are plenty of independent collaborators. Participants have motives and benefits from the implementation. Most of them have clear duties

and responsibilities tied to the success of the collaborated process. There are several well-defined tokens present in the process. Ownership related information is a good token. With the old and new interactions, there are a lot of ways that the collaborators will benefit from the new token model and the new interaction model. There is established trust at the moment, which is based on the parties' experience in the past. Even though the execution seems orderly, currently transparency is limited, and operational redundancy is very high. Almost all possible blockchain related trust injection is confirmed to inject trust and efficiency into the new process model. It is identified that the majority of transactions can be automated with smart contracts. Our framework has been followed well in the above example, and the process is a very good candidate to be improved by blockchain technology

Who?	What?	Where?	Why?	When?
Independent collaborators Factories, Land transportation providers, Freight forwarders, Customs brokers, Governments, Ports, Ocean Carriers, Insurance, Retail businesses.	**Digital assets used in the transactions** Shipment, Export certificates, Container.	**How participants interact with each other** Participants currently interact with several media of communication including online, e-mail, fax and paper. There are several business-to-business custom integrations.	**Current trust issues** Participants can hide the issues and defer responsibilities due to insufficient, imprecise, corruptible, forgettable and not provable information.	**Events in the system** Several handover events where a participant delivers the item, and another receives it. Government approval Customs clearance Loss and Damage
Are anonymous participants allowed? No. This process requires participants to have identities and permissions.	**How is this information currently represented and stored by each participant?** Product details, Shipment status (OK, lost, damaged), Ownership of the shipment, Documentation, Approvals.	**How do the interactions change with peer-to-peer networking?** There would be great transparency if every stakeholder can access others and receive information from all. They can create more successful plans with more information.	**What are the quality issues with current service?** It is not clear where the shipment is, why it is late, whose mistake delayed the arrival.	**Which events can trigger transactions that can be handled automatically?** Several payment and acknowledgement transactions can be automated with the delivery events, e.g., custom duties to be paid when the item is in the port.
Can any participant approve or govern the steps of this process? Each participant has a major role in the governance of this process.	**What are the book-of-record process dependencies?** Factory is the book of record on the content Land transportation providers and ocean carriers are book of record on location and destination Ports are book of record for departure, arrival.	**Which interactions need which tokens?** Factories, land transportation providers, customs brokers, governments, and retail businesses need product information token. Customs brokers, ports, ocean carriers, and retail business need container token.	**How is trust provided?** Extended communication, Data sharing, Process tracking, Tamper-resistant transaction history, Audit trails, Fraud prevention, Transparency.	**Which of these interactions are contractual in nature?** From factory to the retail store, many mini transactions and payments can be coded in smart contracts and executed by sensor events, e.g. 30% of the payment to be paid to factory at the time the shipment leaves the factory. 20% to be paid when shipment is in the ocean carrier.
What are the DLT benefits? Each party can have a clear view of the process details and see incoming shipments and provide their process details downstream.	**What is the information current intermediaries request and provide?** Freight forwarders coordinate the movement of goods to their destination and handle the necessary paperwork. They would request product and destination information and provide estimate of arrival.	**What are each participant's roles?** Since there are several equal contributors, the roles can be distributed uniformly. Participants can all form nodes to create new blocks. Due to the business volume, they all have stake in the health of this blockchain. Privacy concerns between competing businesses should be handled at the token level to hide details that should not be shared.		

Figure 9- Framework responses- Supply chain - Global trade

Who?	What?	Where?	Why?	When?
Independent collaborators The seller, the buyer, their lawyers, their banks, their spouses, insurance companies, the power utility, the gas company, city utilities, land registry and government revenue taxation agencies.	**Digital assets used in the transactions** Real estate ownership, insurance, power and gas contracts, city utility services, mortgage application, mortgage.	**How participants interact with each other** Currently there is one to one interaction between participants. There is process based centralization around lawyers. Buyer interacts with her lawyer and her lawyer interact with most other process stakeholders.	**Current trust issues** Buyer does not see the process state. Her relation is solely based on her trust in the lawyer and her perception of the reliability of the process Seller does not know when the funds would be deposited Buyer is not sure if ownership is transferred Buyer is not sure if utility contract is in effect Bank is not sure if insurance is valid and not cancelled.	**Events in the system** Sale agreement Closing Mortgage funding
Are anonymous participants allowed? No. This process requires participants to have identities and permissions. Another alternative is to have the incorporated entities as identified while individuals anonymous. Trusted such as lawyers can introduce the anonymous entities to the system in order to enable their anonymity while validating, they are real.	**How is this information currently represented and stored by each participant?** Buyer and seller has paper documents. Lawyers has paper and scanned documents. Bank has mortgage agreement Insurance company has insurance contract details Power and gas company has service contract details Land registry has the title information.	**How do the interactions change with peer-to-peer networking?** There would be great transparency if every stakeholder can access others and receive information from all. As the needed information is already shared, the number of interactions between the participants would decrease significantly.	**What are the quality issues with the current service?** Why there is gap in information held by different public agencies and the banks? Why do buyers need to provide the same information again and again?	**Which events can trigger transactions that can be handled automatically?** Closing event can trigger several transactions: land transfer, utility, gas, power bills activation. Insurance starts. Money transfers, etc.
Can any participant approve or govern the steps of this process? There are some major roles in the process. Banks, government and lawyers. Governance can be done by all the major stakeholders. Distributed governance. Roles like buyer and seller are not suitable for governance.	**What are the book-of-record process dependencies?** Land registry is book of record for title.	**Which interactions need which tokens?** Lawyer-Land Registry-Real estate ownership Lawyer-Insurance-Title Insurance contract Buyer-Insurance-Home insurance contract Buyer-Power and gas companies-Power and Gas contract Lawyer-city utility services-City utility services contract Buyer-Bank – Mortgage Bank-Lawyer-Mortgage	**How is trust provided?** **Extended communication** – Buyer and seller can receive the extended communication events and know about the status. Income tax authorities are notified from the sale immediately. Tamper-resistant transaction history – All steps would be on the blockchain so there is no dispute. For example, there is no dispute that city utilities bill starts from the closing day. There is no dispute that power bill starts from the closing day. Tamper-Evident Logs, Audit trails. In case of a dispute, the events that happened are all in the blockchain. Fraud prevention. Every detail is shared on the blockchain about the sale. For instance, a lawyer trying to commit fraud would be obvious as all steps are on the blockchain.	**Which of these interactions are contractual in nature?** Closing, land transfer, utility, power, gas. several of these interactions are contracts. Smart contracts can execute the sale, transfer responsibilities, change the ownership, and transfer the money.
What are the DLT benefits? Seller and buyer can benefit with the ability to access to a repository to observe the state of the process. Lawyers can communicate the details, manage the signatures and close the deal transparently.	**What information do current intermediaries request and provide?** There are not many intermediaries in this process. The main process issue is the number of interactions between entities and risks associated with it. In order to understand the entities in the process, we need to look at every one-to one process.	**What are each participant's roles?** Mortgage – Buyer signs, bank provide funds, lawyer attach the fund to closing agreement.		

Figure 10- Framework responses - Real estate sale process

3.1.5. Conclusion

Applying blockchain technology without a multi-dimensional assessment of the business process may result in an unnatural application of blockchain that cannot provide the desired benefits. In order to prevent this problem from happening, we introduced a prescriptive approach for transforming business processes. The Blockchain Technology Transformation Framework (BTTF) is a structured way of assessing whether business processes can be improved with blockchain technology.

BTTF applies to any existing business process or a new business process candidate. Beside our use case examples in supply chain and real estate, other industries such as finance, government, insurance, and energy are well-known application areas that can benefit from applying BTTF. Applying BTTF to more sensitive business processes such as the ones in the healthcare industry would reveal the critical compatibility issues between the process and blockchain technology.

A limitation of the BTTF is the manual nature of the analysis. Our research will continue on this topic, and we will develop a tool in order to automate the planning and execution of BTTF based analysis. This tool will help in understanding the details of the analysis questions, evaluating the answers, informing on the impact of the choices, identifying possible conflicts, generating ideas on the opportunities as well as comparing the analysis of different processes. The comparison ability can also improve our framework with the possibility of an empirical assessment of the framework. This empirical study can also include real-life use case studies to evaluate the impact of adopting the framework.

3.2. A Financial Evaluation Framework for Blockchain Implementations

After creating a solution to delivery assurance by using the process and questions provided by BTTF, we continued our research with one of the top obstacles confronting blockchain implementations: cost-effectiveness [1]. Blockchain solutions such as ours are exposed to the next research question: “How can we make sure the solution is financially viable and acceptable?” and “What are the criteria and point of views in this assessment?”. In order to answer these research questions, we conducted the following study and created a financial evaluation framework to analyze and evaluate the financial fitness of blockchain implementations. This framework guided us through defending the viability of our solution with a structured set of criteria and complete point of views.

This chapter is submitted, accepted and published [3].

3.2.1. Introduction

Blockchain is becoming a critical priority for enterprises [161]. With the tech giants embracing and enabling it [162], more enterprises are considering to adopt blockchain solutions to improve their business capabilities or modernize the current technology stack. Similar to any new technology adoption, benefits and costs of the implementation depend on numerous parameters mostly specific to the adopting organization as well as the target solution. For each blockchain, for each set of participants, and as a solution to various target business problems, there can be different costs and benefits of implementing a blockchain.

In the literature, there is no study providing a framework to decision makers aiding financial assessment of their blockchain implementation projects. With the lack of structured framework, executives can simply get carried away with the hype and make inaccurate estimations about the financial aspects of the blockchain implementation. With financial factors of the blockchain implementations, it is also possible to compare this new technology with the alternative techniques and tools.

Our novel contribution is providing this financial evaluation framework. This paper presents a structured framework to evaluate the cost and benefits of the targeted blockchain solution. This framework evaluates different aspects of the blockchain project and results in a set of formulations that will detail the overall financial model. Since the value of each detail depends on the project details, it is not possible to calculate a resulting monetary amount. However, following the framework will leave the only remaining task to be placing numeric values on the items.

This paper structures the evaluation process by dividing the overall scope into focus areas. The first area of evaluation is on what purpose blockchain serves in the target architecture. The second area is focusing on the features that blockchain provides. The third area is focusing on the costs that blockchain potentially reduces. The fourth area is other environmental factors and motivation. Finally, the fifth area is the actual implementation and operational costs.

At each focus area, we present the related factors to be considered in the evaluation. We prefer a cumulative approach to the value statement of each area. Therefore, the financial value related to the area is the weighted sum of the values from each factor. The value of the factor is relative to others in the organization. Two organizations can use different values for a factor. At the least, the financial gain from the factor benefit different organizations differently. For example, for a large size, high profit, mature company, the value of retiring legacy systems can be very high. On the other hand, a young start-up would see nearly no value in this factor. An organization can value the same factor differently year over year according to their budget and strategic direction.

The weight of a factor is defined by a specific project or use case. For the same organization that value the factors in a uniform way, these values would contribute to the overall value with respect to the use case. For a use case under observation, the weight of the same factor would be defined with the scope of the project.

After going through all these five areas, an evaluator can have a profound understanding of the factors forming the financial value. When the analysis is complete, this paper will continue with a use case and demonstrate the application of the framework. The application of the framework will still be on a high level as presented use cases are still theoretical. However, the evaluation would give an idea that applying blockchain is better.

3.2.2. Benefits

3.2.2.1. What is the role of the blockchain in the target architecture?

Blockchain implementations typically have at least one of the following roles in the overall solution. Alternatives are incremental in functionality and value. The first one is the most straightforward choice, and it is the most replicable structure with conventional techniques. Therefore, it is the least value. While the last one is the most complicated, and if the business problem requires it, it is the most valuable. Every consecutive choice will build more features, and conventional techniques would gradually be inefficient to replicate the added value.

3.2.2.1.1. Blockchain is a shared information database

Blockchain technology implementations often are seen as a shared database [163]. Participants of the blockchain issue their transactions to the database. Moreover, the transactions are communicated to all participants to be formed into blocks and get persisted. All participants access the same records. There is a single version of the information.

3.2.2.1.2. Blockchain is a distributed information database

Each transaction, and then when transactions bundled, each created block is communicated to all participants, and each participant updates their copy of the database. This behavior is the same as a distributed database [164]. This behavior compares to a no-SQL document database where each block is a document with all the metadata as fields.

All participants have access to all records. Even if a participant is not online for a time frame, when this participant comes online, can download all missed blocks from other participants. A brand-new participant takes longer to catch up by downloading a larger number of blocks. Blockchain becomes distributed, replicated, and a single version of the truth.

3.2.2.1.3. Blockchain is a validated immutable transaction database

Even though there are multiple versions of the blocks in the time of creation, consensus eliminates the invalids, duplicates or misfit. Depending on the underlying digital assets, there can be specific business logic in the validation. There are also infrastructure requirements about signatures, encryption, and data format checking as part of validation. Validation and consensus make the data more secure, valid, relevant, and trusted. After the validation, each node appends

the new block to the chain. The blockchain is called an append-only database [165] since previously validated blocks in the blockchain are not updated with new transactions, simply the new states are appended as new transactions included in the new block.

3.2.2.1.4. Blockchain is an integration platform with a validated immutable transaction database

Participants of a blockchain network collaborate over the blockchain network by sharing information in the form of transactions. The seller, the buyer, banks, factory, the land transportation company, ports, shipping companies, the receiving port, customs, delivery company, and destination receiver all issue transactions for order, bank-letter-o-guarantee, production of an item, custodianship of the traveling item, customs documentation, receipt or arrival, and payment. Some participants may also benefit from these communications without actively issuing transactions. Insurance companies have a stake in the loss and damages. Government officials have governance interest on audit, taxation, and duty. Blockchain is an integration platform [166] for all these participants.

3.2.2.1.5. Blockchain is an immutable business process management database

Smart contracts add custom application capabilities to the blockchain. In business process management systems (BMPS), business process entities, and the business rules defined around them form a business process. The business rules control interactions and interactions create/update instances of the business process entities. A BPMS blockchain [167] contains entity instances with their metadata waiting for their next interaction.

3.2.2.1.6. Financial model reflection – Value of the solution

$$V_{area}\begin{pmatrix}\text{Role of the}\\ \text{blockchain}\\ \text{in the target}\\ \text{architecture}\end{pmatrix} = \sum_{i=1}^{5}(w_i * v_i)$$

$$i = \{shared\ database, distributed, validated, integration, BPM\}$$

Figure 11- Value statement of the role of the blockchain

After defining the purpose of the blockchain in the target architecture, its estimated value becomes an input to the financial model. Shared, distributed, and replicated databases have minimum incremental value as similar features can be obtained by implementing conventional database solutions. Validation of the transactions, immutability, having an integration platform,

and running business processes have more and more value. Advance roles in this scale usually include and goes with the less advanced ones. A validated immutable transaction database is assumed to be distributed, replicated, and shared. The formula adds a value of all the roles, but the value of each role should be calculated incrementally as the value is based on what it builds on top of the previous category of the role.

3.2.2.2. What are the desired features?

Literature [168] indicates that several features of blockchains can turn in to financial benefits. This paper list the main ones below to create a model that asks whether the desired solution needs these features. If a feature is needed, the overall financial model will include the monetary value of having this feature.

3.2.2.2.1. Enhanced monetary integration – smart contracts

A blockchain project can have integration with other blockchains. Most notable examples of this integration are when a business process blockchain is in integration with a digital asset such as cryptocurrencies [169]. This integration introduces automatic monetary settlements capability to business activities. There is no need for separate invoicing, itemization of invoices with business activities, double checking, payments related to order, settlements, and clearinghouse. There is no two different understanding of business events. There is no clearinghouse about them. No intermediaries to settle. No bank-to-bank transfer, No “Did you send?” “Did you receive?” "What happened to payment?" questions. Monetary integration minimizes payment risks. Instant settlements become possible and available.

3.2.2.2.2. Greater transparency

Transparency is the extent of openness and information sharing. For a corporation, it is the extent to which activities and information are observable by external entities. In conventional systems, the governing body decides the level of transparency. Each organization decides the set of sharable information for themselves, and the selection reflects what this company claims to be the truth. While there are many trustworthy corporations, names such as Enron, WorldCom, Bernie Madoff, and AIG would suggest that every claim cannot be trusted. Every corporation to be the trusted authority about its information is functional but not dependable.

Moreover, in the business ecosystem, there are multiple parties in each interaction. This multiplicity results in multiple versions of information. Whenever a conflict arises between parties, usually each party would claim that their version of the information is the truth [5] . Such conflict between otherwise trusting parties is expensive to solve, sometimes so expensive that conflicts can be avoided by merely accepting write-offs.

3.2.2.2.3. Enhanced security

If the control logic of a system is exposed and hacked, there can be system-wide damage limited to the system resources. Hackers took control of giant construction cranes [170] and showed that central controls mean a single point of attack. Attackers concentrate on this single point, and the protection of the resources forming this single point becomes too expensive or too restrictive. Blockchains are built on the distributed architecture where the loss or capture of a single resource is not threatening the greater system. The distributed architecture of blockchains makes DDOS attacks very infeasible. When a small number of the participants turn malicious, the rest of the blockchain has the power to cut them out of the system. Digital signatures and tamper resistance characteristics of the blockchain also make sure each block of the chain remains unchanged after its creation. Since there is no single point of attack and since the data corruption is not possible due to the digital signatures and tamper resistance, hackers do not have a chance to attack, update the data, or destroy any information.

Permissioned and private blockchains use a role-based security layer that restricts the operations to roles and data to privileged users on that specific data. Besides advantages of the distributed architecture, shared data, access security, role-based security and data security, blockchains can use no-knowledge-proofs to enable a level of encapsulation where business use cases require anonymity or pseudonymity.

3.2.2.2.4. Improved end-to-end traceability and assurance

Whether it is for export market requirements, product recall management or counterfeit prevention, traceability is essential for reducing risks [171]. Livestock, food, automobiles, and diamonds are known products with regulations, restrictions, and emergency management such as recalls. Their provenance is vital to avoid items with the uncertain origin and to prevent supporting any illegal entities.

Blockchains bring improved access to business information transparently and reliability. With blockchain's inclusive nature towards information sources, more and detailed information can be collected. All aspects of the business process can be traced end-to-end with the blockchain. With IoT sensors added to the information sources, details collected can fulfill assurance requirements for many businesses. Blockchains can answer the question: What really happened?

3.2.2.2.5. Increased process efficiencies and speed

Peer-to-peer communication is the building block of blockchain technology. Compared to layered systems with intermediaries and platforms that require clearinghouse style settlement activities, blockchains promote peer-to-peer interaction. Blockchain capabilities also enable granular handling of records. Businesses with blockchain infrastructures can avoid error-prone bulk operations where error handling is a challenge. Individual processing also enables healthy transactions to be processed much faster while unhealthy transactions suffer from their own issues.

3.2.2.2.6. Sharing economies

Sharing economy pioneers are disrupting businesses. Blockchain is the next version of sharing economies coming out for total disruption [172]. Ability to do peer-to-peer transactions is going to open more opportunity and benefits for masses. Sharing economies equipped with blockchain have significant advantages for large companies as well. Outsourcing well defined and distributed tasks remove the need for procuring, hiring, and allocating resources. These resources, such as personnel, comes with additional costs such as benefits, insurance, planning, management, and payroll. Changes can further disrupt these complicated systems and replace the intermediary authorities with the help of blockchain technology.

3.2.2.2.7. Financial model reflection – Value of the features

$$V_{area}\begin{pmatrix} Desired\ features\ that \\ blockchain\ implementation \\ brings \end{pmatrix} = \sum_{i=1}^{6} (w_i * v_i)$$

$$i = \begin{Bmatrix} monetary\ integration, transparency, security, \\ traceability, efficiency, sharing\ economies \end{Bmatrix}$$

Figure 12- Value statement of the desired features of the blockchain

These features are possible to obtain with blockchain implementation. Each feature's corresponding value would be estimated financially based on the use case. Assigning a value to some of these features is harder for some than others. For example, the value of transparency tends to be recognized under other subjects such as reduced conflicts. Some features may not be usable for the target business use case. For example, traceability may apply to identifiable assets more than commodities. Valuation of efficiency, speed, and security is possible with comparisons with alternative solutions. Monetary integration may not be implemented immediately when the project starts. There may be proper cryptocurrency or other financial instruments at the time of blockchain establishment. However, the ability to implement the integration in the future is valuable as well. Smart contracts and cryptocurrencies enable a type of business process integration that is hard to achieve by conventional means. Above all other features, sharing economies is a mega feature that gives businesses an Uber like reach towards involving partners, allocating resources, and tracing operations.

3.2.3. Costs

3.2.3.1. Which costs does blockchain reduce?

Benefits also come in the form of cost reductions. This paper lists the potential cost reductions that organizations can benefit from. Evaluation of each cost reduction opportunity and estimation of the monetary value creates an input to the financial model.

3.2.3.1.1. Removal of the intermediaries

Systems integration, especially on the international level, is full of intermediaries. For example, the Swift system is an intermediary for more than 10000 institutions in more than 200 countries. Operations in this system depends on the mediators called correspondent banks, as well as the swift system. The intermediaries increment fees. It takes several workdays to complete the transfer with minimum transparency of where the money is at a specific moment. Technologies that intermediaries require can also be proprietary. Each member organization takes on technology implementation cost of technologies that the Swift system requires. There are operational costs, such as transaction fees. Commissions and fees build up as there are more hops in the transfer. Similar cases of intermediaries and related costs exists in supply chain industry where geographically distributed companies conduct business without common standards. The lack of

common languages and standards creates a gap in processes and are occasionally filled by third party intermediary companies [173].

3.2.3.1.2. Streamlining clearinghouse structures and settlement processes

Clearinghouse structures take part in both sides of the trade. Stock trade is a simple example where stock exchange clearinghouse processes deliver money to the seller and stocks to the buyer by receiving it from the other party. Clearinghouses resolve conflicts and simplify the complexity of the market for the participants. Stocks, commodities, and bonds markets may seem simple at their straightforward trading, but each market has their complexities such as options, futures, and derivatives. While their service is valuable for their industry, clearinghouse structures and settlement processes are obvious targets of the new age of disruption.

Peer-to-peer versions of the same businesses are more flexible, innovative, and independent. Since peer-to-peer implementations avoid clearinghouses and intermediaries, these processes save from commissions that intermediaries charge for the provided trust and settlement processes.

3.2.3.1.3. Reducing settlement time and the time value of money

The time gap between the delivery of goods/services and the issuance of the payment is a risk. Reducing settlement time can reduce the risk. With instant payments, there can be more confidence and willingness for trade. Money in-transit also means cost as there is time-value of the money. For one trade this cost can be negligible, but considering the volume of trades, the lost time-value of money is significant. Instant settlements both help organizations on the cash flow, and reduce loan interests paid as a result of delayed income.

3.2.3.1.4. Removing obstacles such as missing documentation

Multiple participants in the business process usually mean multiple inputs, multiple hops, and chain of events as well as incremental information. International shipping of goods needs at least eight pieces of documentation [174]. This requirement means eight pieces of documents that need to be validated, protected, and verified. It also means multiple chances that a document will be missing, and the shipment will stall. Each delay is lost time and money. Perishable goods have even higher risks and preservation costs. Corporations can estimate these costs as they are usually apparent as a loss even when they are not traceable in detail

3.2.3.1.5. Removing the burden of proof

For business processes that lack single authority or for simple interactions that were designed to be based on trust, at the time of conflict, there is a cost for collecting proof and finding the truth. Most processes continue smooth and optimized when everything happens as expected, and no extraordinary events occur. However, when things go as unexpected, it is hard to know what exactly happened. Authorities who typically control the flow of information are considered to be trustable. Parties use their records as proof when things are unrolling as planned. However, if an authority is responsible for the delay, damage, mishandling, and harm, then the authority's records lose reliability. Blockchains add significant value by carrying an immutable ledger and providing proof of the series of events.

3.2.3.1.6. Reduction of insurance rates

Insurance companies are stakeholders for almost the majority of actions and activity in the western world [6]. Insurance companies suffer from the inefficient exchange of information, inefficient risk profiling, fraud, and manual processing. Organizations that carry their business on the blockchain-based solutions can negotiate better rates as the risk of fraud is less, exchange of information is efficient, fraud detection is easy, liabilities are explicit, data sources are united, and processes are reasonably automated. [175]

3.2.3.1.7. Financial model reflection – Value of the cost savings

$$V_{area}\begin{pmatrix}\text{Costs that}\\ \text{blockchain}\\ \text{reduce}\\ \text{or remove}\end{pmatrix} = \sum_{i=1}^{6}(w_i * v_i)$$

$$i = \begin{Bmatrix} middleman, settlement, lost\ TVM, \\ obstacles - missing\ docs, evidence\ collection, insurance \end{Bmatrix}$$

Figure 13- Value statement of the costs reduced or removed by the blockchain

Which of these costs apply to the business, and whether they are reduced or removed in the blockchain solution needs to be identified and accounted for in the financial model? These details depend on the nature of the business.

3.2.3.2. What are other factors and the motivation for implementing a solution?

There are some other factors which are the custom realities of the organization or the solution. Blockchain value estimation must consider the answers to these questions such as whether there are existing systems to be replaced, whether the human resources are ready for the technology, whether the laws and regulations are for or against the blockchain-based solution, and whether the industry members sharing a motivation are essential drivers and parameters.

3.2.3.2.1. Existing systems in place.

If there is a system in place for the business, there will be additional costs for system replacement. Migration of old records to the new blockchain solution, migration of participants to the new integration points, potentially running both systems side-by-side for a period and decommissioning old systems are typical costs.

3.2.3.2.2. Uncomplying partners

There is a risk that some collaborating parties would not or cannot integrate with the blockchain solution. Developing adaptors for these parties will eliminate the risk but introduces more development, testing, and operational costs.

3.2.3.2.3. The pain of change - Starting a new business on a new technology

If the blockchain-based business model is new for the corporation, there is a risk that the design of the new solution on the blockchain model will have incompatibilities. It will need iterative processes, multiple implementations, and improvements before the system to work at its ideal performance.

Corporations also should not underestimate the impact of transparency on their people. Having all activities on the transparent and permanent database may make the workforce feel getting on more liabilities. Transparency makes people obey the rules and avoid acting outside of them even if there is a benefit for the customer with a small bend of the rules. This inflexibility may be for or against the business model, especially from customer satisfaction and exception handling angles.

3.2.3.2.4. Compliance with laws and regulation.

If there are regulations that blockchain solution can comply more efficiently, it would be a great motivation for using the technology. For example, if the Canada Deposit Insurance Corporation (CDIC) would require the financial institutions to integrate into a blockchain system to collaborate and communicate, not complying may result in penalties.

3.2.3.2.5. Industry trends

If an industry is migrating to a blockchain solution for collaboration between the member businesses, there would be extra motivation with added benefits on standardization. If all banks are sharing customer information on a blockchain, every bank will try to join for providing the potential advantages to their clients.

3.2.3.2.6. Financial model reflection – Other factors

$$V_{area}\ (\text{Other factors}) = \sum_{i=1}^{5} (w_i * v_i)$$

$$i = \begin{Bmatrix} Legacy\ systems, uncomplying\ partners, pain\ of\ change, \\ laws\ and\ regulations, industry\ trends \end{Bmatrix}$$

Figure 14- Value statement of other factors

These factors are the most challenging to quantify. If there are legacy systems, or if business partners are not willing to join a blockchain solution or company human resources are feeling blockchain as a threat, there would be resistance and costs. There can be a veto or resistance against these new principles introduced by the blockchain technology. Laws, regulations, or industry trends towards blockchain would be positive motivation and increased perceived value.

3.2.3.3. What is the cost of implementing or operating a blockchain solution?

Previous sections in this paper list the fundamental motivations, related benefits, and costs as the perceived values for the benefits and estimated cost reductions are significant drivers for change. This section will detail the cost of procuring the blockchain solution and listing the operating expenses.

3.2.3.3.1. Public vs. permissioned/private blockchains

Public blockchains allow any participant to join the blockchain and take part in the block creation and consensus. Since the participants are not authenticated and limited, there is an open and limitless race to create the new block. In order to have only one winner of this race, there are consensus mechanisms that blockchain networks employ. Proof of Work (PoW) is the most well-known mechanism that forces the block creator to solve a cryptographic puzzle before broadcasting the new block. Bitcoin cryptocurrency uses this mechanism, and it is infamous for the amount of wasted energy. Some would argue that as long as the overall system is healthy, energy lost in the competition is not a waste. Others are especially worried if one blockchain can lose an amount of energy as high as the consumption of a developed nation, what would be the consumption if there would be a lot more public blockchains. Proof of Stake (PoS) is another mechanism that distributes the responsibilities of block creation with the weight of the stake one has in the system assuming that more stake one holds, more it would protect the system. PoS and other lower energy consuming mechanisms are emerging. PoW is still the most reliable mechanism, and most valuable public blockchains use it.

Public blockchains with PoW requires much processing power and energy for infrastructure to support that processing. If one decides to join such blockchains and take an active role such as block creation, it will require extensive computing infrastructure and will be reflected in the electricity bill as well. If a participant is only interested in issuing transactions, even if the public blockchain is using PoW, this participant does not need to do mining. There would be other mining nodes doing mining for the incentives.

3.2.3.3.2. Cost of participating in a blockchain

There is no strict definition of being a part of a blockchain. Also depending on the blockchain type and volume of transactions, requirements would change. Assuming the target project already has the remaining infrastructure, blockchain related additional infrastructure is limited to becoming a full node. A full node has and receives all the transactions and blocks. It is possible to refer to the Bitcoin network for estimation of the cost and estimate on the similarity to infrastructure requirements of bitcoin full-nodes [176]. These requirements are a desktop or laptop with an updated version of its operating system, 200GB free disk space, 2GB RAM, and faster than 50KB internet connection. These are relatively simple requirements that are possible to

procure at less than $1000. There are several resources where the cost of running a full node is reported to be less than $100/month [177].

Permissioned blockchains are implementations where at least the fundamental operations on the blockchain are restricted to some authenticated participants. If participation is completely restricted, they are also called private blockchains. Authenticating clients for blockchain access also enables authorization and allows assigning different roles to participants in the blockchain ecosystem. One of the most critical roles is the block creator. This vital role can be restricted to the more trusted parties in the blockchain. Cost of running a permissioned blockchain is low. Amazon web services have some pricing for the hosted blockchain services. The prices from this vendor can be a benchmark where there is no other infrastructure cost. For a HyperLedger blockchain, the price of running two nodes is estimated to be less than $2/hour for a production network. Procuring a test network costs approximately 30% of the price of a production network.

These costs of a simple infrastructure based on commodity hardware can be considered low compared to expenses in most projects where the scope includes a complete standalone infrastructure. Blockchain software can run on various platforms. Therefore, hosting decisions are mainly related to the infrastructure policies of organizations. If policies direct running the blockchain software on specific infrastructure such as on legacy platforms like mainframes, there would be a much higher entry cost for the project.

3.2.3.3.3. Do you need new hardware?

Whether the infrastructure of an organization consists of a mainframe or a network of servers, it can run blockchain applications on the existing infrastructure. Base applications are not resource-intensive. Contrary to what is reflected in some resources [178], cryptographic requirements involved in being a blockchain node (not a miner) is not new and is not more than previous systems with security layers such as two-way-SSL and digital signatures in SAML assertions. The volume of the inpouring data is determinant for storage space. Depending on what blockchain contribute to the solution, all the records can be accessible all the time or space can be saved by pruning the old states of each asset that is updated with newer versions of information and state added to the chain.

3.2.3.3.4. Financial model reflection – Cost of implementation and operations

$$V_{area}\ (\text{Other factors}) = \sum_{i=1}^{3} (w_i * v_i)$$

$$i = \begin{Bmatrix} Public\ blockchain\ participation\ and\ PoW, \\ private\ blockchain\ participation, hardware \end{Bmatrix}$$

Figure 15- Value statement of implementation and operational costs

Implementation and operation costs are most quantifiable items in the financial model. They are highly related to the nonfunctional requirements such as the volume of data, designed scalability, number of transactions, and number of nodes per participant. Whether mining activity is necessary or not is the most significant factor, as discussed above.

3.2.4. Financial Model

Below is the general financial model that is a combination of all the factors listed above. The process of evaluation starts with identifying whether these factors apply to the target business process. Some solutions may not apply to all businesses. Deciding whether features are relevant and whether listed cost savings are applicable would draw the financial scope of the solution.

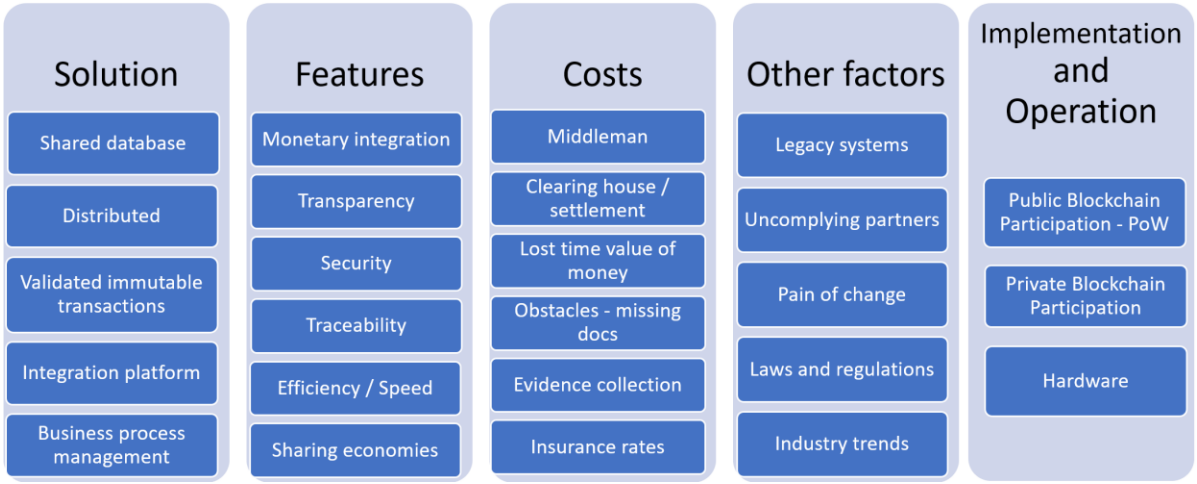


Figure 16- Consolidated financial model chart

3.2.4.1. Details of the financial model

Even though the groups are created by bundling similar subjects based on how they factor in overall finance of the solution, some items may have an adverse behavior. For example, if the

provided transparency requires further data protection measures, the cost can be reflected as a negative value on that item.

In this model, colors are used to mark the factors. Blue is the neutral color. Neutral factors are factors that do not have a significant benefit. When a factor is significant positive value on the favor of the blockchain solution, green color marks it. Red color marks negative factors.

There are multiple ways to conclude the evaluation. Initial assessment would be over the benefits vs. costs. If the green colors are dominant on the presentation, it is a positive sign for blockchain utilization in the solution. Rare cases of green factors would mean limited benefits. Similarly, a red-dominated model would mean there are several costs and should be recognized as a mismatch or as a warning on the bottom line.

After this identification of significant factors and color identification of their impact, quantification of each item and cumulation of the results should follow. Quantification can continue with the estimation of value, cost, risk, or opportunity. Sum of all values for all factors should provide overall value to consider the result of the financial model.

3.2.4.2. Use case - High volume package delivery

Our use case to demonstrate our financial evaluation framework is the high-volume package delivery. In this use case, we are evaluating the blockchain technology implementation in a package delivery business. This use case assumes the company is targeting to grow their business and reduce costs.

The assessment starts with a review of each framework factor and identifying whether it is a positive, negative, or neutral factor. The next step is to quantify the non-neutral items, and the cumulative numbers would suggest whether this solution is a “better” solution.

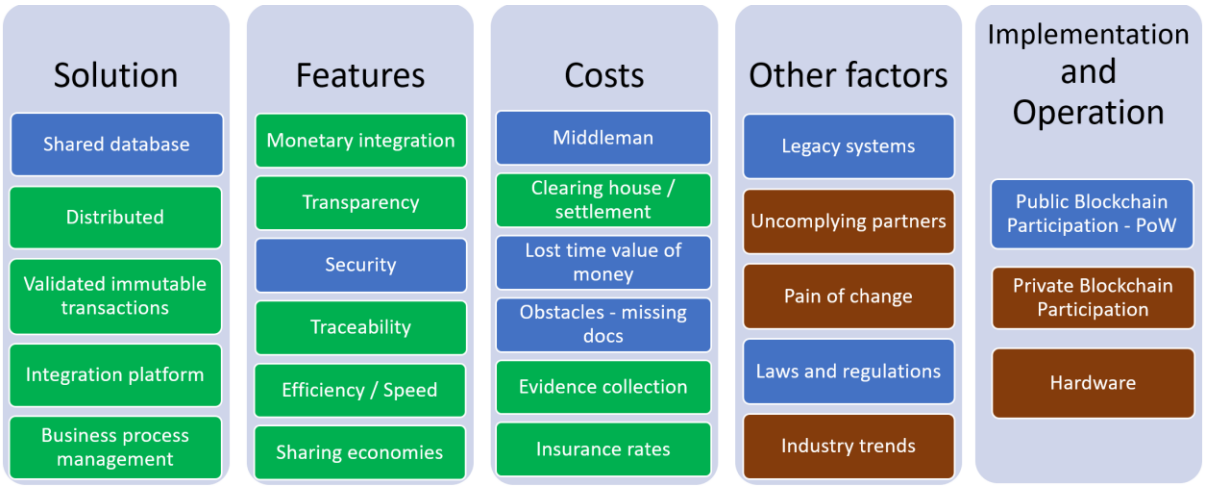


Figure 17- Consolidated financial model chart for high volume package delivery

In this use case, the entire delivery resource network as well as other stakeholder business entities will share the blockchain platform. The distributed architecture of blockchains will bring the advantage of high availability. Any node in the network, including the nodes that represent the most significant business entities, is not a single point of failure. The system will continue functioning even if some nodes are down. Blockchain is a validated immutable transaction platform for this use case that will collect the sensor information in order to mark status and delivery events in each delivery task. It will also be an integration platform between the parent company and other contributors such as sub-contractors. Each contributor can run their part of the business processes on the blockchain while the standard processes that can benefit all will also reside on the blockchain.

Monetary integration adds payments processing capability as part of the business transactions. Compensation of workforce and sub-contractors will be processed in real time within the blockchain transactions. This model would work with cryptocurrencies perfectly however when it is not possible to use digital money, fiat currency payments can be recorded in this system. This would bring traceability to the payment. This blockchain solution can be a gateway to sharing economies on parcel distribution business where people who has access capacity help with individual tasks. Students in their free time can deliver parcels and get an instant compensation for their help. With the transparency and traceability that blockchain technology provides, the involvement of external parties can be traced by themselves and by the business process owners. There will be several ways to collect data, and with the evidence quality immutable transactions of the blockchain, finding proof will no longer be a burden. Peer-to-peer interactions would

increase efficiencies. Newly introduced parallelism with shared economies can deliver the packages in much improved average end-to-end timelines.

Current practice of collecting mission data and bulk data uploads of the events in to the system would be eliminated. Blockchain solution is superior as at any time it will serve the latest state of tasks. In case there is a dispute, blockchain will have an undeniable trail of evidence. If more participants are added to the blockchain such as the IoT devices at homes and perhaps homeowners' mobile devices, there would be even more events and evidence of delivery. Since the sensor data is recorded as well as all delivery events including the chain of custody, when disputes happen, the blockchain would provide enough information to analyze and detect the responsible entities. The risks in loss and damage are expected to fall or would be precisely identified, which may result in reduced insurance premiums.

There are some obstacles to the implementation as well. Blockchain implementations, in general, suffer from not reaching the tipping point on the acceptance. If the partners and subcontractors of the delivery business do not accept the idea and do not comply with the new rules, there can be an adverse effect and perhaps loss of partners. The delivery personnel may also be negative on the extreme traceability idea as they are the ones being closely monitored. Their mistakes would be exposed quickly. Industry trends currently are favoring the monopolies and closed systems for the delivery companies due to economies of scale and privacy aspects of business. Openness and collaboration that blockchain brings may not be the industry direction in short term. However, industry may change with foreseen value.

A private blockchain infrastructure would be created for this solution. Even though the cost of private blockchains is less than public blockchains, there would be an initial cost that need calculation. Technical unknowns such as how IoT devices would be connected to the blockchain require more research.

Without the details of the business environment and quantification of the values, we can only comment on the estimated importance and value of the factors. We believe the number of green factors indicate the excellent opportunity to apply new techniques and improve the business. There are several benefits listed with many cost-cutting opportunities. The strategic benefits of the sharing economies and traceability are far higher than the cost of implementation. Operational

benefits of distributed systems such as high availability despite the loss of some significant systems are also invaluable.

3.2.5. Conclusion

Blockchain technology had been a popular subject. Despite numerous ideas, use cases and research in the literature, financial aspects of blockchain implementations had not been analyzed methodically.

In order to assess the soundness of a blockchain project, stakeholders should evaluate the benefits and costs. Benefits are due to the role of the blockchain in the solution and the features that blockchain introduces. Costs are either reduced expenses as a result of addition of blockchain to the ecosystem or other costs that are created due to addition of blockchain. Every blockchain project would incur implementation and operational costs as well.

In this paper, we provide a novel framework that evaluates different aspects of a blockchain project. Our framework results in a set of formulations that will detail the overall financial model. Since the value of each detail depends on the project details, it is not possible to calculate a resulting monetary amount. However, following the framework, the evaluator will find enough guidance to accomplish the assessment task while covering all aspects of cost/value brought by the implementation. We also demonstrated this by applying the framework on high volume package delivery use case.

Next steps in our research include automation of this framework. This automation will enable us in applying and testing the framework with a wide variety of real-world use cases. Our research group is currently working towards creating a questionnaire that will collect the necessary data. We will proceed with further validation of the framework and enhancement with the data collected from use cases. The cost information collected from real life projects will give us more idea about the weights of the factors which is currently not differentiated. Business value of the blockchain benefits are also to be evaluated statistically after related information is collected. These statistical analysis of the costs and benefits would also inform us about the importance of the factors with a comparison of financial impact of factors with business value of each blockchain benefit.

3.3. Automation and Security with Smart Contracts

After creating a solution with BTTF and validating the financial feasibility of our solution with our financial viability framework, in this section, we are focusing on the automation and security aspects of our solution. BTTF indicated that blockchain technology solutions could support applications by automating the interactions between participants in a single atomic transaction using smart contracts. While this automation adds several advantages, our research indicated that smart contracts have security issues. We surveyed these issues, categorized them, and indicated the risks introduced by these issues in blockchain implementations. This work provides insights and answers the key questions on automation of the aid delivery operations on a blockchain. The findings also greatly influenced our choices in the subject of blockchain security.

3.3.1. Introduction

A new era of trust-based applications is emerging with the invention of blockchain technology. Nakamoto showcased an application of currency ownership and transfer application [52]. Bitcoin was the first known application of the technology. With the success of the bitcoin as a sustaining monetary platform, blockchain technology got the recognition to become a technology suitable for general implementation.

Blockchain technology is a software implementation of a distributed ledger concept. Blockchains record each transaction into the ledger with the order of occurrence. Blockchains group the recorded transactions to blocks. Cryptographic hashing function of the blockchain seals each block by calculating a hash value. A blockchain application records the hash of each previous block into the newly created next block in order to cascade the tamper-evident effect of chaining through hash values. At any point, any block in the chain can be verified by rehashing the block and comparing this value with the hash previously recorded in the next block. This basic technique of chaining through hash values prevents tampering by making it detectable and verifiable.

Smart contracts [179] are programs that represent business processes (Figure 18). They are serializable replicated bundles of code and state objects designed to be a part of blockchains. As participants add smart contracts to the blockchain, similar to other ledger transactions, a new block in the chain includes these smart contracts. Each transaction that updates the smart contract state also goes into the next block created after the changes. Each participant of the network receives a replica through the block distribution mechanism. Chaining of the blocks makes smart contracts immutable like other transactions.

After the contract is on the chain, participants can interact with the contract by calling its methods. This newly added contract can call other contracts on the chain with their defined methods. A contract also becomes a participant in the chain, which means it can also have transactions such as sending, receiving and owning digital assets.

In this research, we focus on the Solidity [180] programming language and Ethereum [181] blockchain. Smart contracts are a strategic opportunity for Ethereum. Ethereum is positioning itself as the internet of the future. It needs reliability in its smart contract frameworks. In order to provide the required reliability and to address the customizations required to make the blockchain abler, Ethereum community promotes the correct execution of the smart contracts without vulnerabilities.

```
Get ($5) from (Customer)
When Event (Pizza boy delivered)
        Give ($4) to PizzaCompany
        Give ($1) to PizzaBoy
If deliveryTime>requestTime + 30 min
        Return ($4) to Customer
        Give ($1) to PizzaBoy
If no delivery in 60 min
        Return ($5) to Customer
```

Figure 18- A pizza-order smart contract code (Pseudo)

Ethereum network has a compensation plan for the processing power dedicated to operating the smart contract applications. In the Ethereum network, participants register their contracts or participants call a method of a contract. Each of these operations can be done with the

fee attached to it. The fee is called gas and how much gas needed for a smart contract operation depends on the instructions involved in the operation or program execution. The caller specifies the amount while triggering the operation. Each miner would recognize this amount as a budget to run the program one command at a time. Miners spend some of the budgeted gas for each command they execute until all the gas is consumed. If the budget provided exceeds the execution cost, participant initiated this operation will receive the refund of the excess amount. If the execution cost reaches the provided amount in the contract operation before the end of the execution, the state of the contract would be rolled back. Miners do not return the consumed gas. Miners would keep the fee while contract would be unsuccessful. Pricing of the gas is a complicated process, but for the sake of focusing on the vulnerabilities, we will not go into the details of pricing.

Security smells are clues that point to a deeper problem in the programming space. The root cause of the smell may have an impact on the availability, integrity, and confidentiality aspects of the information security. With adequate guidance, even inexperienced eyes can spot some of these risks for information security. Despite their easy recognition, due to the dearth of targeted studies informing developers, security smells are not handled properly. There are multiple studies on security smells for various software platforms [182]. This research aims to be a pioneer study in blockchain technology regarding security smells.

To sum up, our aim is spreading knowledge and awareness for preventing security issues for smart contracts. Our contribution is a novel categorization of security smells. We reviewed 28 security smells. We classified those security smells according to the context they were identified at: security smells in the smart contract's execution environment, design, or coding. We inform the reader to recognize security smells and identify their occurrence in order to produce better smart contracts.

The rest of this paper is structured as follows. The next section is our literature review on the tools previously developed. We also list some of the previous incidents to establish the level of impact and importance of this research. We provide information on smart contract interactions in order to understand the related issues better. Section 3 introduces security smells in the categories we defined, explains them and describes how to identify them. Section 4 details the future direction of this research.

3.3.2. Motivation

In this research, we focus on the security vulnerabilities of Solidity language and Ethereum blockchain network. In particular, we try to answer the following specific questions:

- What are the known patterns of security issues?
- What are the categories of these issues?
- How can we identify them?
- How can we prevent them?

These questions are important for two main reasons. First, most Ethereum smart contracts deal with money. When a smart contract carrying money has an issue, there is a chance that the money in the contract can freeze. There may not be any way to transfer that money out of the contract. Locked money is mostly a consequence of a vulnerability. Parity wallet is a famous example of an exploited vulnerability that froze millions of dollars' worth of ethers in a contract [183]. In order to save the money, significant participants of Ethereum suggested a controversial manipulation in the network. Creating a new version of the chain, also called as a hard fork, is the only known way to correct this mistake. This issue could have been prevented by secure programming practices [184] [185].

Reputation risk is the second reason for this study. The expectation from smart contracts is high. For the blockchain world to create a trust-based business process management, it is essential that the smart contracts work flawlessly. Vulnerabilities listed and explained in this paper have to be avoided and prevented in order for new participants to adopt blockchain-based businesses. Blockchain does not have to be a risk that businesses take, so we need to work towards creating better systems.

Immutability of the blockchains makes sure the issues are accessible forever. This unforgiving historical record is another reason that the analysis of programs and detecting whether these security smells exist in the code must be a fundamental part of smart contract acceptance. The reputation of the blockchain companies is dependent on the quality products and services they provide. When the subject is smart contracts, it is vital to make the right move at the first try.

We conducted this research as an addition to the existing knowledge base of smells in other programming environments since there is a difference between classical programming and

blockchain contracts programming. There is a lack of trust and a significant conflict of interest between who creates, who calls and who executes smart contract applications. Once the creator of a smart contract deploys the contract to the blockchain, there is no way to modify it. The inability to modify means there is no way to fix the bugs that were in the new contract after the creation. Vulnerabilities risk money as smart contracts are mostly about money and the exploitation of vulnerabilities result in loss of money. An innocent issue such as a mistyped variable can become a vulnerability to trap real money in production. Finally, hackers can read the smart contract code, understand the logic, find vulnerabilities and exploit them. If there is a vulnerability, they can do what it takes to take advantage of it behind the anonymity of public blockchains.

We carefully collected the reports on vulnerabilities from limited sources available on the internet. We categorized them in order to increase awareness on their impact and root cause. With this categorization, we can understand the threat. We can also create solutions that would target a set of issues possibly towards fixing the root cause instead of one vulnerability at a time.

Our first category is the dependence on the environment. This category brought out the conflicts between the nature of distributed applications and implementations. Such smells are an indicator of the misfits as smart contracts. The second category is mainly design and packing/deployment issues. If the application is designed to have an ever-growing collection that will impact the overall performance, this is a smell for an improper design. Library dependencies, versions, and languages used are all part of the design and packaging. Trust-based interaction with another blockchain hosted entity is the next category as it is transferring the control of execution to the trusted entity. These smells lead us mostly to availability issues. The following category is external interaction or dependencies that impact the integrity of the contract operations. The last category is similar to coding smells that induce a variety of integrity issues in the smart contract.

3.3.2.1. State of the body of knowledge

Analysis tools flag 45 percent of existing contracts as vulnerable [186]. This high percentage of vulnerable elements on a cryptocurrency blockchain also indicate why we need to learn and spread the knowledge on vulnerabilities with hopes of preventing malicious activities. Currently, developers are resorting to already existing research on smart contract vulnerabilities. This work is highly scattered, and not organized. There are websites, Ethereum documentation, research papers, and forums containing bits of information on vulnerabilities. The number of

information resources is not low. However, the level of details is insufficient to have a good understanding of the issues. The majority of resources provide high-level descriptions instead of details and use cases. There is a lack of proper categorization of security smells, which leads to confusion.

There are ways to identify and prevent vulnerabilities. The most common among those are making sure issues and solutions are documented, fuzzing the inputs to make sure vulnerability does not exist, mutating the contracts to make sure prevention is sufficient for the test cases and replicating the tests from similar contracts in the same blockchain [187]..

Research indicates the need for blockchain oriented software engineering in order to understand vulnerabilities and to promote safe programming practices [184].

Oyente [186] framework is a python based static analysis tool to detect some of the vulnerabilities. It groups the vulnerabilities into the following categories: transaction-ordering dependent, mishandled exceptions, timestamp dependence, and re-entrance handling. The Oyente tool classifies contracts with these categories, and a related paper [186] evaluates the tool accordingly.

Contract Fuzzer uses the fuzzing technique in order to identify vulnerabilities in smart contracts [185]. Contract Fuzzer starts with an analysis of the interfaces that the smart contract exposes. It generates fuzzing inputs for these interfaces and analyses the execution logs of the application in order to detect vulnerabilities.

Securify [188] is a pattern-based verifier that classifies contracts using two pattern categories: compliance patterns and violation patterns. When a smart contract is under the scope, Securify collects the patterns from the smart contract and compares it with the two categories of patterns that it has. Securify represents contracts in its domain specific language and evaluate them with the patterns.

Smartcheck [189] is another pattern-based analysis tool that transforms the smart contract code into XML representation. It uses XPath to check every contract to identify if patterns are present.

The common issues to all the research articles we reviewed and the existing tools we could find are related to accuracy. Most studies indicate that they are suffering from high levels of

precision and recall. Our research will help understand why detecting the vulnerabilities is a difficult task. Since the smart contract business scenarios are very different from those of conventional programs, it is not easy for current tools to identify which part of the code was developed on purpose and which parts are the results of mistakes. Some tools also include manual steps to compare and eliminate the list of vulnerabilities [188].

3.3.2.2. Attacks: motivation and significance

Most popular blockchains are modeling a paradigm called cryptocurrency or digital coins. Cryptocurrencies are digital assets that these blockchains manage. Participants issue transactions on the native digital coin of the blockchain and typically change ownership of the digital coins as part of the business they are conducting. Most digital coins are convertible to government-issued currencies. Therefore, these platforms managing the ownership of currency are the target of hackers with financial gains in mind.

Traditionally there have been two type of attacks on the popular blockchain systems. The first type is a hacker who attacks the blockchain network directly. This type of attack mainly aims to take down the blockchain network, disabling it or taking it over. Other types of attacks aim to steal valuable assets or to damage the integrity of the system through issuing invalid transactions. Malicious entities carried both types of attacks to popular cryptocurrency blockchains. Smart contracts related attacks are mainly in the second category. A smart contact related incident is a result of deployment and execution of a smart contact that contains vulnerabilities [187].

Researchers created a database of security incidents in the blockchain space. Smart contracts related incidents have a significant share of 22 percent in this database [187]. This set of issues is what participants can avoid with secure programming practices.

3.3.2.3. Smart contract lifecycle

Blockchain networks define the lifecycle of smart contracts in detail (Figure 19). After the development of a new contract, the creator (sender) of the contract adds it to the blockchain network. With this transaction, the contract becomes part of the chain. Each contract has an address deterministically calculated from the address of the sender, and this address identifies the contract. Participants use this address as a handle to the contract object for any consecutive interactions. Each interaction is a transaction, and the subsequently created blocks of the blockchain persist

these transactions. Participants can send money to a contract. They can also execute a method of a contract by issuing a call. Both interactions can happen repetitively, and any participant can initiate them. Sending money is a common use case where participants use the contracts to store funds temporarily. Bidding contracts or investment contracts are some examples (Figure 20) of such contracts. Contracts, as part of their flow, can send/return money to any participant or other contracts. Besides the methods that handle funds, developers of a contract can code any methods into the contract program during development. Typically, the business logic that the contract handles resides in these methods. These methods of the contract can access the state information of the contract and use it as a data store. Finally, the business logic handles the final step in the contract's lifecycle where the contract goes for termination when it is no longer needed. This process typically returns the remaining funds to their final destination and marks the contract as inactive.

Figure 19- The lifecycle of a smart contract

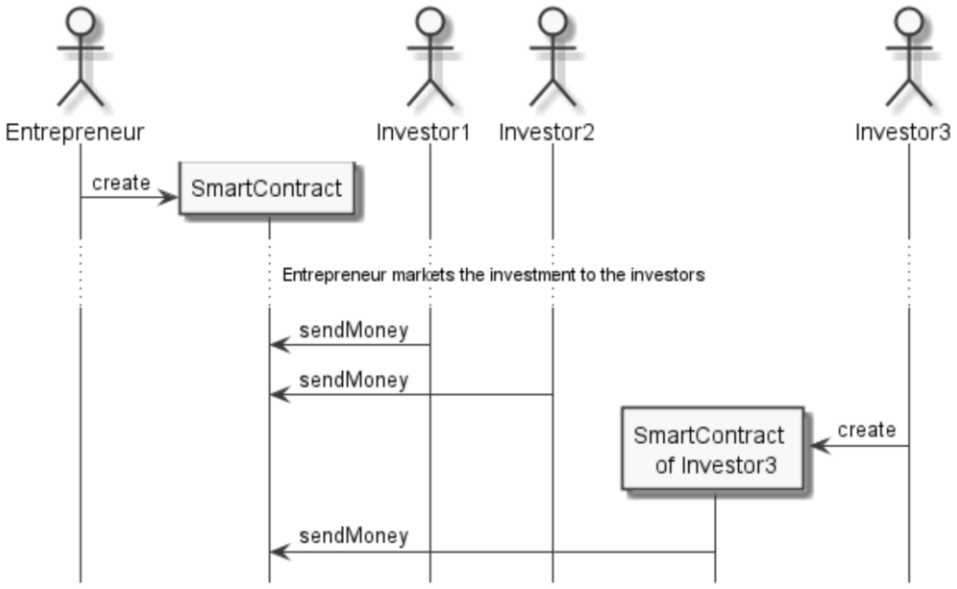


Figure 20- Sample investment smart contract sequence diagram)

3.3.3. Security Smells

3.3.3.1. Dependence on the environment

3.3.3.1.1. Transaction ordering dependency

A smart contract can receive several calls that may end up in the same block of the chain (Figure 21). Considering the business logic that the contract has and the audience that it is serving, this number can be high. Developers must design each contract to be deterministic despite an unknown order and number of interactions. In the timeline of events and with the series of blocks, regardless of the order, the result should be the same. Otherwise, a miner can add the transactions into the block planning to take advantage of the order dependency [186].This aspect of the contract execution makes it vulnerable for miner attacks. This vulnerability is expected to be exploited in an environment where each actor is trying to maximize his benefit. If the contract has this vulnerability, before the new block includes the interaction as a transaction, it gives an opportunity to the miners to use this knowledge to their advantage. If the business case for this contract involves interactions in a competitive nature such as a bid or offer, the miner can have a clear advantage to reorder transactions or to make a competitive bid [190]. Another use case can be one involving a digital asset whose price change with demand. There could be an unfair advantage based on the order of the transactions [188].

Pattern analysis can detect this vulnerability. However, due to the business nature of the contract, there is significant difficulty in distinguishing whether the occurrence is a vulnerability, or it is part of the design.

Figure 21- Blockchains do not have to include the transactions in any specific order

3.3.3.1.2. Timestamp dependence

The timestamp of the host environment can be used by the keyword “now”. Since miners manage the host environment, environment variables such as timestamp cannot be used safely

[185]. Static code analysis can detect this vulnerability by searching the keyword “now” [190]. Developers may try other ways to check the time. The number of blocks since the creation of a contract may give an idea about the time elapsed. If developers are using such methods in their code, pattern analysis can identify the occurrences.

3.3.3.1.3. Using block-hash as a random number

Supplying random numbers to a smart contract is not easy [191] especially considering that all the significant nodes of the blockchain network will run the same contract. Randomizing the business outcome and the deterministic nature of contracts conflict in this respect. Some contracts use the block-hash value as a random number [190]. The block-hash and random numbers can be a vulnerability in an environment that the code of the contract is to be executed by miners and the outcome can have a conflict of interest. Currently, it seems not feasible for a miner to define a block-hash maliciously. However, if the stakes are high, consensus mechanisms can pick a candidate block from one miner vs. another where the set of transactions are different and consequently block-hashes are different. Static analysis can identify usage of block-hash and random numbers.

3.3.3.2. Design and deployment issues

3.3.3.2.1. Gas limit and loops

Participants pay a fee for Ethereum nodes to execute their contract-related calls and for broadcasting the block that includes the resulting state of the executed contract. This price is called “gas”. It is an upfront fee to be allocated while registering a contract with the Ethereum network.

If the gas reserved for the contract is not enough for the execution of the contract, the contract state would be rolled back [192]. This rollback would consume the allocated gas. There would not be a return to the owner. This scenario can be prevented by adequate calculations or by preventing operations that may not have deterministic steps. For instance, all loops included in the contract must have a limited number of iterations. If the developer cannot calculate the number of iterations, adequately calculating the amount of gas needed will not be possible, either.

The gas limit is not only an issue about the contract that contains the loop, but also an issue for the contracts that may call other loop containing contracts.

3.3.3.2.2. Malicious libraries

A contract can reuse a library code by calling the library contracts with a particular call, named delegate call. This call creates a vulnerability by letting the library access the state and attributes of the contract. Having arguments such as "msg.data"' lets the caller craft further behavior for the victim contact to implement [185].

It is relatively easy to detect usage of external libraries with keyword match - however, the specific vulnerabilities introduced by external libraries are generally hard to detect [189]. Some tools prefer to create false positives with the keyword "library" due to the significant risk that libraries present.

3.3.3.2.3. Using inline assembly

Assembly may not seem to be a natural language of an open source platform. Most distributed applications that are executed by independent nodes also prefer higher level languages over Assembly. However, in an environment where every operation costs the caller in gas spending, using Assembly language is a way to save cost. Using Assembly makes the execution cheaper for ordinary tasks such as string manipulation [193]. The vulnerabilities in the Assembly operation come from the complicated low-level nature of the language. In case the assembly section of the code creates issues or errors, the contract becomes dysfunctional. It is hard to detect such vulnerabilities as it requires assembly level static code analysis. Code analysis tools can recognize the Assembly code and raise warnings without further awareness of the content.

3.3.3.2.4. Compiler version not fixed

Developers specify the version of the compiler they would like to use at the beginning of the contract code. This specification helps the virtual machine to execute the contract with the same instruction set where it was tested [194]. There will be differences among different versions of a compiler. A newer version may introduce new vulnerabilities. Specifying an exact version is possible. It is also possible to specify a broader range such as any version after a specific version. Static analysis can detect whether the compiler version is specific or not. Since there is no guarantee that a newer version of the compiler would introduce variations in behavior, the output of the analysis would be an indication that the code is not following secure programming practices.

3.3.3.3. Misuse of trust, control of execution and re-entrancy

3.3.3.3.1. Re-entrancy

Contracts can call other contracts, and this interaction can occur in a chain model. There is no limitation in this chain of execution on how many times one of the contracts will be involved. A simple example of this behavior is where Contract-A calls Contract-B which is followed by Contract-B calling Contract-A. This behavior of a contract being called more than once in the same execution chain is called re-entrancy. Typically, a call from a caller contract to another contract gives the control of execution to the receiver of the call. The caller executes commands before this contract-to-contract call. The caller might be planning to execute more commands after this call is complete. If the callee calls the caller contract back, there can be unexpected commands executed from the set of commands that exists at the caller.

Re-entrancy vulnerability can be demonstrated with a money transfer business case. Figure 22 is the pseudocode for an investment scenario where the entrepreneur is returning the money invested by the investors. Figure 23 is the sequence diagram of the normal execution of the contract. When the smart contract is refunding the investments, each investor is just accepting the money. Figure 24 demonstrate the malicious version of the sequence diagram. Here when the entrepreneur's smart contract calls the investor's smart contract, it turns back and calls the same method of the entrepreneur's smart contract. This call-back makes the entrepreneur's smart contract to start refunding again, which would send money to the malicious investor one more time.

```
refundingMoneyToAll(){
    loopAllInvestors:investor
        money = investor.investmentAmount
        if (investor not paid)
          send (money) to investor.address
        mark investor as paid
}
```

Figure 22- A contract for refunding investment in a new company (Pseudo)

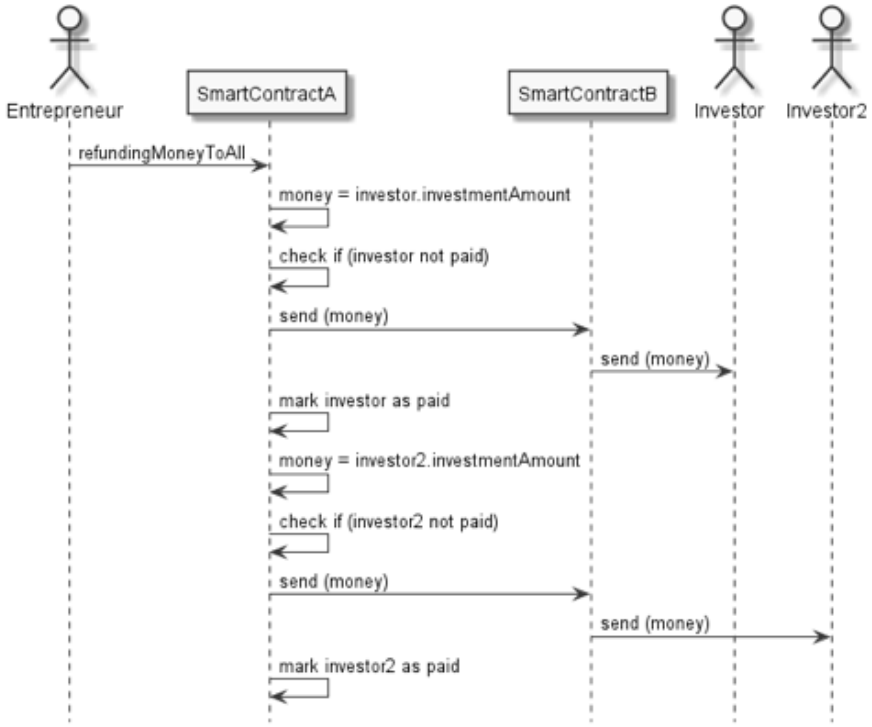


Figure 23- Expected sequence diagram of the code in above figure

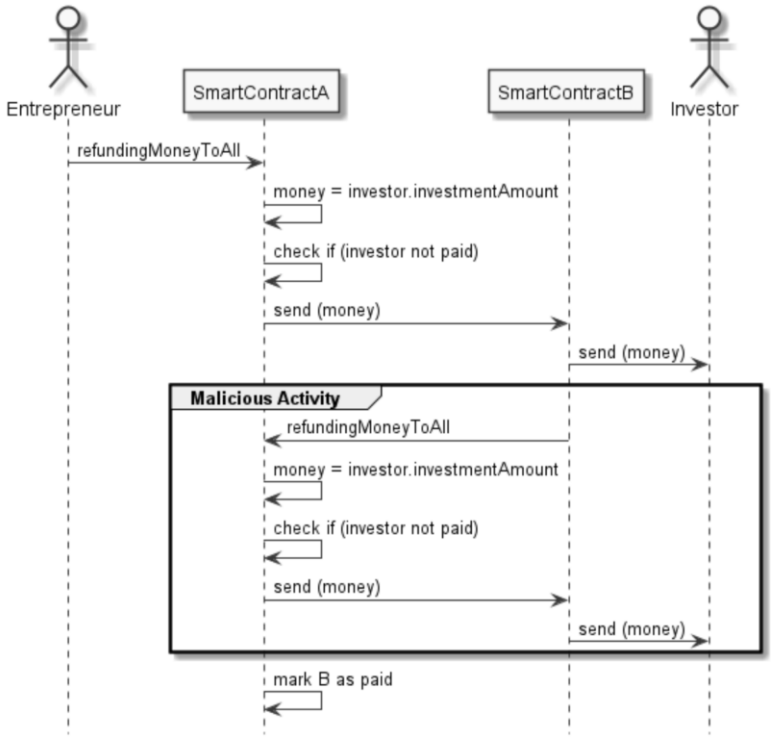


Figure 24- Malicious version of the sequence diagram of the code

Re-entrancy is a vulnerability if the contract code is not written in a manner to prevent the adverse effects. Detecting this vulnerability can be accomplished by pattern analysis. If the contract code is idempotent, or at least if it can avoid any updates when called more than once, then it would not be vulnerable. Detecting whether the code updates the state after the call can identify the vulnerability. Dynamic analysis of fuzzing inputs and mocking the target contracts may also identify whether any undesirable behavior is observable.

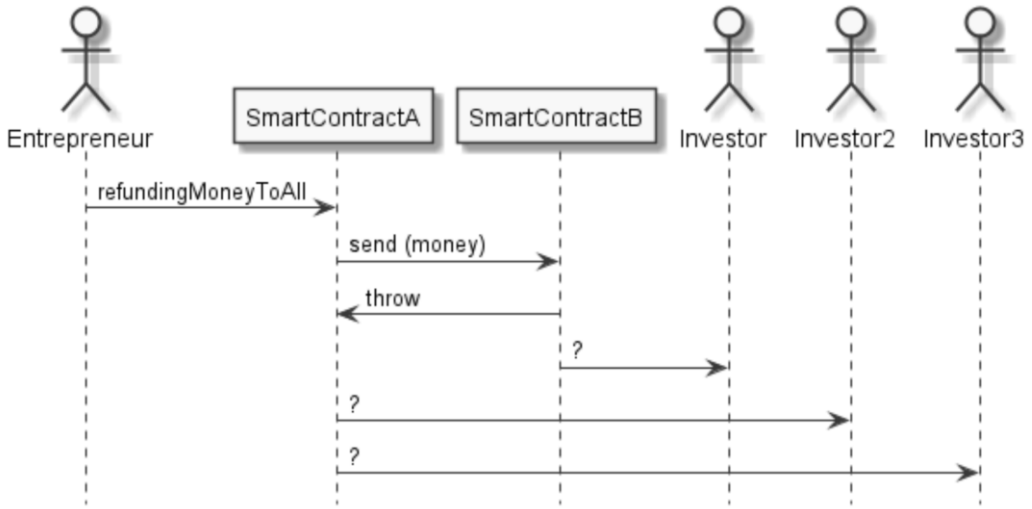


Figure 25- An exception preventing the business flow to complete

3.3.3.3.2. Exception disorder

Exception disorder is a common defect in the execution pattern of the smart contracts in which a method call to external entities can leave the contract paralyzed. If an exception occurs during an external call, all remaining operations in the contract will not be completed.

Developers must check the result of a call in order to decide whether the process can resume or it should be interrupted. Code analysis can detect this vulnerability by checking whether the code is evaluating the result of the call.

Figure 25 provides an example of the vulnerability where a series of operations are to be made. In this example, an entrepreneur is refunding the investments of the investors, and one of the investor's smart contract is throwing an exception. At this line of the external call, if there is no check, the smart contract may not continue with the rest of the operations such as refunding the other investors.

3.3.3.3.3. Unexpected throw - DoS

If the execution of a contract depends on communication with another contract, there is always a risk that the called contract can make decisions based on the logic coded in the caller contract.

The auction process is an example of this behavior. An auction contract needs to return money to the previous bidder when a new bid is better than the old one. However, there are safe and unsafe ways to handle this refund money call. The safe way would be enabling each bidder to request the refund themselves and perhaps communicating that they can call to get their money back.

In this example, making a call to an external contract to send the money before accepting the new bidder's bid is an unsafe design. In general, sending money to other contracts is unsafe due to its dependence on other contracts and multiple vulnerabilities it opens. The suggested safe solution is a pull system for external contracts as described above [194].

3.3.3.3.4. Unexpected revert - DoS

Very similar to the unexpected throw, in the event of a contract depending on other contracts, commonly related to sending payments, the target contract may create a DoS like behavior by simply rejecting and reverting the operation [195].

A typical example of this would be iterating over a list of receiver contracts (addresses) and reverting the whole operation just because one of them issued a revert. The same pull system is advised to be the solution. It is primarily for decoupling the contracts. Meanwhile, it is not clear how the other contracts would know to call these contracts in the pull system.

3.3.3.3.5. DoS with block gas limit

If the developer coded an operation that requires integration with an unknown number of other contracts, such as returning money to an unknown number of participants of a campaign, then the transaction may not get completed- with all the required gas -in one block due to the limit of the gas that can be spent in one block [190]. This condition would require dividing the operation into multiple tasks and tracking the results of the individual tasks.

If the solution involves dividing the operation into blocks, then there is another risk of an event to happen in between the pieces of the operation.

3.3.3.3.6. Unchecked external call

A well-known example of this issue happens at the creation of a conceptual organization named Decentralized Autonomous Organization (DAO). The smart contact of this organization has been a target of hackers and with a high resulting re-entrancy cost to the blockchain network participants [185].

If there is an external call, the contract gives the control away to the external entity, which can be malicious. When needed, additional markings and checks should accompany this call. First, it is recommended to mark the external variables in order to remind the reader which variables are representing tainted sinks. Using names with a prefix such as "Untrusted" is recommended in some resources [194]. Moreover, since the control is handed over to the destination contract, all related vulnerabilities must be mitigated. For instance, the callee contract may try the re-entry vulnerabilities therefore before the external call a contract must change the state in order to prevent re-entrancy issues.

3.3.3.4. Unsafe external interaction

3.3.3.4.1. Use of tx.origin

Use of "tx.origin" for checking the identity of the caller can be open to exploitations. A method should check for the caller instead and should use "msg.sender".

3.3.3.4.2. Send instead of transfer

Send and transfer are two different ways to wire currency to an address. The main difference is that send returns false if there is an issue with the operation and transfer reverts the transaction. Propagating the exception is the advantage of the transfer and not being able to propagate the exception can lead to vulnerabilities for the send method.

Another similar mistake is to send money to an address but not checking the outcome. Caller contract must check the outcome of the send method, and if there is an issue, the transaction should be reverted [189].

3.3.3.4.3. Gasless send

Gasless send is a condition where the contract does not reserve sufficient gas in order to do its final cleanup. Typically, this final cleanup is sending the remaining digital asset to the final destination or returning it. If there is not enough gas to return the remaining ether, the ether may get stuck in the contract.

Gasless send may also happen due to the recipient contract having an expensive fallback function that spends more gas than it was formerly reserved. This issue may happen maliciously but cannot be confirmed as it would look like a planning issue more than a planned attack [185].

3.3.3.4.4. Using self destruct

The "self-destruct" operation is a terminal operation for a smart contract that marks the end of life for it. It is useful as the blockchain no longer will keep the contract for future consideration. As the last step, a typical contract would send remaining money to an address. Having a self-destruction option in a contract is a risk for early termination. There is a significant risk of using this method and sending the money to self or to an address that is not functional. Any other contract that sends money to a destructed contract is also at risk. [196]

3.3.3.4.5. Using throw, revert, assert, require

Using a throw function in order to reject the current execution of the contract can be a valid way of interrupting the flow. If the smart contract code identifies that the current state of the contract and inputs do not meet business conditions, or if the technical checks indicate an issue, then the contract application can use throw to communicate this exception and rollback any changes.

The vulnerability is mostly on the caller side as the rollback is cascaded and the exception must be handled at the caller as well. The reason for the throw is also not communicated well in the Solidity language. An alternative could be using the "return" function [197]. However, in this case, all the rollback has to be handled in the code. The gas would be consumed with the throw and can also become a vulnerability to the caller if the gas is not plenty for the mitigation operations.

Revert, Assert, and Require functions are the new versions of the mechanism that is "deprecated" with the usage of the throw command. Revert is same as the Throw while Assert and

Require contain conditions for which the Revert operation will be executed. The difference between these functions is also at the gas usage details [198]. For readability reasons, Require is better than Throw or revert [199].

3.3.3.5. Vulnerable coding practices

3.3.3.5.1. Balance inequality

The balance field of a contract indicates the remaining balance of money in the contract. The owner of a contract may calculate the amount of money that should be in the contract. However, the value in this field may be different. Occasionally, some money is sent to a contract intentionally or accidentally. Just like a real-life wallet, the critical fact is that this field should contain more money than the owner desires to spend. A common mistake is that the programmer expects an exact amount in this field and makes a check of the value with strict equality. One must remember that any participant intentionally or accidentally can send money to a contract. Developers must use ">=" comparator for all comparisons making sure the contract has enough money [189].

3.3.3.5.2. Redundant fallback function

In the smart contract interaction, there is no compiler level check for the existence of methods at the target contract. Therefore, a call to another contract may or may not find the target method. For this specific case where the called method does not exist in the contract, developers may provide an unnamed method with no parameters and not returning any response. When there is no method found in the contract, the virtual machine calls this catch-all type method. This function can receive ether if also marked accordingly.

3.3.3.5.3. Typographical error

In Solidity, += operation is a valid operator. The validity of this operator is no surprise considering the roots of the language. However, =+ is also valid and using this operator instead of the += have different results [200].

3.3.3.5.4. Integer overflow/underflow

Numerical operations' behavior in Solidity can be different from other languages. Especially integer operations show a variety of behaviors when the value is small or large. For

instance, an overflow occurs when an integer addition result is beyond the maximum of the used integer type, while an underflow occurs if an integer subtraction result in a value less than zero.

If an integer value undergoes to a subtraction that will result in below zero values, it can have an outcome that is close to the max int. If the addition operation on integers exceeds the max int value, it can result in a value close to zero which is the remainder of the value when it rolls after the max int. This vulnerability requires extra checks before the operations. Pattern analysis can spot the lack of extra checks, or safe math library usage and mark the flow as a vulnerability.

3.3.3.5.5. Unchecked division

Integer division is also a warning in Solidity as there may be some rounding that can produce slightly different results than expected [189]. Developers must add extra checks to prevent such cases of division. Division by zero is another example of a vulnerability if it goes unchecked.

3.3.3.5.6. Unsafe type inference

Automatic detection of data types helps developers in rapid code development [201]. In Solidity, a developer can define a variable with the "var" keyword and expect the compiler to infer the value with the type of the assigned value. For instance, "var c= true" defines a variable named "c" and the compiler infers the type as Boolean as the type of the assigned value is Boolean.

3.3.3.5.7. Implicit visibility level

Visibility levels in the Solidity language are different from the traditional levels. For instance, private keywords in the Java language signify encapsulation. External entities cannot access or read the private data. In a public blockchain, on the other hand, there are no hidden values. In Solidity, all variables are visible to the public. The private keyword has importance when contracts are used as a template to create other contracts (derived contracts). The derived contract cannot access the private items in the source contract. [202]

Creating smart contracts that require privacy of data must not trust the simple accessibility keywords such as "private". Developers cannot assume that the "private" keyword will hide the values in the fields. Network participants cannot freely change the value of such a field, but they can read the data.

3.3.3.5.8. Address hardcoding and sending

It is possible in Solidity to initialize a variable such as an address with a value. There may be several reasons for this, such as marking a particular destination. One discovered vulnerability is related to the address usage and caused by the lack of address validation and the lack of strict data structure [203]. The address and the amount of currency are represented back to back in data transfers. If the address is truncated, one digit at the end, it leads to the increase of the amount of transfer by ten folds.

3.3.3.5.9. Array length manipulation

It is possible to manipulate the "length" field of an array with standard arithmetic functions [204]. A simple code to decrement the value of this field can bring the value to an underflow. "anArray.length--;" can make the array size set to max int. This vulnerability can disable a contract.

3.3.3.5.10. A setter method that transfers power to the caller

A mistake can be very ordinary when the programmer codes a method that lets the caller assign a new owner to the contract [188]. Such a method can transfer all the power of ownership of the contract to the caller, through which any participant or any smart contract can call smart contract methods.

3.3.4. Conclusion and Future Direction

In this paper, we reviewed 28 security smells. We classified those security smells according to the context they were identified in: security smells in the smart contract's execution environment, design, or coding. It is necessary to know the security smells and identify their occurrence in order to produce better smart contracts.

Mission critical processes can be exposed with limitless vulnerabilities if they are not implemented on robust platforms. With the security smells analyzed in this research, our conclusion is that reliability of the smart contracts (in Ethereum platform) is not sufficient for confident adoption of smart contracts in access control systems. Processes that can have critical impact to people's lives such as computational public safety also need to wait for improvements to prevent significant vulnerabilities or availability of mitigation.

We have several natural next steps to our research. The first possible next step is to automation of detecting the smells. Detecting smells would require us to develop an enhanced tool to conduct the variety of analysis highlighted with each smell. Our categorization of the smells shows the inherent variety of the issues. We can also pick one of the areas and focus on it. For instance, a tool to analyze the inline Assembly would benefit stakeholders greatly as they cannot read those sections as comfortably as they read Solidity code. Assembly analyzer can also help the overall performance of smart contracts as Assembly commands can be executed faster. Assembly commands also spend less gas.

Another next step can be to quantify this study with the number of occurrences of these smells in existing contracts. This effort would show us the trends, and we would be able to see whether occurrences of these smells are decreasing or fluctuating with time. A categorization of smart contracts and numerical analysis on which type of contracts are creating which category of smells would help understand the difficulties developers and designers are having using the environment. Perhaps Ethereum and Solidity are not adequate for some specific business ideas.

Our novel idea to continue is to create a new type of smart contract that can heal some of these security smells. Currently, smart contracts inherit their immutability from the blockchain. We will continue our research on developing a new type of smart contract to change this behavior slightly to heal the issues without impacting the trust base of the contracts. In practice, contracts are binding agreements. However, parties in the agreement can issue updates and amendments to an existing contract while adapting to changing conditions. In the technical setting, contracts can be as useful as their agility. Smart contracts cannot fulfill the update requirements with their current model. A new type of smart contract with an ability to evolve can adapt to these requirements. This update ability must not conflict with the fundamental principles of blockchain technology. An update in this new type of smart contracts does not intend to replace the old contract which the blockchain held in the previous blocks. In the new smart contract design, a new block will persist transactions related to this update operation. The new smart contract model will include and enforce the conditions of the update in every contract. An ordinary contract can include a list of beneficiaries that can vote for the update. A specific contract such as one that serves as an access control system should have several features serving to the nature and sensitivity of the operations. Features can include a panic button that can be triggered by specific contributors to lock down the contract until a set of access process managers audit the incident and re-enable the contract.

3.4. Utility Blockchain for Transparent Disaster Recovery

After completing the underlying frameworks, we used our findings towards our first use case which is primarily concerned with disaster operations. We start with the use case of a limited impact natural disaster situation (severe damage caused by high winds) and implement a solution using blockchain technology. This study provides insights and answers to the key questions on suitability of blockchain technology on providing a reliable information layer to disaster recovery teams. This study helped us start forming our fundamental arguments on the suitability of blockchain implementations at the times of emergency conditions where normal systems and processes are not functioning.

3.4.1. Introduction

In this paper, we review the current problems in energy and utility industry, and discuss the role of blockchain technology in providing potential solutions. Blockchain technology is an opportunity for most businesses as it fundamentally changes the way of doing business between peers. By removing the need for the middleman or a central authority, blockchains let their members transact businesses directly, i.e. peer-to-peer.

Energy and utilities are bedrocks of civilization. This fact is made more noticeable when there is a severe service disruption. We present a novel use case on how a blockchain-based system can be used effectively in a disaster recovery scenario. We detail the advantages of the blockchain technology in restoring the service and increasing the transparency of the overall system.

3.4.2. Utility Industry

The utility industry is traditionally a high friction environment. Several actors are involved in transactions and operations. Whether it is a trade or service, lack of trust between the actors has always required a central authority to oversee and regulate interactions. Costs such as broker fees

make transactions slower and more expensive [205] as the central authorities need to be involved for every significant transaction.

Beyond what is required due to regulations, the data sharing and reporting rules in this industry do not promote access to data. Even for the limited interactions happening, due to the increasing number of the actors, fragmentation can only be avoided by standardizing data formats across multiple organizations and by enabling inter-operability.

Utilities are essential for the livelihood and health of customers. Therefore, sustainability and resilience of the system are essential. Any ideas for improving system health or recovery speed are invaluable.

The market is changing with further involvement of consumers especially in the electricity distribution industry where consumers are becoming producers thanks to solar panels. As the marketplace is getting crowded, there are assumed risks of fraud, error and invalid transactions. Considering that autonomous entities are also joining the business ecosystem, a trustable and secure way of conducting business is important.

Blockchain technology is not a magical tool that can single-handedly transform the energy industry [205]. However, the benefits of blockchain technology such as increased speed of exchange, auditability, reliability and high availability are disrupting the traditional thinking [206] in the energy sector.

3.4.3. Blockchain Experience in The Utility Industry

3.4.3.1. Microgrids

Recently, the utilities industry is feeling an impending threat to bottom lines. This threat is coming from whom the significant players of the industry have been serving for decades. Ordinary people are installing solar panels on the rooftops of their houses and selling electricity to a neighbor. The industry perceives this as a risk. The distribution model and the scenario of just one household trading with another is the smallest scale of the pattern. The risk becomes significant when sufficient households in a neighborhood are producing electricity for every home in the neighborhood. The neighborhood being self-sufficient means the utility company losing their business. Since there is no middleman charges or commissions with peer-to-peer trade, there is

less money for the established corporations in the market. Further, the price of this retail produced electricity can be lower than that offered by the utility company.

These microgrids of self-sufficient or mostly sufficient neighborhoods [207] create intelligent energy networks where the prosumers can trade energy. Each prosumer is independent to use strategies that will make them more successful in a distributed market instead of all consumers trading with the single central authority of the local energy market (LEM).

Peer-to-peer energy trade can open the doors to a barter universe [208] where participants can exchange their surplus of different types of products. A barter mechanism can help facilitate a cashless trade option for the benefit of all systems participants even the ones that consistently over-produce.

Blockchain technology can facilitate peer-to-peer electricity trade in a microgrid. The overall system will benefit from the added resilience [209] with blockchain features such as not having a single point of failure. Since blockchain applications are stronger with increasing number of participants, one blockchain can handle a large-scale implementation. Using a blockchain does not mean lack of uniform rules. Blockchain technology provides distributed management capabilities that enforce network-wide rules.

There are many projects explicitly aiming to facilitate such trade on blockchain platforms. There are small-scale implementations such as LO3 Energy managing a microgrid in Brooklyn with 200 smart meters [210], Enerport enables selling or gifting in Ireland [211] and PowerLedger that facilitate the neighbor-to-neighbor trade in Australia [212].

There are some metropolitan scale implementations such as Tokyo Electric Power Company [213]. Grid+ [214] and Enerchain [215] are replacing the utility company with the blockchain infrastructure while distributing wholesale power.

In the international scale, WePower [216] is a company that facilitates the trade of energy by tokenizing the energy on the blockchain. Smart energy contracts of WePower enable its consumers to execute the trades reliably. The WePower project has support from Lithuania, Estonia, Spain, and Australia.

It is not just about selling the energy. In Spain, Endesa and Gas Natural Fenosa prove that big utility companies can also benefit from blockchain while buying and selling energy [217].

3.4.3.2. Which blockchain to use for utilities?

Every energy sale implementation does not need to have a dedicated blockchain. The literature offers detailed analysis on the suitability of current popular blockchains to microgrids trading [218]. Such research lists most relevant distributed ledgers for energy transactions. A new implementation can use one of the reviewed blockchain platforms that are suitable for its own conditions.

Some utility industry blockchain implementations are built on cryptocurrencies in order to use the underlying system as a payment vehicle. Implementations that require avoiding the use of popular cryptocurrencies can use the specific cryptocurrency named NRG Coin [219]. NRG Coin is created to carry out payments and rewards of the energy trading systems.

The integration of cryptocurrency is standard practice in energy market blockchain projects [208]. A large-scale system such as European Energy Market trading system uses the token and smart contracts of existing cryptocurrencies. Using both entities together helps complete the payments and execution of the agreements on the same blockchain infrastructure.

Most businesses require privacy. Where the anonymity of the blockchain provider does not serve the energy trade requirements, there are alternative solutions. PriWatt is a token-based energy trading system that handles the privacy issues in common blockchains by hiding the intermediate price signal on energy trading transactions [220]. PriWatt promotes additional anonymity for the transactions by enforcing the generation of new messaging addresses for each new trade negotiation.

IoT universe consists of small-scale devices and elements that have several issues related to take part in a peer-to-peer trade. A decentralized method is essential [221] for the auditability and visibility of the processes, transactions, and issues. Without transparency of a blockchain, a peer-to-peer trade could be open to mistakes and errors. Identifying such mistakes such as pricing issues can be faster with blockchains. Iota cryptocurrency is a blockchain implementation that aims to address the inter-device transaction issues in IoT with a high throughput, high availability and low transaction costs.

Using a cryptocurrency blockchain does not necessarily mean cryptocurrency holdings are necessary for the participants. A credit based payment scheme can also facilitate trade between the

IoT participants. At the end of the billing term, participants can settle with local currencies. This methodology helps the trading platform to benefit from the mature cryptocurrency blockchain and avoid creating a new blockchain.

3.4.3.3. Energy harvesting networks

Current implementations of blockchains in the energy market are isolated based on the location of implementation and low volume of transactions. Beside the small-scale trade between low volume individual participants, there are industrial-scale implementations of energy harvesting from natural resources. Energy harvesting nodes can trade the surplus energy utilizing P2P energy trading [222].

3.4.3.4. Vehicle-to-Grid networks

Vehicles can be involved in electricity trade in many ways. One of the favorite scenarios is where an autonomous vehicle uses charging stations and pays the price of electricity [223]. This scenario is an example of how blockchain technology creates a medium for other new technologies to flourish. Non-autonomous electric vehicle charging platforms such as BlockCharge [224] can increase the availability of charging stations by simplifying the billing process in a secure and reliable way.

Electric vehicles can also be energy producers where it is operationally and financially feasible. They can feed their stored energy back into the power grid to help the network during peak demand [222]. This transaction can be registered using blockchain technology. Energy trade can also happen between vehicles. A vehicle can sell its energy to a neighbor vehicle and use blockchain technology to record the sales transaction. Involving blockchain would enable this transaction to happen in a P2P manner [225].

3.4.3.5. Green certificates or white certificates

Renewable energy certificates or green certificates help organizations prove that the electricity they provide is generated from renewable sources [226]. Solar, wind and wave energy are examples of such sources that can be used to receive green certificates. Production facility information is essential for the certificate issuance and this information is stored in national registries. Benefits of owning such certificates vary from state to state. By trading these

certificates, organizations transfer the rights to the benefits. Flexinergy blockchain is an example implementation of green certificate blockchains [227].

White certificates in Europe aim to be similar to green certificates. An organization that reduces energy consumption receives these white certificates. The benefits of white certificates are transferrable, therefore the certificates are tradable. Moreover, since this trade can happen beyond the borders of the issuing country, there are multiple amounts of costs attached to conduct a trade of certificates provided by multiple countries [224]. Blockchain-based trading of such certificates is a great use case where standardization of the trade environment benefits all trading partners. Storing the certificate on a blockchain makes the authenticity of these certificates much more reliable since the tamperproof provenance is accessible through the blockchain.

3.4.3.6. Smart contracts

The smart contract feature of the blockchains is a candidate to replace the physical contracts of the energy trade. Smart contracts can settle the exchange of energy using the agreed upon price.

Another benefit of using smart contracts in the energy internet is that it enables producers to price their product according to system load. If the system requires producers to be discouraged to maintain system stability, a dynamic and demand based pricing can be implemented with blockchain technology [228]. Users in a peer-to-peer environment are usually selfish. Blockchain technology can be used to form an incentive mechanism to curtail this [229].

In a cryptocurrency based blockchain, there is an added benefit to energy trading with an instant settlement. Instead of trading parties settling in several days or months, they can settle in a blockchain as soon as the registration of the transaction with the blockchain is complete [230].

3.4.3.7. Consumer impact

Customers are looking for better prices and better service. Better prices are usually an end-result of competition. One advantage of having a blockchain-based utilities market is that since sales happen on the standardized media of the blockchain, changing suppliers is more comfortable and quicker [223].

In many municipalities, energy consumers can sign contracts with one of the competing sellers [231]. Blockchain-based energy trade platform would be a natural fit for the facilitation of such open competition. Trading parties can conduct energy sales transactions on the blockchain

using a bidding interface for the consumer to discover the best price [232]. Blockchain technology is suitable for bidding applications, and GRIDNET protocol is an example that uses a bidding feature as part of their system.

There is one more benefit of using blockchain technology to enable peer-to-peer transactions. In a world where the central authority does not need to transfer electricity, there would not be any power lines in communities. Avoiding power lines may not be very probable for the northern countries where there is a high dependence on grid provided energy. However, with the help of battery technology storing the excess power, it can be a reality for sunny states.

3.4.4. Issues

There are many issues to be solved before blockchain technology is accepted as a revolution in energy markets.

3.4.4.1. Scalability

Blockchain transactions are complicated. There is no intermediary; however, every node in the system is expected to contribute. There are data collection, verification, and block creation tasks. Nodes need to be involved in consensus activities and they are expected to vote for the acceptance of the newly created blocks. The verification mechanism can reduce the performance of the overall system [221]. This performance degradation may be a limitation for blockchain networks to carry high volumes.

3.4.4.2. System as a service

Energy trading parties benefit from blockchain networks, but it is not clear how the blockchain service providers benefit from blockchain operations [221]. There are activities like coding, governance, maintenance, forking, and monitoring. It is crucial that sufficient number of participants benefit from these activities so that operations do not stall with blockchain related issues. There are several possible solutions to this problem. There may be incentive programs for such operations such as a transaction fee or where the network compensates this service with electricity. Alternatively, each trading party can do their part as a blockchain participant. Each party can be running a node of the blockchain and contribute to all blockchain activities listed above. Smart meter infrastructure can handle these activities.

3.4.4.3. Reliability and security

It is crucial that the energy system be resilient to attacks. Security failures can be dangerous or life-threatening. With adequate measures, energy system must prevent potential cyber-physical or even catastrophic cascade of failures. Blockchain networks may have an issue in this area. Decoupled and distributed network structures do not allow a proper perimeter security. Since there is no central authority, having contingency plans may not be possible either.

Energy trading of IoT devices has its security risks. For instance, it is insecure for some IoT nodes to trade with each other in a non-transparent environment. In such an environment administrators cannot audit and verify transactions in real time [222].

3.4.4.4. Privacy

IoT nodes that trade electricity carry a risk of revealing information about the entities that own these nodes. The amount of energy sold from devices may be classified as confidential information. The amount of money earned from the transaction can be a trading secret. Identities of trading parties can be confidential as well [222].

The blockchain that facilitates the transactions in the network can reveal patterns of energy usage, patterns of energy production and can predict one's past and future activities. Privacy-preserving smart contracts are possible, but they tend to be more complicated and expensive [233].

3.4.5. Blockchain-Based Disaster Recovery

3.4.5.1. Environmental factors

In a country with harsh winters like Canada, power lines are usually a victim of natural disasters. Red Cross continuously warns Canadians that winter storms or extreme cold can occur suddenly in Canada. Strong winds and freezing rain can be at destructive levels to the power lines.

In January 1998, parts of eastern Ontario and Quebec were hit by three storms in one week. Power lines could not carry the weight of the accumulated ice. Transmission towers were down and about one million people were left without power.

It was not as strong as 1998, but in the last days of winter in 2018, in Toronto, there were severe winds and many trees were down destroying electric lines.

When a power line is pulled down by a falling tree, the damage may not be only to the power line but to the power infrastructure of the houses as well.

Figure 26- Fallen tree pulled down the power line

Figure 27- Power line pulled and damaged the power infrastructure of a house

For such damage, there are rules and regulations as to which organization and which crew can handle which part of the issue. In our sample scenario, a big tree is down on a power line, and destroyed the external power infrastructure of the house. Multiple crews need to work in order to restore this. There are requirements, responsibilities, work, compensation and risk for multiple stakeholders.

3.4.5.2. Problem definition

This power outage can continue for an extended amount of time. Under the winter weather conditions that contributed to the disaster, mainly high-speed winds and cold, losing power is very uncomfortable for families.

The problem continues to mountain as the restoration of service becomes a long and expensive process. While a family is sitting in their cold home without electricity, they have almost no means to know the progress of the process including ETAs. In disaster scenarios, it is possible that there are high volumes of issues slowing the system down. However, without transparency, people waiting for help are left in the dark.

If everything goes well, the parties may do their part and power can be restored without further damage. However, if further damage is incurred due to events during restoration, it should be attributed correctly to the responsible entity. This can only be done with adequate information. When a system does not provide information to the participants, further conflict resolution is usually problematic.

For example, there is a surfacing risk of repair services being overcharged during a disaster where a high volume of repairs is needed. To prevent such overcharging reaching fraud levels, the system needs to include an audit mechanism.

3.4.5.3. Stakeholders and actions in service restoration

The principal stakeholder is the owner of the property as there is probably an actual danger of live wires on the ground or there is a power outage. When an insured property is involved, insurance companies are stakeholders in every issue, risk, and expense. For any harm to people, insurance companies and lawyers are involved and become stakeholders. The power company is a stakeholder as it disconnects and reconnects power. The power company typically is responsible for fixing the majority of the damage to the wires and they are involved for removing the fallen tree off the power lines. If the damage occurs to the private section of the electric infrastructure such as the pole that is attached to the house, the owner of the property is responsible for handling the repair efforts. The owner of the property has to hire a certified electrician to fix the hardware. Regulations enforce a safety inspector to inspect the repairs before the power company can reconnect power [234]. The safety inspector inspects the repair and leaves a small card at the end

of inspection. This card typically indicates the inspection certification number. Finally, when all activities are completed, the power company reconnects electricity. [235]

All these activities happen while there is minimal precision in scheduling. The lack of transparency and busy schedule during the disaster make things even more chaotic. The above participants involved in the restoration of the service gather minimal information and they do not share it efficiently.

3.4.5.4. Proposed solution

We propose to manage this disaster recovery effort with blockchain technology. In this disaster recovery and service restoration blockchain, each party will register and communicate the information and plans transparently. Figure 28 and Figure 29 demonstrate how this blockchain will host scheduling details, task status, open issues and planned activities. This platform will communicate all the information to all parties. Blockchain technology will create a tamper-free copy of the history of the case. Timelines, events, actions, and decisions will be evident in the blockchain.

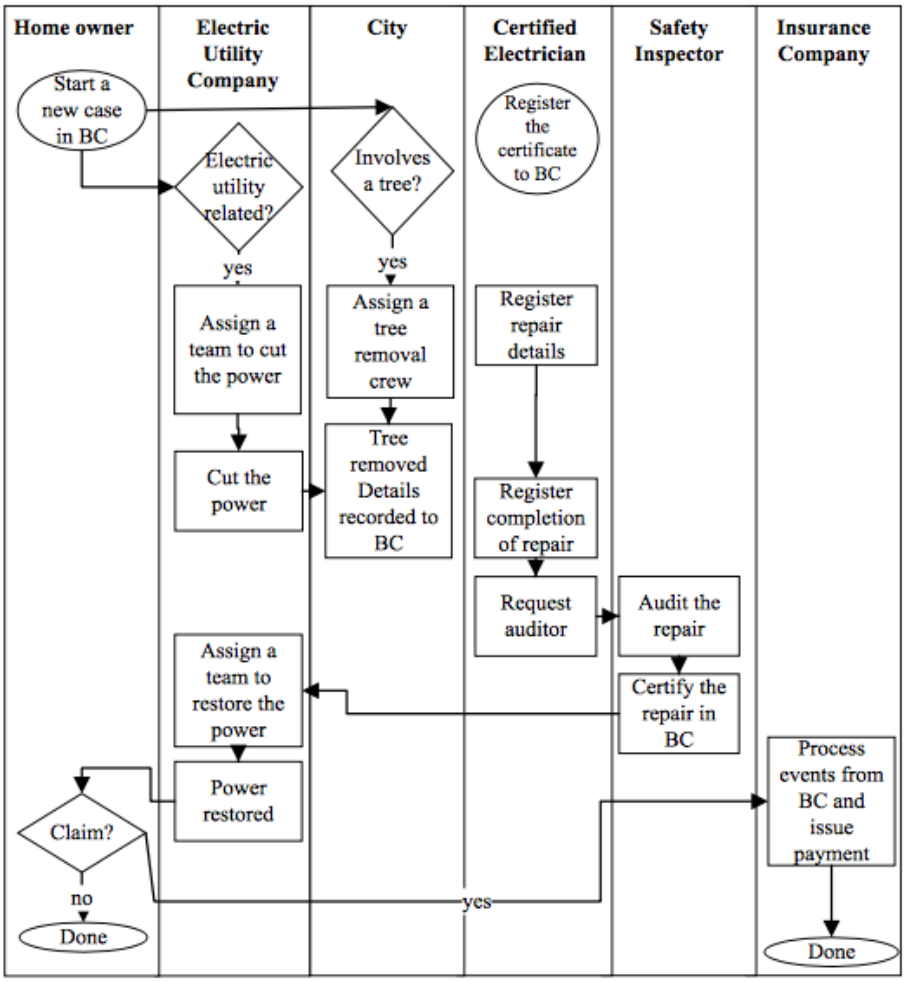


Figure 28- Cross functional flow chart of the blockchain events

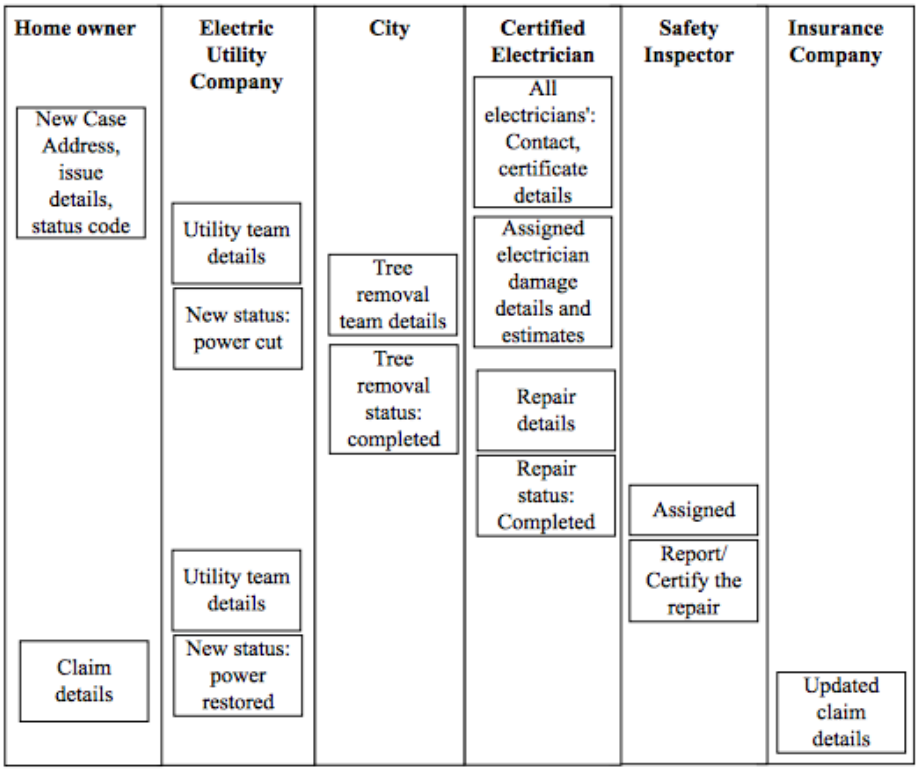


Figure 29- Chart of the blockchain stored information (vertically sorted with time)

In case of a dispute, evidence related to the case can be produced easily from the tamper-free records of the blockchain. Insurance claims can be resolved with extended clarity. Service can be restored much faster as this information channel would help identify issues and improve service quality.

Participants would record and keep many levels of details on the blockchain such as the certification number of the electrician that fixed the damage and the identity of the crew that removed the fallen tree. Service quality issues would be addressed with the information on the tamper-free blockchain structure.

Many useful statistics such as the service timing statistics of the inspector, the number of cases serviced, response time statistics, and prices for the services provided would be auditable and reportable. Any fraud cases can be investigated with this information. Time would not work against the evidence. If there is abuse in the system such as overcharging or unnecessary overtime charging, it would be detected with the reliable information from the blockchain.

In case of a dispute, the blockchain can help with the quick resolution of the case. Lawyers, insurance companies, police and other authorities can decide faster and better with tamper-free information.

3.4.5.5. Metrics

Blockchain solutions provide us some metrics to prove the effectives of the implementation. It may not be feasible for comparing the number of disputes and ease of resolution of them. But we can measure the ease of identifying the fraudulent reporting. Cryptographic hashing is a fundamental feature of the blockchains and comparison of hash values reveal the difference in the sources. Blockchains are also replicating the data between the stakeholders. This replicated data also creates witnesses who has the same version of truth as each actor. Together with replication, cryptographic hashing would be used to prove increased trustability. Some other values can be measured in the implementation such as speed of blockchain transactions as well as the throughput and the capacity of the system. These metrics will be used to assess whether the proposed solution can handle the expected load in the target domain.

3.4.6. Conclusion

There are several use cases of blockchain technology in the utilities sector. We presented the variety, benefits, and issues of these solutions recognizing that most of these use cases focus on the trade aspect of utilities. Blockchain technology facilitates better service when neighbors are selling electricity to each other or when vehicles are interacting with charging stations.

We identified a potential blockchain solution for the service restoration after a disaster. We propose using blockchain technology to capture the details of the restoration operations where several actors are working together and several stakeholders are depending on. We provide details on how transparency helps with this scenario and how a blockchain can facilitate the transparency. Through this solution, we show that blockchain technology can be used for temporary relief of the burden caused by a disaster.

Blockchain applications add transparency to the businesses. With the number of parties and the business risks increasing in a disaster recovery use case, we see that the benefits of blockchain also expand.

3.5. Blockchain-Based Transparent Vehicle Insurance Management

Disaster operations and IoT domains converge in the use case where relief efforts are delivered using high technology vehicles. Integrating a variety of vehicles such as Autonomous Unmanned Aerial Vehicles (UAV) to disasters requires the integration of a collection of technologies. Blockchain technology ensures the continuous collection of reliable data from vehicles. With this vital role of blockchain technology in the vehicle domain, we develop two use cases and use them in our research. First, we conducted a survey of blockchain implementations and opportunities in the vehicle industry. We concluded that blockchain technology adds value to the services and information provided by autonomous vehicles.

3.5.1. Introduction

Even though there is a high volume of information content about blockchain technology, successful implementations have not caught up with the volume of publications. There are several infeasible implementations due to lack of understanding. Like most technological tools, blockchain can provide business benefits when its features are suitable to solve the business problem. In other cases, it may merely provide some advantage that may not justify its implementation costs.

In what follows, we present a literature survey of blockchain applications in the automotive industry. This survey highlights the leading use cases of the blockchain technology in this industry.

Following that, we present a novel use case and a blockchain-based solution for the insurance record of motor vehicles. We then present the details of the design and the benefits of such a solution. We also list the issues that a blockchain-based application needs to address. We conclude our paper with the future directions of this research.

3.5.1.1. Blockchain technology

In order to understand blockchain technology, one must understand the importance of record keeping. Record keeping has been a factor to facilitate cooperation between people in large groups and eventually contributed to the formation of large-scale societies [27]. Due to its complexity and importance, keeping a history of transactions is a task for trustable authorities. These authorities keep a book of record about the activities in their subject domain. For example, a bank is a selected authority in the finance field to keep a book of record for financial transactions. A bank can keep records of activities, events, applications, and decisions. In case of a dispute, the bank's records are the truth. For motor vehicles, manufacturers, dealers, and owners all interact with the government's motor vehicle agencies. Records kept by these agencies have always been considered as the source of truth.

A ledger is a structured list of transactions that represent the state of entities, activities, and events. Since their discovery, ledgers have been proven useful for several purposes such as reconciliation, audit and issue resolution by recording a relevant history of transactions. Distributed ledger technology (DLT) is a system based on the premise of communicating ledger entries to the stakeholders. Commonly, a DLT communicates each transaction to each participant of its information network. When a member of the network records a new transaction, every other stakeholder receives the same transaction record. This level of replication turns every stakeholder to a witness of all the transactions. Denying or tampering the transactions becomes harder with the increasing number of witnesses.

Blockchain is a specific type of DLT that packages transaction entries into blocks in order to facilitate more structured communication. With the help of cryptography, each block contains the hash values of its transactions and the hash of the previous block. This pattern of each block containing the hash value of the previous block is what makes the structure called a "chain." Each new block created is appended to the chain of blocks. Participants of the network check the validity of the block with its transactions and form a consensus on acceptance. Blockchain networks are tolerant to participants' availability. Any member of the network can be offline without impacting the network. When a participant becomes online again, it can download the blocks that are accepted when it was offline. With the hash values included and structured as a chain, it is mathematically infeasible to tamper the blocks. Upon receiving a block or several blocks, a

participant can validate the blocks, and identify any forgeries. With this ability to identify forgeries, blockchain is a tamper-resistant ledger.

There are two types of blockchain networks based on who can be a participant. A public blockchain is where participation is not restricted. Anybody can be a member, receive the transactions, issue new transactions and create a new block. Participants of public blockchains are equal and anonymous behind the public-private cryptographic key pairs. Implementations of public blockchains have different measures to guarantee the healthy operation of the blockchain and to prevent malicious activities. Meanwhile, permissioned blockchains identify the users and assign predefined roles to them. Business rules of each implementation define the restrictions to participation in the blockchain. This blockchain may also have restricted roles and responsibilities for participants. Operations such as forming new blocks play a significant role in permissioned blockchains.

Blockchain technology is a trust provider. Participants who otherwise would not trust each other can use this technology to create a medium for collaboration. Having a ledger to depend on enables more business opportunities between entities that otherwise would not easily trust each other.

3.5.1.2. Industry, information, and blockchain

The automobile industry has always focused on producing better vehicles. With the recent technological advancements, this industry has found great opportunities to improve and innovate. From battery technologies to big data and AI [236], there are a lot of great tools that help this trend. This industry is committed to innovation. A European Commission report reveals an automobile manufacturer (Volkswagen) to be the top R&D investor in the world [237] in front of Microsoft, Intel and Apple. Eight of the top 23 R&D investors in the world are part of this industry [237]. This orientation suggests that auto manufacturers would embrace innovative technologies like blockchain once their benefits are proven.

The volume of collected data on vehicle-related interactions is also increasing. Previously, automotive industry defined identifying attributes such as VIN, engine number, make, model, year and color of the car. These data originate at the creation of the car, and mostly stay unchanged if the vehicle was not subject to significant reconstruction. Dynamic attributes such as ownership related data include the owner, license plate, insurance and several types of taxes. Even though it

is changeable, these data do not frequently change either. In the last decade, the data we would like to retain on vehicles and their interactions increased many folds. In this decade of disruptive technologies, we need to record behaviors, interactions, and step by step history of events. It is beneficial to record who can drive the car, performance of the car, driver's driving performance, purpose of the journey (business or leisure), odometer readings at the beginning and end, signaling patterns, and much more.

3.5.2. Background Study

There are several subject areas in the automotive industry that can benefit from blockchain technology. In this section, we present current applications of blockchain technology on automotive vehicles.

Utilization of blockchains is reaching to a broad set of targets. This large set of ideas is an indication of benefits that blockchain technology is adding to the industry by convincing its major players. Mobility Open Blockchain Initiative (MOBI) [238] believes that blockchain technology is going to enable a whole range of mobility services.

3.5.2.1. Payments

The lightning network and smart contracts are opening many opportunities for recording sensor data in major blockchains like bitcoin. Secure communication and payment can be defined between electric vehicles, charging stations and operator corporations using blockchains [239] [240] [241] [242]. Hybrid vehicles can also sell electricity to each other and record these transactions on a blockchain [225].

Currently, wireless charging of devices is considered to be a practical topic. Blockchains can be used to facilitate this transaction [243]. Even though the implementation is not widespread, there are several types of wireless charging stations under discussion. There are ideas to build vehicle charging stations at traffic lights or parking areas where charging happens while waiting or parking. Blockchain technology is very suitable for recording such a transaction to be used to facilitate payments.

3.5.2.2. Autonomous vehicle charging

Autonomous vehicles have a lot to benefit from a tamper-free ledger. They can pick the charging stations using blockchains [244]. In order to provide a reliable ledger of the events, a blockchain can record charging station and vehicle communication including the acknowledgment of the energy transfer and payment for the service.

3.5.2.3. Odometer fraud prevention

Motor vehicles are durable products that have long lifetimes. That is why second-hand sales are very common. The used car industries serving this market are large with an annual business volume of hundreds of billion dollars. Only in Europe, this volume is reported to be 180.4 billion euros [245]

One of the most common frauds related to used vehicles is odometer fraud. Lowering the mileage of a vehicle by tampering an odometer and would increase the perceived value of the vehicle and trick buyers to believe the vehicle is in better condition than it is. When cars are transported beyond state borders, tracing their history becomes even more difficult. Odometer fraud is costing Europeans as much as 9.6 billion euros as of 2014 [246]

A blockchain periodically recording odometer values can prevent this fraud. Such a blockchain can also record odometer values when a significant or witnessed event happens. Significant events can be service visits or the renewal of vehicle license stickers.

It is certain that a car odometer tracking platform running on blockchain technology is beneficial for recording the complete lifecycle of a car, informing the interested parties with tamper-free information, and helping the community with injected trust in order to let them reach a more precise valuation of vehicles [247].

3.5.2.4. Re-vinning or re-build

Auto thieves change vehicle identification number (VIN)s of vehicles to re-market them as clean vehicles. A blockchain to correlate the VIN to other attributes of a vehicle can help prevent this type of fraud. An accessible history record can also reveal whether a vehicle had an accident where the insurance inspector marked it as damaged beyond repair. Mechanics repair these vehicles with low quality or unsafe methods by collecting main pieces from multiple vehicles and

fusing them. This repair may not be visible to inexperienced consumers. However, it can be unsafe in high-stress conditions such as high speed or a collision [247].

3.5.2.5. Vehicle to vehicle comm. in intelligent transportation systems

Inter-vehicle communication is one of the emerging topics in IoT. There are several use cases of enhancing the driver experience with inter-vehicle communication. Blockchain technology can help build an inter-vehicle communication system by hosting features such as admission [248]. Announcements communicated vehicle to vehicle can improve the driver's experience. Blockchains can be used to record these communications. The credibility of the received messages can be assessed using a blockchain [249]. Blockchain technology can also be used to provide incentives to this platform [250] [251].

3.5.2.6. Vehicle forensics and insurance

Connected and Automated Vehicles (CAV) adds several new data to the potential disputes. The decision-making capacities of such vehicles are based on sensor data and in case of an incident, the sensor data is part of the evidence to be used in the decision to identify a resolution. Recent literature proposes forensic systems to be built on blockchain technology. Both B-FICA [252] and Block4Forensic [253] are proposals for a forensics blockchain. Their major challenges are IoT data volumes and timely communications. Collection of forensic data shows flood like characteristics while on the other hand, usage is very rare and generally much after the fact.

3.5.3. New Use Case

In this study, we are focusing on the following new use case that can help revolutionize the auto manufacturing and insurance industries.

3.5.3.1. Tracking insurance records and preventing fake proof of insurance

Auto insurance is mandatory in many countries. Each driver is obligated to have insurance to drive and must produce a proof of insurance ownership when requested. In Ontario, the proof of insurance form is known as a pink slip because of the color of the forms provided by the insurance companies. Drivers are the centre of the insurance-based communication in Ontario. Drivers provide the proof of insurance coverage when pulled over by police, buying/leasing a car, registering a car, and when renewing the license plate stickers. In all these occurrences, drivers

deal with each party separately. For example, a driver buying a new car, purchase insurance from the insurance company and carry the documentation to the car dealer for the release and licencing of the car.

There are a lot of manual steps in the process of providing a proof of insurance. Manual steps and physical evidence-based systems are open to fraud such as forging vehicle insurance cards and selling them [254]. High insurance prices motivate people to accept such risks. There are several use-cases of fraudulent activities around insurance records. In official grounds, there are consequences for using a fake document, but drivers bet on the inability of the authorities accessing the correct information promptly. Since most incidents in which drivers are asked to present proof of insurance do not reach official grounds, drivers may use fraud to get out of a current trouble situation. There are several reasons for the manual process to be misused between the parties that does not trust each other. All these parties are dependent on the quality and reliability of this information. The risk of error in communication is also high where a driver is carrying and filling forms.

A blockchain for obtaining, sharing and verifying insurance records will help stakeholders as a reliable sharing platform and a ledger of events. Drivers can further share the pink slips through the blockchain. Such a blockchain can even record this sharing event in case there is value in tracking who requested to share which record and shared with whom.

The main motivations for a blockchain solution are the requirement for transparency, collective nature of contribution and participants' lack of trust to each other. A secure centralized database solution of similar purpose would have challenges in ownership, maintenance and governance. The conflict of interest between the parties would prevent a solution that would be owned by an external entity. Decentralized solutions such as blockchain are also more resilient to the attacks as there is no single point of failure.

An alternative solution could have been storing the same information in a centralized database. Even though the technology for this solution is available for long time there are several reasons that there is no such implementation. Main reason is the difficulty of governance, responsibility, management and administration of such a central system. Endless questions starting with "Who will.." ends in no party tackling above mentioned difficulties. Blockchain solution proposes liberty in joining and collective actions based on democratic behaviors to operate. Equal

rights, responsibilities and cost lies to every major participant. Individuals would benefit from better service quality and automation of the system. In case of a dispute, all parties benefit from justice that better quality evidence brings. Distributed nature of the blockchain also increase its reliability and availability. Distributed management would make sure no party single handedly modifies the data especially where there is conflict of interest between the parties. Distributed systems are more resilient against denial of service attacks or service outages.

3.5.4. Design

The solution to the difficulties in tracking insurance records is creating a blockchain platform to enable all participants to communicate, share and record information. We have a phased approach to the production roll out. The first phase will be the insurance records as described in this paper. The following phase will include an extended set of capabilities targeting vehicle-based information including telematics.

3.5.4.1. Participants

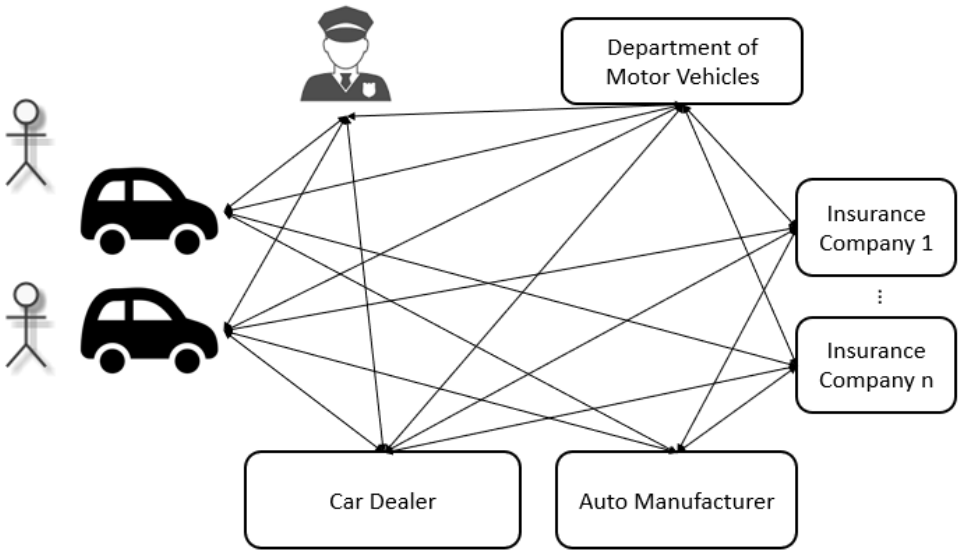


Figure 30- Participants of the blockchain-based solution

The participation in the proposed blockchain network is as depicted in the Figure 30. Participants include individual drivers, business organizations such as insurance companies, and governments agencies.

Individual drivers are key participants in this ecosystem. Like in most systems, benefits provided to the individuals and their adaptation to the new platform will define the success of this project. Even though individuals who do not own a vehicle can access this system, we expect most individuals to be drivers with vehicles, purchasing insurance, and using the interfaces provided by the system. Depending on the privacy rules and concerns, individuals can be a full node in this system involved in all communication, or they can be allowed to access only limited information via their insurance agency. We discuss this matter further in the privacy section. At this time, we assume they are a direct participant in the system.

Businesses will uncover great opportunities with the blockchain to improve their data collection and precision. Businesses such as manufacturers and dealers are significant contributors to this system. Manufacturers can improve their brand image by contributing to this project. Currently, dealers are under obligation to check whether customers have insurance for the vehicles they are buying or leasing. This check is highly dependent on manual steps and paper-based communication. Adoption of the new blockchain solution will eliminate the need for unnecessary risk of information gathering through manual channels. Moreover, in the future, businesses can significantly benefit from product-based telematics. Service reminders and performance monitoring of the vehicles are some of the possible use cases for this information.

Insurance companies have several benefits to their business due to the quality of data collected with the blockchain. First of all, preventing insurance fraud translates to more business for the insurance companies. Removal of pink slips and all other manual forms of communicating the insurance information not only will save from paper mailing services, but also collect reliable information in case of incidents. Insurance customers will get better service by using the electronic communication and sharing of information. The blockchain will record all relevant events. Stakeholders can use some of this information in the future for determining promotions and pricing.

Government agencies are another set of contributors to the system as they can collect reliable information quickly by using the technology. Governments mostly depend on voluntary

data delivered to them. For example, during the license sticker renewal, drivers voluntarily provide their insurance details such as the insurance company and policy number. The blockchain can significantly improve the quality of such data where governments receive the same information directly from the blockchain without the risk of mistyping. Lawyers can also be participants of this blockchain. They can use the ledger information in case of a dispute.

3.5.5. Platform

Since we need separate roles for participants of the blockchain network, a permissioned blockchain is a good fit for our problem. Therefore, we started designing a blockchain solution based on Hyperledger. Hyperledger is a product set of open source tools and libraries needed to form a blockchain. A blockchain project in Hyperledger consists of the following entities: “Insurance Record” and “Insurance Sharing Record”. Table 3 presents these entities with a representative set of attributes. In future projects, adding more attributes relevant to future use cases will improve the overall solution.

3.5.5.1. Assets

The main assets in this system will be the record of insurance and the sharing record of insurance. The insurance record will be the primary record in the blockchain representing the proof of insurance. Dealers will create this record at the time of car sales. VIN and vehicle specific details will be added to the record. Dealer will set the status as "Initialized" for this original record. Following this initial record, the driver will share this record with insurance companies by sharing the driver public key. Since the insurance company accesses blockchain records, they can locate and access all the insurance records that belong to this specific driver. Assuming the next step will be completing the sale of the insurance, the insurance company would enter fields related to the insurance business such as the “Insurance Company”, “Policy Number”, “Start Date” and “Expiry Date”. When any company issues new data into the system, related records have to have their signature to validate that an authorized participant issued this update. The sharing record of insurance is the record for the event of a driver sharing her insurance information with another party. This typically happens when there is an accident and proof of insurance is to be shared.

Table 3- Assets and Attributes in the Vehicle Blockchain

Asset Name	**Attributes**
Insurance Record	Insurance Company, Policy Number, Driver Public Key, Status, Start Date, Expiry Date, VIN, Make, Model, Year, Dealer Signature, Insurance Company Signature
Insurance Sharing Record	Driver Public Key, Shared-With Key, Incident Code, Expiry Date

3.5.5.2. Smart contracts and automation

One of the most significant features of the blockchain networks is automated processing through smart contracts. As much as the blockchains are used to store transactions, they can be used to create contracts to produce transactions in the network.

There can be several use cases for smart contracts. Smart contracts can help execute manufacturer recalls for each vehicle. A user interface can display this information to the vehicle. The vehicle owner/driver may respond to this with decisions. All actions would be recorded on the blockchain to be tamper-free. There can be no denial of the interaction and responses.

Thanks to cryptocurrencies and other financial advancements in the blockchain technology, even insurance payments can be managed on the blockchain. There can be smart contracts that create a payment depending on the vehicle's usage statistics and driver's performance that month. The driver should be able to accept and execute such contracts from the user interface provided by the car.

Table 4 lists the transactions. From this list of transactions, the insurance expiry event is the only one that can be automated with smart contracts by our blockchain solution.

Table 4- Transactions in the Vehicle Blockchain

Transaction Name	**Description**
Insurance Creation Event	A new insurance record is requested. Identification information for the car would be recorded. Status will be "Initialized"
Insurance Creation Event	Insurance company completes the preparation of insurance. New information such as policy number, start and end date are added. Status will be "Active"
Insurance Expiry Event	Expiry date specified for an insurance record has passed. A record will be created with Status = "Expired"
Insurance Information Shared	Owner of an insurance record provided permission to share this record with another participant.

3.5.5.3. Interactions

3.5.5.3.1. Purchase of a vehicle

Purchasing a new vehicle is a use case that includes several manual interactions. After a driver decides to buy a vehicle, she needs to collect the information and communicate with an insurance company to purchase insurance for the vehicle. With the insurance information, the driver contacts the dealer in order to complete the purchase. All these steps and possible errors on the phone calls can be replaced with the following flow in Figure 31

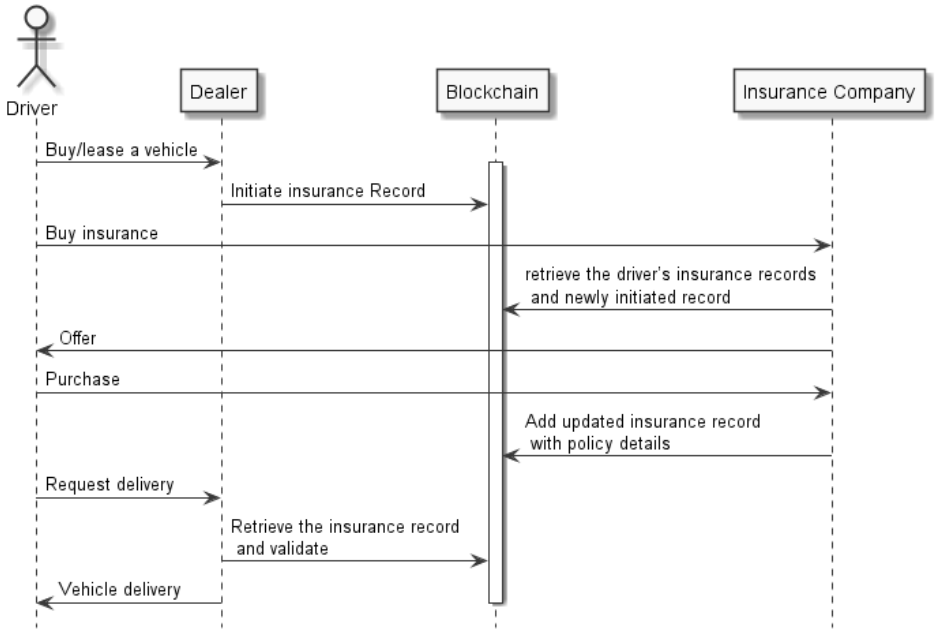


Figure 31- Sequence of steps while purchasing/leasing a new vehicle

3.5.5.3.2. After an accident

One of the main use cases regarding multiple untrusting parties is the motor vehicle accident use case. When a small accident happens, drivers are supposed to exchange proof of insurance documents (pink slips), and contact their insurance with information they collected. They typically need to spell several coded information on the phone with their insurance company. The following flow in Figure 32 replaces this manual data transfer and related errors with a blockchain-based flow.

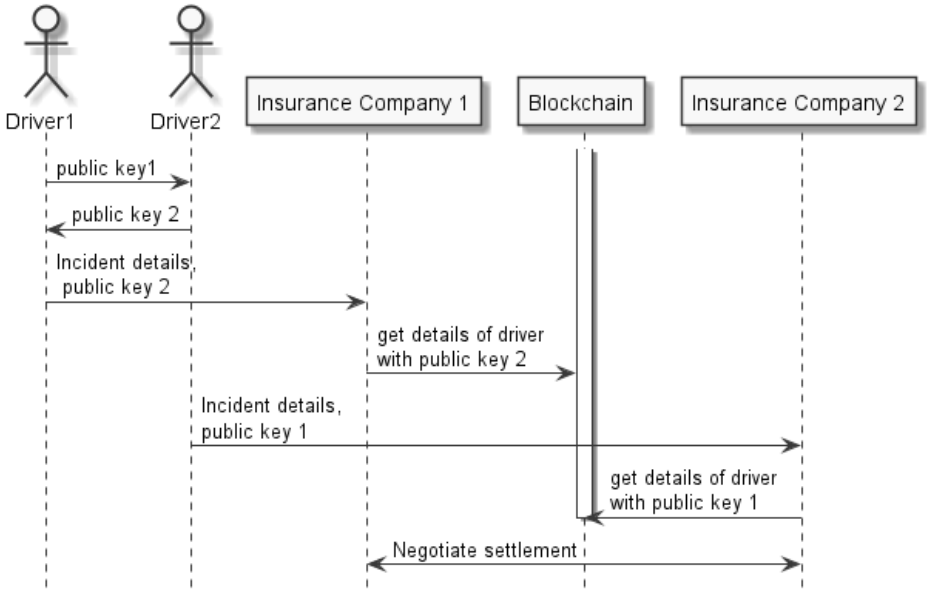


Figure 32- Sequence of steps happening after an accident

3.5.5.3.3. Police control

A convenience feature of the new blockchain system will be sharing documents with all interested parties such as the police. When a vehicle is pulled over and the proof of insurance is requested, the driver can let the police officer access the document with a key as depicted in Figure 33.

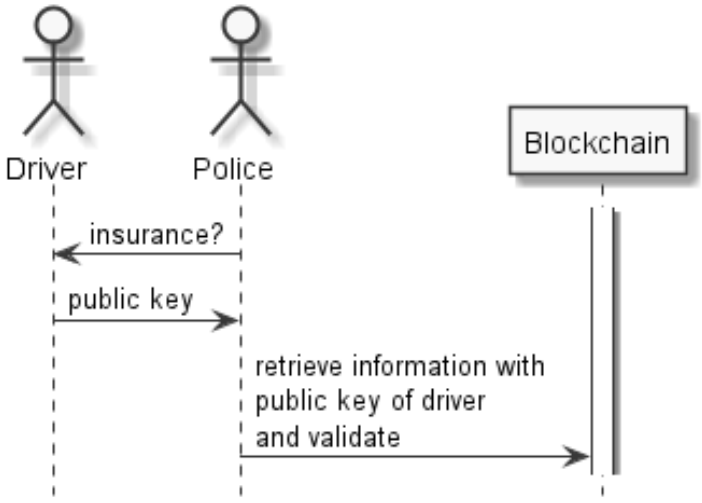


Figure 33- Sequence of steps during a police control

3.5.6. Challenges

Blockchain systems are enablers, but they are not the solution to all problems. There can be more than one blockchain-based solution to solve a single problem. Once the blockchain application satisfies the business requirements, we should investigate if the blockchain solution is a fit for non-functional requirements as well. We can decide on the suitability of the solution after the analysis of the issues. Below are some of the significant issues.

3.5.6.1. Collaboration

Blockchain systems can only provide benefits to participants who are collaborating. Even for a simple data collection and communication application, parties need to agree on the fundamentals of the blockchain. The structure of records, roles and responsibilities are some common fundamentals that are worth focusing on at the beginning.

Each party would assess the benefits of the platform and decide what the value for themselves and their customers is. There may not be enough motivation for collaboration due to unproven benefits in a simple use case. However, blockchains provide mutual benefits and long-term potential. Most players who only comply with the standards enforced by the governments may now be tempted to join the collaboration. Most participants will find the incentives around increased information flow. Transparency would enable them to create cost savings, prevent forgery, increase reliability and reduce inefficiencies. Such benefits will convince participants to maintain the decentralized system. At the times of conflict, blockchain will provide evidence for the resolution. Parties of the conflict will benefit from reduced timelines and increased accuracy of justice.

This blockchain solution is probably the most secure data sharing solution that this industry has experienced before. Cryptography enables secure recording of all communication. Non-repudiation features may improve trust. Blockchains enable ground-breaking levels of sharing data. Participants that are realizing potential benefits would increasingly utilize this solution. Proper execution and better communication can solve collaboration issues.

Creating a new blockchain or utilizing an existing blockchain for a new solution requires participants to be knowledgeable about the potential benefits of a blockchain network. If the participation ratios cannot reach representative percentages, then the benefit of the blockchain may

not be realized. If enough individuals and corporations would not adopt the technology, it is not possible to see the advantages of sharing. If government agencies are not involved, it would be relatively hard to achieve collective advantages such as producing statistics to improve services.

We believe there are enough reasons for all these participants to adopt this solution. However, the cost of governance may discourage the creators. In the case of high costs being an obstacle, implementing a minimum viable product will prove the initial value of the solution.

Blockchain networks need governance. A consortium must define the rules of the blockchain operations. This consortium's primary task should be the safety of the blockchain operations. In case forming such a consortium is difficult, an incentive structure may help to pay developers and contributors for their service.

3.5.6.2. Data privacy and security

Our proposed network is a data sharing network, and the biggest concern of such a network is privacy. There will be several different categories of data that will be stored in the blockchain and can be accessed by participants.

Using a permissioned blockchain, participants can have access rights according to their roles in this network. Only vehicle dealerships can issue new vehicles. Only insurance companies can create insurance transactions and related smart contracts. There are several other roles and matching activities in this solution.

For personal data, there are several concerns. Most of these concerns are to be addressed by lawmakers. The transparency of blockchain networks can be established to the extent of the permissions from governments about the privacy of citizens. There would be concerns about whether the blockchain is sharing too much to create vulnerabilities for a malicious person to exploit. The participants can access any information on the blockchain. This level of sharing means one corrupted participant means all the information in the chain is available to a malicious third party. With this risk, we kept the amount of information on the chain to be at a minimum. We excluded all personal information about the drivers including their addresses although the address is a piece of information on the Ontario pink slips which would be exchanged with other drivers in case of accidents. In case this implementation can include more information without privacy

concerns, some of the driver's personally identifiable information would be useful to store in the chain.

Finally, our system is operating with the public keys of the drivers in order to protect their identity. Another way to add more anonymity is for the driver to use a different key-pairs to record each type of data. This way it would not be clear whether one driver or many drivers have all these blockchain transactions. When the driver decides to share the data and want the recipient to link the identities, she will share the set of certificates or public keys. Where public keys are not enough for maintaining privacy, advanced cryptographic techniques such as zero knowledge proofs and bilinear pairings must be used to safeguard privacy.

3.5.6.3. Transaction fees

Creating the blockchain and maintaining the operations have costs. Pricing is an essential factor in the promotion of the proposed solutions. Currently, Bitcoin network transaction fees are so high that an ecosystem that depends on the Bitcoin network would pay high prices for executing a high volume of transactions. Altcoins are focusing on lower transaction fees, but the capabilities and reliability of these altcoin networks may not be as high as Bitcoin or Ethereum.

An alternative solution to the issues at the typical public networks is to create a custom network. For the systemic requirements around a custom network, there must be some incentives for the participants to get involved. In public blockchain implementations, participants need to handle blockchain operational tasks such as creating a new block.

In case the new block creation duty is given to a specific set of participants, there should be measures to prevent any misuse of this power.

3.5.6.4. Scalability issues

The blockchain technology has a well-known scalability problem. Several sources [255] [82] are indicating this as the most significant risk facing the widely accepted blockchain implementations. There are several research projects and advancements in this area.

The solution to the performance requirements can be enhancements like the "lightning network." The lightning network typically records the transaction off the chain until the termination of the channel. The lightning network concept is a proposed solution for the bitcoin blockchain in order to keep the volume down, filter the unnecessary recordings, and therefore

increase the capacity through increasing throughput. The lightning network suggests to use the main blockchain not for every transaction but for the summary. It is similar to recording the transactions at the local repository of the "Segregated Witness" and having period-end reconciliation with the main blockchain [88].

Vehicle-related transactions can utilize this approach for vehicle-related transactions in order to decrease the volume and cost of transactions. Bitcoin can process about five transactions per second; the lightning network can process more than thousand transactions per second and as a comparison, the transaction giant Visa network can process 56K/sec [88].

For permissioned networks, the scalability issues are less significant. As the network has roles and not all roles are available to each participant, consensus operations do not take a long time. Especially when selected participants are assigned to the block creation task, the performance of the network increases. As decentralization increases, performance decreases. Blockchain solutions cannot be compared with any centralized solution as centralized solutions do not operate under trust-seeking environments, but rather use the authority of the centralized system to decide without delay. Permissioned networks are the closest to this model by providing the trust to defined roles. By assigning roles, the solution will have a minimum burden of consensus-seeking.

3.5.7. Conclusion

There are several use cases of blockchain technology in the vehicle industry. We have presented the variety, benefits, and issues of these solutions in a survey format in order to understand the industry as well as the blockchain adoption. Blockchain technology facilitates better service where all participants need a transparent and accessible environment to share information.

Our contribution is the new use case for creating a vehicle insurance ledger using blockchain to share the vehicle insurance records. We also contribute the digital asset design, smart contract automation design and interaction design. We propose using blockchain technology to capture the details of the insurance where several actors are collaborating, and several stakeholders are depending on. We provide details on how participants can benefit from transparency with this scenario as well as how a blockchain can facilitate transparency. Through this solution, we show

that blockchain technology can be used as a communication medium between otherwise untrusting parties.

A future direction for our research would be the connected cars and telematics aspects of the auto industry. Connected cars will bring numerous opportunities to auto industry. The data collected will be beneficial for manufacturers, insurance, owners and governments. Insurance companies can take advantage of this technological front and start giving discounts to voluntarily provided reliable information. When a blockchain has the record, its tamper-free feature protects all parties. Insurance companies, individuals or any other third party cannot change the records once recorded. Since the records in a blockchain are persistent indefinitely, this system can be a perfect driving history to be used for years to come. Individuals can present their public keys or signature to a new insurance company to get better discounts. Young driver programs may consider the ledger to prove the maturity of the driver. Driver's license renewal can consider this history. It can be transferable between states to aid license exchange in case the owner moves to another state. In further cases, the records can assist the court in cases related to the behavior pattern of the drivers. The same blockchain can be used to record alcohol levels of the driver with proper accessories provided. A further use-case would be recording full event logs including details like breaking and signaling behavior for further analysis. We believe all these new features can be developed on top of our current implementation of the insurance record blockchain.

4. Main Challenge: Blockchain-Based Aid Delivery

After developing the solution framework, the financial evaluation framework and the security/automation analysis, we could answer the research questions on how blockchain implementations can be successful, cost-effective and secure. We also conducted analysis and blockchain-based design in disaster recovery and vehicle themed use cases.

Our next steps in the research is to design a general delivery assurance framework for modelling blockchain-based delivery assurance. In this section, we present our work that provides guidance on how blockchain technology can be used to implement delivery assurance applications. After detailing the delivery assurance framework, we continue with the application we adopt to demonstrate and validate our framework related to blockchain-based aid delivery. We conclude this section with the details of our experiment and validation. Contributions to our research program described in this section correspond to the items circled in red in the figure below.

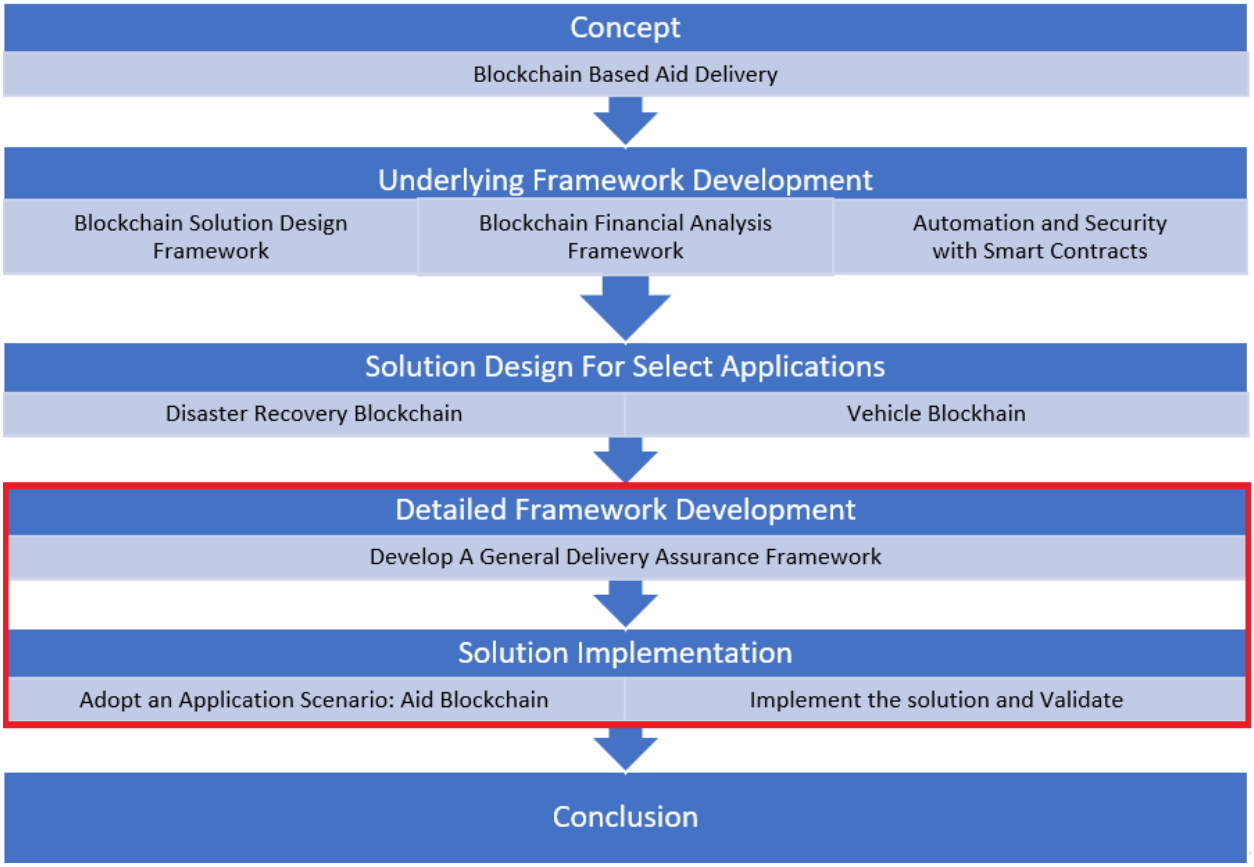


Figure 34- Research program - Detailed framework development and experimentation

Our central contribution is a blockchain-based delivery assurance framework. Blockchain and IoT Delivery Assurance on Supply chain framework (BIDAS) provides guidance to build blockchain solutions to be used in a variety of applications concerning delivery systems to record delivery events. BIDAS not only records the delivery contact between the delivery service provider and the receiver, but also is able to record the events happening to the package along the delivery path.

Advances in IoT enable a wide variety of sensors to be placed in to monitor everything from the temperature to velocity and acceleration. All this data can be communicated in near real-time with the anticipated advances in wireless technologies such as 5G. The BIDAS framework guides the audience to create blockchain systems as a medium to combine conventional techniques and these new technologies. In order to show the information asymmetry in the light of IoT technologies, BIDAS models the agency theory as in the following figure.

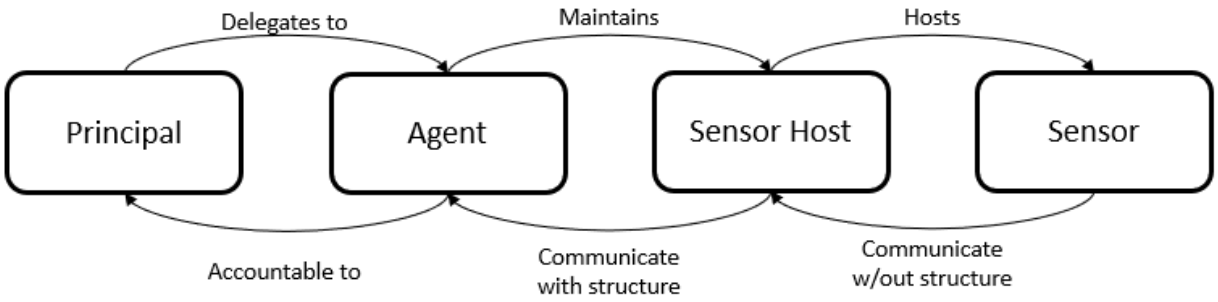


Figure 35- Principal-Agent-Sensor Host-Sensor model of BIDAS

BIDAS forms the backbone of our work towards blockchain-based aid delivery and guided us with the steps and principles to apply blockchain technology to the delivery industry. Findings in this study include the techniques to model a delivery business as a blockchain implementation and the role blockchain can play in providing proof for the delivery events.

We adopted an aid delivery application to validate our delivery assurance framework. Blockchain-based Aid Delivery Assurance (BADA) application is a complete reflection of the various findings in previous sections of this thesis. It is a disaster relief application, including vehicle interaction and delivery assurance. This application is defined with BTTF and designed with BIDAS. By adopting this application, we demonstrated the possibility to deliver aid and use the assurance model of blockchain technology to improve aid delivery service. We finally developed a blockchain system to test the validity of our delivery assurance framework and aid delivery solution. Not only did we construct the system, but we also tested its performance.

In this section, the following research questions are addressed.

Research Question	**Addressed by**
How can we apply blockchain technology to the delivery industry? What are the techniques to model delivery business as a blockchain and what are steps of this process? What role blockchain play in providing assurance of delivery?	BIDAS
Is it possible to deliver aid and use the assurance model of the blockchain technology to improve this service?	BADA

Figure 36- Research questions addressed in Chapter 4

4.1. Blockchain-Based Delivery Assurance Framework

The centerpiece of our research is a blockchain-based delivery assurance framework. Blockchain and IoT Delivery Assurance on Supply chain framework (BIDAS) provides guidance to build blockchain solutions to be used in a variety of applications concerning delivery systems to record delivery events. BIDAS not only records the delivery contact between the delivery service provider and the receiver but also is able to record the events happening to the package along the delivery path.

BIDAS not only considers delivery operation as human operated handover tasks but also as a network of sensors monitoring everything from the temperature to velocity and acceleration. BIDAS assumes that the near real-time flow of this information into a blockchain systems helps resolve information asymmetry in the classical agency theory.

This chapter is submitted, accepted and published [7]. © 2019 IEEE. Reprinted, with permission, from M. Demir, O. Turetken and A. Ferworn, " Blockchain and IoT for Delivery Assurance on Supply Chain (BIDAS)," in *IEEE Big Data 2019- IoT Big Data and Blockchain (IoTBB'2019)* , Los Angeles, California, 2019

4.1.1. Introduction

The supply chain industry has been focusing on blockchain research due to the structure of the industry where conducting business requires numerous contacts and handovers. This interest resulted in the existing literature to mainly focus on the handover of the goods with RFID tags scanned by the agents of the supply chain infrastructure. These events are typically recorded in the blockchain to be shared with all the partners. This sharing scheme is commonly designed to take advantage of the similarities between a shared database and a blockchain. Implementations typically use permissioned blockchains or a hybrid solution of permissioned blockchains with a public blockchain due to the privacy requirements of the businesses.

The scope of this paper is a subsection in the supply chain business context with a specific focus on what is called "the last mile." The last mile is the final task in the delivery process, at which point, delivery is marked as completed. Business processes assume the ownership of the

deliverable is transferred to the client when goods are handed to the client or its representative or left at their property. Last-mile is often considered to be a costly section of the overall delivery process [256] as it is often the least efficient link in the supply chain, reaching up to be 28 percent of the total cost of the delivery [257].

Since improvement in delivery performance is a competitive advantage [258], several new approaches to deliveries are introduced or are being researched. Autonomous Unmanned Aerial Vehicles (UAV) [259] [260] and land vehicles [261] [262] are under development as emerging alternatives to conventional delivery methods. New methods also include robotic mobile store experience, which delivers many products to the customer and lets the customer choose which product to keep [263].

Delivery methods are not the only aspect of the industry that is under constant improvement. Delivery companies decorate deliverables with better tools and technologies to closely monitor the process. Besides conventional RFID tagged packages, smart packages with condition monitoring systems are emerging [264]. Condition monitoring systems [265] are collections of electronic sensors that monitor a variety of environmental conditions related to an asset and aid overall reliability of the delivery of this asset. Vibrations, acceleration, temperature, humidity, acoustics, and global positioning are some of the conditions that deliverables are subject to in the delivery process.

Traditional supply-chain industry has been utilizing RFID based IoT operations successfully in collecting sensor information under the governance of centralized authorities. Blockchain technology comes to the rescue when the centralized authority is not sufficient to cover all aspects of the business. When parties with conflicting interests collaborate in a business environment, they need to build trust for the smooth execution of the business transactions. It is typical that when the business goes as planned, there is no apparent need for intermediation; all parties conduct and continue their businesses within their tolerable margins. Yet, trust is critical in times of disagreement; when things do not go as expected, parties need proof, they need a reliable, untampered, and undeniable record of data related to the transaction in doubt. Blockchain technology provides this trust.

Besides its classic benefits, blockchain technology offers solutions to two main problems in the delivery industry. These are “Chain of custody throughout the handover of packages” and “Continuous monitoring”.

Chain of custody is a problem when multiple parties conduct business indirectly through the interaction of their representatives, proxies or agents. These interactions, mainly the handover of packages between independent parties have a security and trust issue. Lack of chronological documentation or paper trail recording the sequence of custody and handovers with sufficient physical or electronic evidence, feeds the issue. This trust issue cost companies in the form of business loss or as expenses such as insurance fees due to difficulties in finding responsible entities for a harm that occurs at an unknown time.

As depicted in Figure 37, delivery transactions start with an initiator. The initiator can be the sender of the packages or a last-mile delivery company who happens to be the first entity that has access to electronic systems that is equipped with IoT sensors that can prove the initiation of the delivery task. The package travels to the receiver who can also be called the receiver of the services as this entity is the receiver of the delivery service. So, the last entity that can be associated with the delivery is the receiver. In this conventional model of communication, while the package is on its way, information related to the business context of the delivery passes through several intermediaries towards the receiver (1 to 6) and through the same intermediaries back to the initiator (6-10). The meaning and time-value of the information depreciate as the information goes through an increasing number of nodes. Accurate information does not reach the stakeholders on time, and it often arrives indirectly. There are risks related to malicious censorship. Indirect stakeholders of the process receive information from multiple parties. It is then costly to filter and merge the information in order to find the truth to be used in business or conflict resolution.

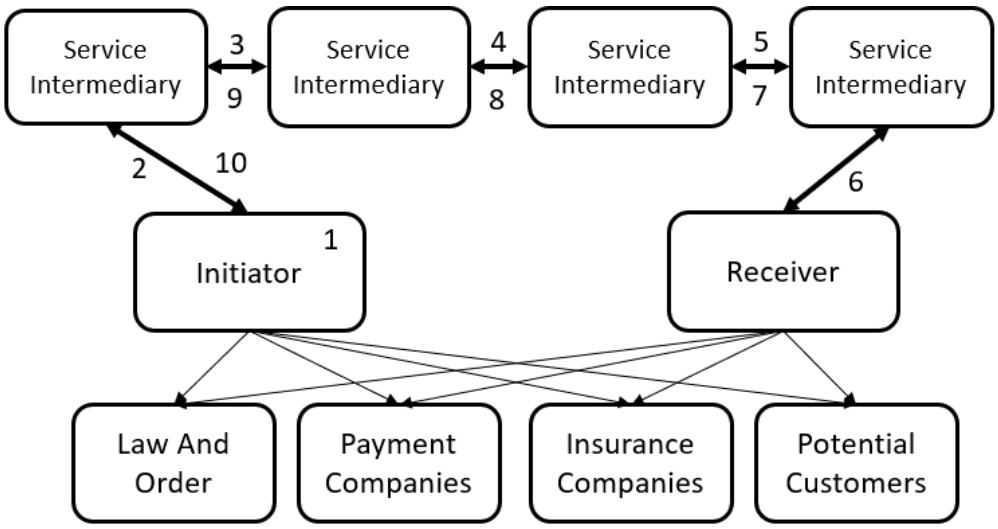


Figure 37- Information flow from delivery initiation to completion

The continuous monitoring problem originates from the traditional data centric IoT application model built with the intention to monitor systems in detail. Advances in the IoT technology made the collection of data possible, but the systems architecture to process the collected data did not advance equally. A broad set of devices collects large volumes of data that needs to be processed and preserved with its original quality. Most delivery vehicles today carry GPS sensors and other telemetry capturing sensors providing high resolution data [266]. Conventional IoT support systems process this data by centralized analytics applications that have a high processing power. Recent advances introduced parallelism to the processing logic. Parallelism such as big data increased the capacity and throughput, however this parallelism took a derivative of the data by stripping its detailed attributes that have the most value related to trust. The lack of trust in the individual devices and security issues have decreased the range of functions that these devices can execute. Blockchain technology is a gateway to more capable IoT systems. Otherwise untrusting parties can cooperate by quality record collection, processing and keeping [27].

There are several similar ideas on the Internet and literature indicating that blockchain technology will revolutionize the delivery industry [267] [268] [269] [270] [271]. These articles also emphasize that a cryptocurrency [272] [273] for delivery business would be successful. However, current work [143] does not provide a framework for solving delivery problems on a structured platform. Instead the focus is on the benefits of the technology and opportunities that it presents [274] [275].

In what follows, we present a literature survey of blockchain applications in the IoT field. This survey highlights the importance of trust and the leading use cases of the blockchain technology in IoT. Following that, we present our framework to solve the above-mentioned delivery industry issues by modeling the delivery blockchain that consists of data from stakeholders, system actors, and IoT sensors. Our framework considers the participants, data models, and interactions. We also present a use case to discuss the framework. We present the details of the design and the benefits of such a solution that follows this framework. We conclude this paper with the critical lessons learned and future directions of our research.

4.1.2. Blockchain Technology Review

A distributed ledger is a system with rules around keeping and sharing data between participants of a network while synchronizing, validating, and keeping the integrity of the information. This shared set of data can be stored and modified in the system. There are live examples of distributed ledgers for discovery services [276], virtual server management services [277], and financial services [35].

Blockchain technology is a type of a distributed ledger that fulfills the reliability promise by chaining the blocks of transactions based on their hash values. By placing the hash of each block into the content of the next block, the system connects the blocks and forms a chain. Even if malevolent parties complete this expensive operation, distributed ledger implementations require consensus to accept the new blocks. Changes in the old blocks would be detected through the comparison with the local copies of the distributed ledger and rejected by other nodes in the network.

Bitcoin, as the first mainstream implementation of the blockchain technology, demonstrated to the world that cryptographic techniques combined with high volumes of participation could create a ledger environment where all parties witness and validate all records. This pattern of record-keeping inspired several solutions in digital exchanges where goods and payments are transferred electronically.

The blockchain concept is not new anymore and using blockchains is seen as a disruptor for all industries [260] around the world. Blockchain technology acts as a trusted agent between

otherwise untrusting parties. With these characteristics, blockchain applications are widely used to integrate businesses and individuals.

Blockchain implementations can vary on participation. Public blockchains enable anonymous participation of members and transparent sharing of all information. This level of participation and transparency is not suitable for all applications. Permissioned blockchains limit the participation and block creation authorities to the designated parties. There are several hybrid blockchains for handling other varieties.

Blockchain providers have met the demand in terms of requirements and flexibility. Especially since the blockchain technology is a comprehensive technology that empowers small players around the globe and gives them an opportunity to participate, global interest in the application of the technology has soared.

4.1.3. The synergy between IoT and Blockchain Technology

Internet of Things (IoT) is the network and ecosystem of devices that collect and share data. IoT networks typically are formed by numerous interconnected devices that are the service provider-consumer interfaces between humans, technology, and organizations [278]. With the perception capabilities of sensor networks, the IoT universe has an excellent detection capability. The environment data such as location, motion, temperature, and acceleration that are collected by sensor units is an invaluable means by which the digital world understands the physical world. Near Field Communication (NFC) devices, Radio Frequency Identifier (RFID) devices, wireless sensors, and mobile phones are standard tools of today's capable IoT ecosystems. IoT networks have the potential to automate a significant number of manual tasks and improve human life [279].

This network of billions of devices demands more of everything. Network bandwidths are increasing to enable a higher volume of communication. Wireless technologies and networking are increasing their coverage to include more participants. IoT infrastructure components are connecting devices to collect a massive amount of high-quality data and to provide further intelligent services. There are several architectures proposed for IoT in order to solve its communication issues. Some of the standard layers include a sensing layer for sensors, networking for connecting the sensors, and a service layer for providing interfaces for clients to integrate into

a network of sensors [280]. Most application integration is centralized at the middleware layers [281] and exposed to tampering by malicious entities.

IBM predicts winners of the IoT technologies will be those who can decentralize peer-to-peer systems and can lower costs. The winning choice would be privacy and long-term sustainability instead of full control of data [282].

Several other challenges in the IoT world can be solved with the collaboration of parties. A good example is how a peer can provide a solution to a device to upgrade its firmware after the manufacturer disconnects the necessary service [283]. Discovery services about the correct firmware file and the conditions to receive such service can be made available with smart contracts which are a feature of blockchain technology.

Decision-making mechanisms based on peer-to-peer networking is essential for IoT. Central trust figures or authorities are not available for every network, and they can be a bottleneck to the overall network where they exist. A community of peers in the form of a peer-to-peer network fulfills this requirement where all decisions are made collectively, and unilateral choices are prevented [278]. Since devices on the Internet will have to act independently, and have to carry their operations individually, peer to peer solutions are essential for IoT adoption.

Condition monitoring systems have a fundamental role in active IoT space [265]. These systems formed as a collection of electronic sensors monitor environmental conditions related to an asset. Even though the global positioning of an asset is the most important information for the supply chain processes, depending on the nature of the deliverable, the data collected about the environmental conditions of the deliverable can be substantial through the delivery process. Fragile or perishable assets can be monitored for vibrations, acceleration, temperature, humidity, and even acoustics. Sensing of unpredictable conditions and automatic recording of this information on a blockchain will be an added benefit of IoT towards better delivery systems [284].

IoT architectures benefit from decentralization since there are high numbers of nodes in these systems and scalability often requires independent operation of devices while producing collective value. Devices in the IoT systems interact with each other and this large-scale interaction can benefit from the injection of trust created with the introduction of a blockchain. Considering the delivery businesses are introducing autonomous vehicles and other non human agents to their business model [285], it is important that blockchain technology certifies that the gathered sensor

data is original and not tampered. This promise of the blockchain technology would make IoT networks a trusted agent in business transactions. When a business event or a monitoring event occurs, IoT sensors detect the event; blockchain technology lets the entities share and use this information. This ability to access the original information brings trust to the interaction, and otherwise untrusting parties can do business together.

Each IoT device may not be a full blockchain node [286]. Each node may not have the processing capacity or data storage capacity to be involved fully. However, they can be sending messages to the blockchain network through their network connection. They can also receive the summary of the related communication with the help of smart home centres.

4.1.4. Blockchain & IoT for Delivery Assurance on Supply Chain (BIDAS) Framework

Supply chain industry has numerous opportunities with the emerging blockchain revolution. In this research, we study a growing segment of the supply chain space named the parcel delivery industry [287]. Our novel contribution to the supply chain industry is the definition of a framework that guides the structure of the blockchain implementations in delivery operations of the supply chain industry.

Parcel delivery is especially a good business area to focus as an increasing percentage of customers are ready to pay more for improved delivery service [285]. This business area is also the most open to new technologies. McKinsey is expecting 80 percent of all deliveries to be completed by autonomous vehicles, including drones [285] in the next ten years.

We targeted delivery operations since we believe this business area can be improved. From the cost perspective, the technology is, and will be, reducing costs compared to the cost of labor for the same amount of work. Scalability and availability of autonomous resources are, and will be, higher. Autonomous options are ready to change the industry entirely as they can deliver 24/7; without a holiday, a weekend break, labor law restrictions or a strike to slow things down.

In order to solve the information flow problems and aid other supporting business processes, we propose a blockchain and IoT delivery assurance on supply chain framework (BIDAS). Our framework targets delivery problems identified earlier in the paper. When a delivery ecosystem is being built, we recommend using our framework as a guideline to define, describe

and implement the blockchain solution. Following the steps depicted in Figure 38, delivery operations can benefit from the blockchain revolution.

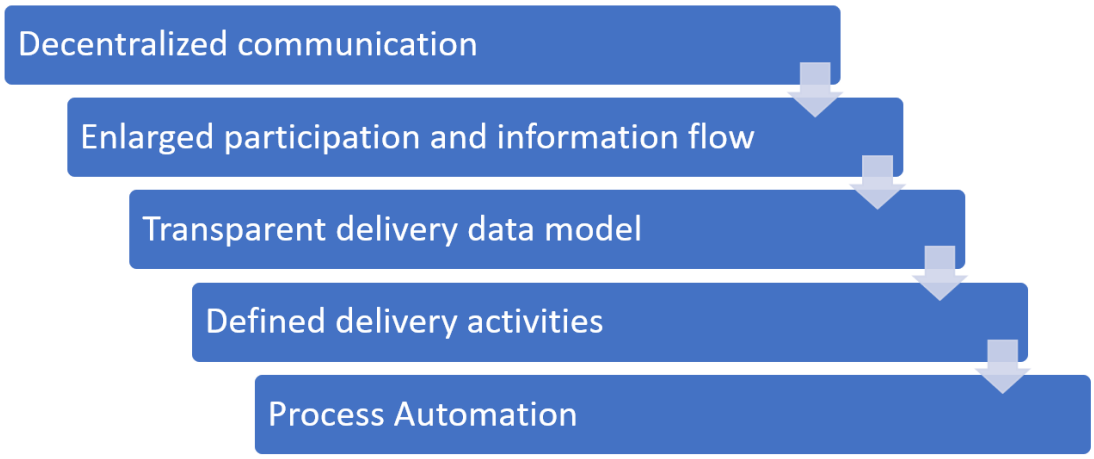


Figure 38- BIDAS framework recommended steps for delivery assurance

4.1.4.1. A decentralized model of business

BIDAS advocates replacing centralized information flow with the decentralized architecture of blockchain systems as depicted in Figure 39. BIDAS fully involves all the service intermediaries hired in the process as well as the passive beneficiary stakeholders. All stakeholders become blockchain network participants. They benefit from transparency and support the system by their active involvement. BIDAS is not only a blockchain framework. Decentralization alone is very beneficial to existing business models.

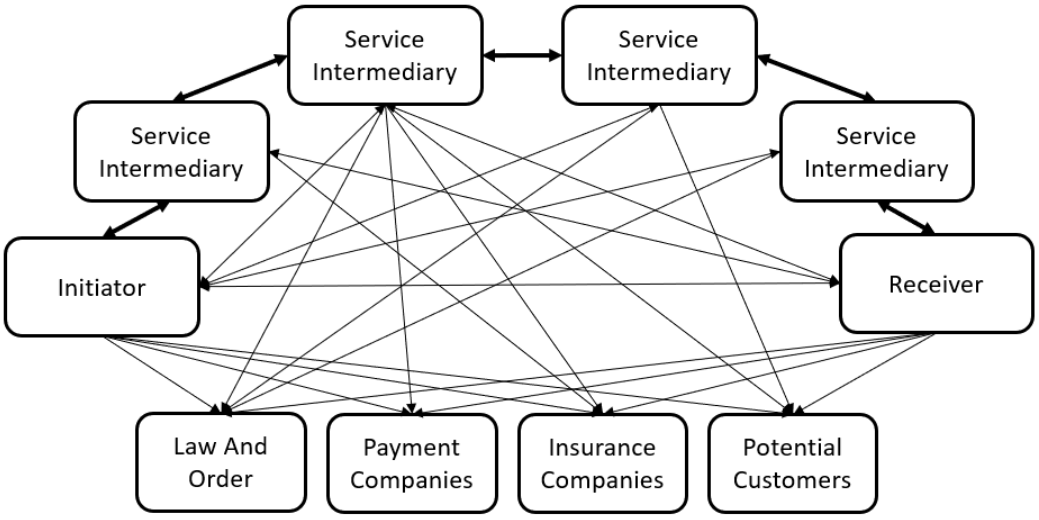


Figure 39- Information flow with BIDAS

4.1.4.2. Participants and information flow

Agency theory identifies uniform information flow as an important aspect of successful business interactions [288]. Asymmetric information prevents best possible outcome to be achieved and results in losses named ‘agency loss’ [289]. Principals and agents in conflict of interest are common in supply chain industry [290]. Despite being expensive with conventional methods, monitoring had been part of solution towards closing the gap of information [291]. BIDAS applies the agency theory and aids the solution of information asymmetry with reliable monitoring using the permanent records of the blockchain.

In BIDAS, principal is the actor that assumes ownership and responsibility of the delivery. Ownership and responsibility are assumed with providing a commitment or when the goods enter its custody. A person or a non-person entity can be principal. A principal assumes the responsibility of the handover actions as part of delivery business directly or through its agents. BIDAS especially focuses on the IoT based delivery businesses. Therefore, agents in BIDAS can be a wide variety of sensors. Beside sensors, infrastructure that hosts the sensors can also be agents.

BIDAS models the interactions as depicted in Figure 41. Delivery models start from a role named initiator. An initiator is usually the creator of the delivery task. Typical examples are an online bookstore or a delivery company receiving a package in one of their stores. From this point on, the delivery operations are a series of handovers where one party hands the package to the next until the package is delivered to its final destination. BIDAS addresses the first problem in the delivery business that we listed above with the label "Handover of packages". The main concern in the handover of packages is the chain of custody. Chronological documentation of electronic evidence is a must for delivery businesses [292]. Blockchain does this evidence collection in a democratic network and on an immutable ledger. The second role in the systems is for the system intermediaries, which are actors in the delivery business that transport the packages towards the destination. BIDAS models the communication flow between the initiator and service intermediaries.

Table 5- List of Roles in Package Delivery Handover

Party Type	**Initiator**	**Service Intermediary**	**Receiver**
Principal	Initiator	Service Intermediary	Receiver
Actor/Agent	Initiator Actor/Agent	Service Intermediary Actor/Agent	Receiver Actor/Agent
Sensor	Initiator Sensor	Service Intermediary Sensor	Receiver's Sensor
Sensor Host	Initiator Sensor Host	Service Intermediary Sensor Host	Receiver's Sensor Host

BIDAS also assumes there can be several layers of intermediaries where some portion of the transportation or delivery business is outsourced to other service intermediaries. The last type of actor in the BIDAS interaction model is the receiver. This role can be assigned to a customer that orders a book or food or any other material for delivery. This actor is the last node in the system. When the goods are delivered to the customer, or in other words, the last interaction between the last server intermediary and the receiver happens, the delivery process is marked as completed. The package delivery handover roles template is listed in Table 5.

For each delivery service stakeholder, there are multiple types of parties. These parties represent different types of actors that are involved in handover interactions. Each delivery service stakeholder has principals and their agents. Beside the principal and agent of agency theory, IoT adds sensor devices that detect and respond to conditions and changes in an environment [293]. In the delivery scenario, sensors can be RFID devices, GPS, thermometers, barcode scanners, microphones and video cameras. Sensor host is an actor that is a structure, device or vehicle such as a building door, vehicles, robots, UAVs, cashier station or warehouse. These four types of actors in the same delivery service stakeholder has relationships as in Figure 40.

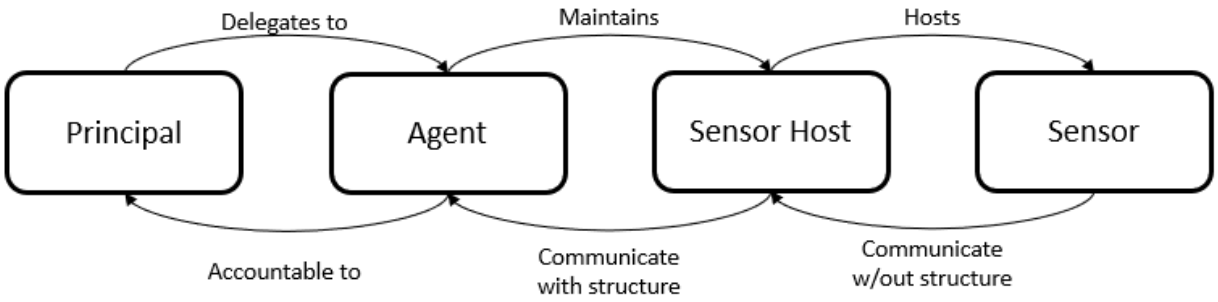


Figure 40- Principal-Agent-Sensor Host-Sensor model of BIDAS

Even though BIDAS provides guidelines to model the communication on the blockchain architecture, handover problems can be solved by modeling business interactions that are depicted in Figure 41.

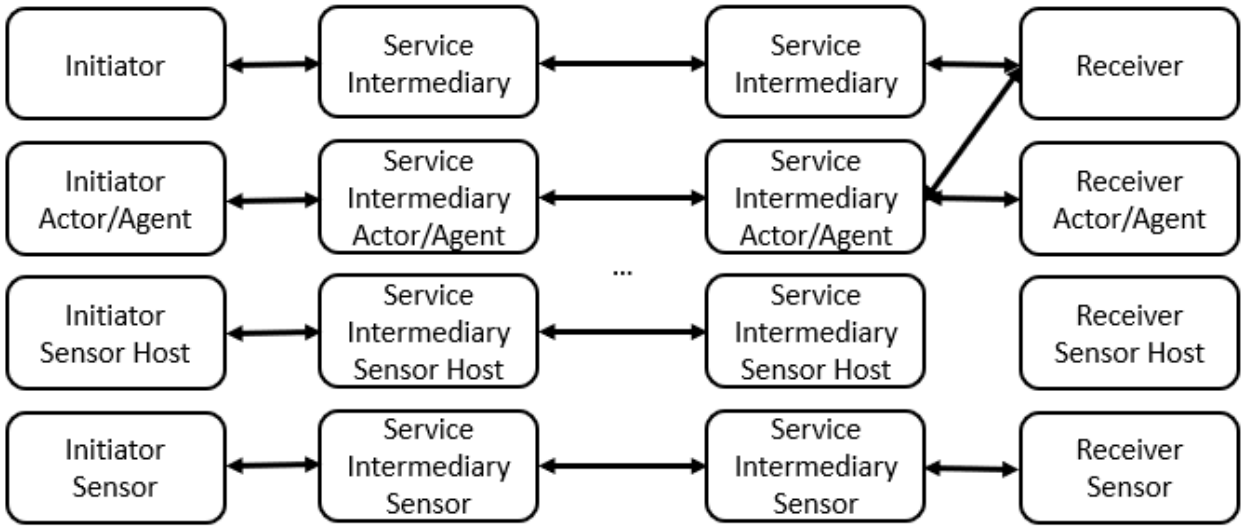


Figure 41- The BIDAS business interactions model

4.1.4.3. Data model

A blockchain-based process is like any other process in terms of modeling the data. Blockchains can be modeled similar to databases where structured or unstructured data are stored. Due to the extended amount of communication, blockchains tend to have a minimum amount of data. Single-purpose blockchains such as cryptocurrencies prefer structured data as the validation of the transactions require all information encapsulated in a transaction to be well understood. For business transaction blockchain implementations, unstructured data is acceptable and expected as the business information tends to vary and evolve.

BIDAS is not restrictive on the data model. Conventional delivery data entities such as Order, Order Item, Delivery Item and Receiver are to be used on the new blockchain-based data communication layer of BIDAS. There are already existing data standards and delivery data model samples [294] [295] [296] [297] [298]. The amount of data to be shared depends on the implementation. There are several privacy concerns about the maximum transparency a blockchain ecosystem can provide. For example, when the receiver information is openly communicated in the blockchain network, all members receive the details. Implementation of a delivery system must have an identity and consent system built-in in order to share the customer information only with the parties that the customer provides consent for.

All sensitive data will be represented in JSON-LD lightweight linked data standard [299]. It is easy to read and write. It uses Json structure. It has a general compliance with RESTful services, and unstructured databases.

Some entities we have defined in BIDAS include Receiver, Order, Order Item, Payment, Invoice, Deliverable, Delivery, Delivery Stage, Delivery Event, Delivery Schedule, Contact Event, Agents (Employees), Sensor Hosts, Sensors and Sensor Events. All Items have their identifiers. Beside the identifiers main attributes for each entity is listed in Table 6.

Table 6- List of Primary Entities

Entity Name	**Attributes**
Receiver	Id, Status, Contact Details, Delivery Destination Details, Coordinates
Supplier	Id, Contact Details, Shipment Contact Details, Customer Service Contact Details,
Order	Id, Order Items, Receiver
Order Item	Id, Amount, Price, Tax
Payment	Id, Amount, Method, Details (Number, Expiration, security Code, Reference Number), Timestamp
Invoice	Id, Total Price, Tax
Deliverable	Id, Packaging Type, Dimensions, Weight, Order Items
Delivery	Id, ETA, Tracking ID, Deliverable
Delivery Stage	Delivery State and Status
Delivery Event	Receiver, Receiver Agent, Receiver Sensor Host, Receiver Sensor, Contact Event
Delivery Schedule	Delivery, Time Period, Date
Contact Event	Image, Signature
Agents (Employees)	Agent Id, Title, Salutation, Given Name, Family Name, Gender, Birth Date, Contact Details
Sensor Hosts	Id, Receiver, Sensors, Contact Details, Serial Number
Sensors	RFID, UID, Serial Number
Sensor Event	Sensor, Latitude, Longitude, Altitude, Latitude Direction, Longitude direction, Altitude direction, Temperature, Pressure, Acceleration, Noise

The Receiver entity describes the last entity that is involved in the series of handovers. This entity is typically the terminal entity where we consider the delivery to be completed. Depending on the business scenario, this entity can be a customer or a building or simply GPS coordinates or an autonomous actor. This information can include identifier, image, or any other data that can be used to prove the delivery. Whether the receiver information is kept in the blockchain in detail or represented with identifiers is the choice of the developer. In case the information is kept off the chain, a resource URL should be included to access the customer information in case it is to be used by a stakeholder. For a delivery notification to be sent, contact details must be available to some stakeholders.

Delivery destination information is the contact destination for delivery completion. An address or coordinates can mark the delivery spot. JSON-LD would make sure the address can also be stored remotely if it needs to be kept confidential.

Order is the representation of a complete list of deliverables to be delivered to a customer that is organized or purchased under a single business transaction. An order may have multiple deliveries in case the items in the order are to be delivered separately.

If the blockchain is to be used as a platform to integrate sales and payment systems as well, these records will also be on the blockchain. Payment amount, currency type, payment instruments, and status will be stored. The monetary integration can be improved with smart contracts for managing the commissions and fees in the process.

Deliverable information is a list of package/product/service information that is part of the same delivery. All the deliverables included in the delivery can be stored in the blockchain either in detail or as a URL representing the item. Standardized handling instructions must be available for each item for all handlers to comply. These instructions also should be in the form of URLs or codes since such information would be highly redundant.

Delivery schedule data contains the timing details of the delivery. Timeframe information can be kept on the blockchain to let stakeholders know when the delivery is intended to be.

Delivery agents used to be the delivery company employee, national postal services worker, or a subcontractor. With autonomous vehicles as an alternative channel to distribute parcels and other deliveries, the agent concept also has a wider variety. Crowdsourcing of the tasks

also makes this role available to more [300]. The data representing the agent will be in the blockchain.

There are some general data considerations that every blockchain must address. Privacy requirements of the stakeholders and record-keeping options are part of our framework considerations. As already mentioned, several pieces of data can be kept off, but available to the blockchain in the form of URLs of identifiers. Record-keeping policies will be addressed with respect to the data storage policy. It is given that the data written to the blockchain is already disseminated to all stakeholders. If the data is kept off the chain, then the data governance will rely on the principal and storage of the data.

4.1.4.4. Activities and automation

Delivery systems modeled with BIDAS not only use the entities to store the information on the blockchain networks like a distributed database but also record the business activities. Activities that are a natural part of package delivery are listed in Table 7. Identifying and utilizing these activities is important since in the blockchain solution these activities map to smart contracts. This gives all stakeholders the ability to create contracts to automate their business processes.

The first type of interaction is the registration of entities other than delivery. Receivers, Receivers' receiving agents, providers, payment companies, delivery agents, and the delivery company can be registered to the system. This can be an upfront activity for larger entities such as providers and payment services, or it can be an on-demand activity for customers and their agents. We will not go into the details of these relatively straightforward activities.

The second type of activity is the operational entity creation, such as the creation of order, delivery request, and payment request. These are business activities that trigger further operations in our blockchain. The delivery event, delivery acceptance, and payment automation are the next category of activities that can be modeled.

Table 7- List of Activities in Package Delivery

Activity Name	**Description**
Registration	For each actor, a registration is needed to be for identification in the system
Create Order	Initiator creates an entity for delivery, order, set the status to order received
Delivery Status Change	Participants update the status of delivery such as shipped.
Observation Recorded	Sensors or sensor hosts records device readings and observations
Handover	Participants indicate that the package has changed hands
Return Delivery Item	Receiver or initiator changes the destination back to the return destination for the order
Cancel Delivery	Receiver or initiator changes the destination to the cancel destination for the order
Complete Delivery	Service provider of the last mile marks the delivery as complete.
Received Delivery	Receiver marks the delivery as received
Opinions Recorded	Parties record their opinions related to the delivery

The final group of activities is on the sensor events. These activities are solely on the monitoring of the deliverable based on sensor information. Monitoring information received from the condition monitoring systems will be recorded in the form of events. A sensor data model will be developed for these events. Each event will be modeled with a data type. Common attributes such as timestamps and duration will be included with the data. With the help of smart contracts, activities such as a thermometer reading in a package can trigger operations if programmed as such.

The delivery completion event will be included in the blockchain. The customer or customer's agent will accept the deliverable and mark the delivery successful. Alternative scenarios such as failure are also to be modeled. Opinions of the parties (word of mouth) are stored

in the blockchain as well. There is a great benefit for the customers with reliable information besides the order and delivery information stored in a tamper-free environment.

4.1.5. Use Case: E-Commerce Delivery

Our proposed solution to the challenges of the last mile is to follow the BIDAS framework and create a blockchain for all participants to record, verify, and share information related to delivery events. In this section, we demonstrate this with an e-commerce use case where a user orders goods from the Internet and an e-commerce company ships them to the customer's home.

This is a good use case as delivering the products purchased from e-commerce vendors to the door is quite standard in the parcel delivery use cases. As part of e-commerce transactions, customers purchase goods through e-commerce company web sites and receive the goods through the delivery channels. The industry also has 68% preference on interconnected systems that enables retailers, shippers, and customers to be closely connected [301]. Therefore, we believe modeling this interaction on a blockchain where all stakeholders have fast and direct access to the information is appropriate.

4.1.5.1. Decentralized model for the business

Blockchain networks mainly differ by the roles of participation and governance of the chain. Public blockchains govern the system with democratic principles that value the majority. As a result of this choice, they are highly dependent on cryptocurrencies to incentivize usage, maintenance, and ethical behavior. Permissioned blockchains solve behavior-related problems by assigning roles to participants. Since consensus mechanisms and other chain lifecycle decisions are made only by identified, and permissioned members, several risks related to a hostile takeover are prevented. Our solution encourages the public to become a member of, and use the blockchain. It is expected that read-only members at least benefit from the opinions in the system related to products and experiences.

4.1.5.2. Participants and information flow

Following the BIDAS framework, we identified the participants and related information flow in the proposed blockchain network is as depicted in Figure 42. Participants include

customers, e-commerce companies, parcel companies, delivery drivers, home IoT devices, smart home centres, and insurance companies.

All participants benefit from this system. First, the distributed system removes the single point of failure for individual operations. Any actor in the system is not connected to the monolithic legacy system they usually use. A delivery person does not need the delivery company systems to be up. Payment details are available even without the payment company being online. Other potential customers can see the opinions about the seller and goods, governing authorities can access the transaction details in case of conflict, insurance companies can resolve the losses, delivery companies can monitor individual deliveries, and overall, transparency encourages increased quality of service.

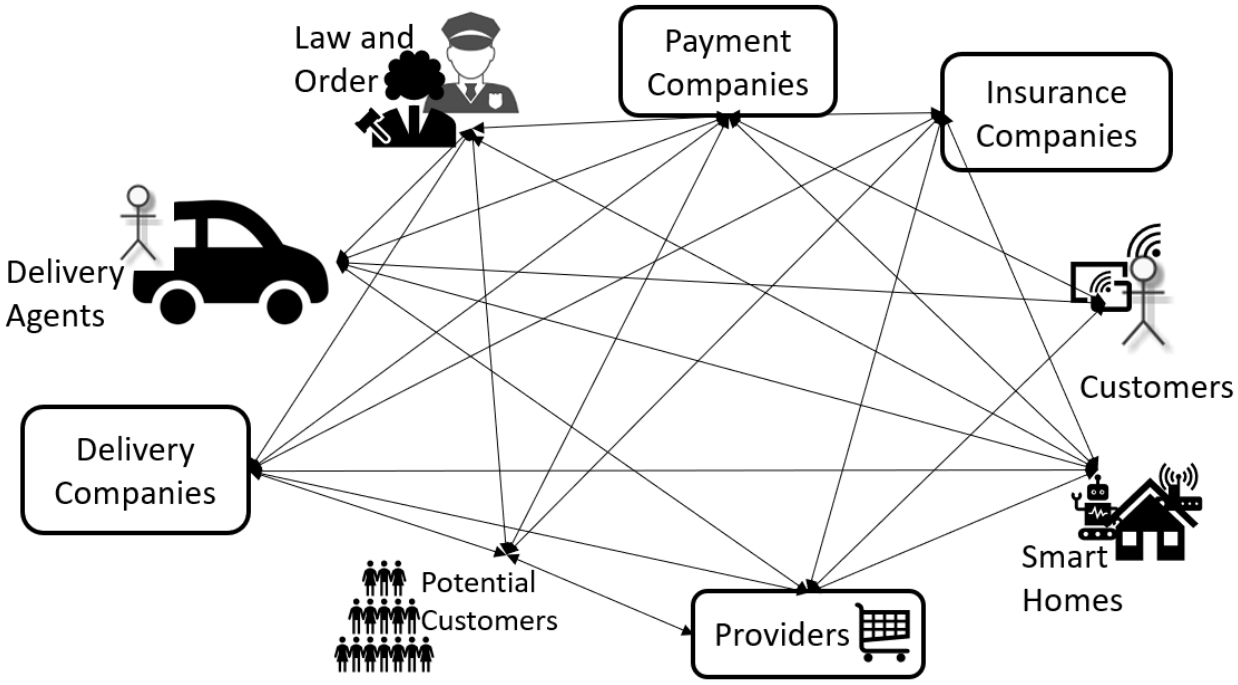


Figure 42- Participants of the blockchain-based solution

In our proposed solution, IoT devices have a vital role in representing the home and occupants of the home. The delivery is only considered flawless when the device accepts the packages and signs for their receipt.

Delivery crews are also key participants in this ecosystem. Currently, delivery companies act as the sole authority on the data and operations from the warehouse to the door. All tracking activities and data belong to them. They also make mistakes, such as delivering the order to the

wrong address. The sharing economy concept is catching up with the delivery business and provides opportunities to crowds to do Uber-style deliveries when they have available time. Our solution also removes the single authority status of the delivery company, but in return, asks for a very high level of transparency from delivery personnel and homes.

Adoption of this solution by various parties will be proportional to the benefits they receive from the system. There is much openness in this design that enables contributions from multiple vendors. Several payment companies can be involved, and several delivery options will be available. There will be more reliable opinion data in this system that are proven to be provided by people who have made purchases. Increasing the quality of the overall e-commerce space will finally benefit consumers with better service, increased quality, and lower costs. Privacy concerns on individuals' information is an ongoing discussion. The level of shared information can change depending on the implementation and time. Future online shoppers may not mind more details to be shared.

Businesses will find numerous opportunities with the blockchain to improve their data collection and precision. E-commerce companies are significant contributors who use the blockchain system to record sales. Blockchain will provide trust to the e-commerce companies as the lack of authority in the ordinary internet shopping will be replaced with the tamper-proof ledger of the blockchain. With the blockchain-based trust in place, starting a new e-commerce company will be more convenient. E-commerce companies can elevate their brand image by contributing to this project. Transparency will bring more trust to opinion collection as well. When the e-commerce company maintains the opinions, opinions lose their reliability due to the inherent conflict of interest. Customers trusting significant e-commerce companies can continue their trust. However, small companies lack the trust in the opinions provided to their website as there can be a conflict of interest between keeping original opinions and sales. The blockchain solution keeps the sales records and opinions together to eliminate the need to verify the opinion provider as a customer.

Blockchain technology created the fiercest competition for payment companies. The payment space has been the number one target for blockchain disruption. Cryptocurrencies introduced digital money without borders. Cryptocurrencies also prove the simplicity in sending money and having an undeniable log of the events. Our model brings a new approach to payments.

If independent payment companies are preferred, they can be involved in the transactions. They can provide the execution of the payment with fiat currencies and register their transactions into the blockchain.

Insurance companies are hidden contributors to the processes. Most credit cards have shopping insurance. Delivery companies have delivery insurance. If an item is missing after its delivery, home insurances can get involved. There are benefits to their business due to the precision of data collected with the blockchain. Prevention of insurance fraud translates to increased revenues for the insurance companies. These companies will also benefit from removing manual and unreliable data collection. In case of incidents, the data in hand will be evidence-grade untampered data. Currently, insurance companies do not know the delivery timestamp. Their offers on insurance, such as damage in the first 30 days, are based on estimates. Precision in this field may benefit them. Most important of all, insurance companies will provide reliable service. The disappointments due to a difference in understanding between the parties in the transaction will be avoided with undeniable records in the blockchain.

Government agencies that are responsible for law and order can benefit from participating in the blockchain network. As more platforms use blockchain and more entities trust the distributed ledgers, courts will accept the information on the blockchain to be dependable. One more significant benefit of government involvement is for taxation purposes. Economic activities recorded on the blockchain platform can be used for tax and audit purposes. Lawyers can also be participants of this blockchain so that they can use the tamper-free information in case of a dispute.

4.1.5.3. Data model

BIDAS data model is a good fit for our use case. Therefore, we will include all the data definitions provided by BIDAS. Our data model includes Customer, Order, Order Item, Payment, Deliverable, Delivery, Delivery Stage, Delivery Event, Delivery Schedule, Contact Event, Agents (Employees), Sensor Hosts and Sensors. Details of these entities will be part of our implementation but not included here due to space constraints.

4.1.5.4. Activities and automation

There are several possible types of interactions in the eCommerce and delivery scenarios, as detailed in the BIDAS framework. Similar to the data model, interactions can be used

extensively depending on the project. A delivery system that uses the blockchain for payment automation would have more interactions compared to a system only focusing on the delivery event.

We follow BIDAS framework and identify all the fundamental activities listed in Table 7. In this specific use case, order creation, status changes, sensor readings, every handover activity, completion, acknowledgment and opinions will be recorded on the blockchain. Smart contracts will be created as needed for the business rules related to these events.

The typical interaction of a consumer is with a web site alone. A shopping cart interaction is followed by a checkout process commonly ending with payment with a conventional electronic payment tool such as a credit card. All information is given to the shopping site where this e-commerce company is the book of record and ultimate authority. In case of disputes, consumers contact the e-commerce company. There are legal boundaries, but in general, consumers need to obey the provider rules and decisions.

Our proposed new interaction sequence in Figure 43 depicts the distributed version of online shopping. This interaction starts with the buyer contacting the provider and communicates the intention to purchase items. At this point, the buyer has their temporary or permanent identity provided to the system, and the provider has their permanent identity to be used system-wide. The provider records the start of the purchase process with the mark "acquisition initiated" recorded on the blockchain. The buyer, at this point, can contact the payment company and initiate the payment process. The payment company records this event to the blockchain. At this point, the purchase is completed. As we can see, the immediate benefit of the new model is the isolation of interactions and independence in choosing the payment processor. The payment information is not shared with the online vendor. This protects the payment information. The payment company and shopping web site are also independent.

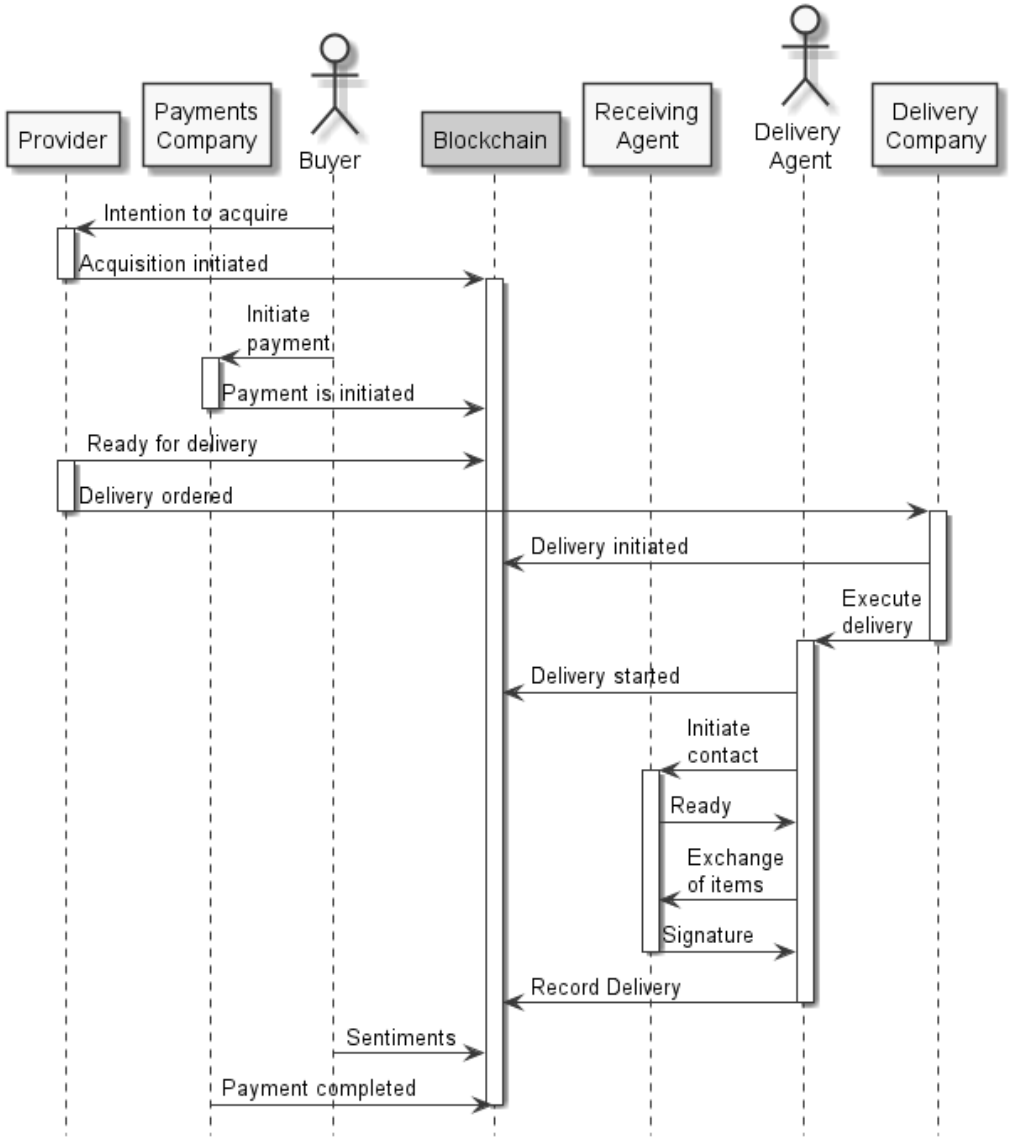


Figure 43- The sequence of steps while purchasing goods

A typical delivery process starts with the provider recording the readiness of the delivery to the blockchain. This step is essential as the item is confirmed to be available, and new participants will be involved. The provider can choose the delivery company to take on this task. Alternatively, delivery companies can bid for the delivery opportunity, but for the sake of simplicity, we will assume that the provider selects the delivery company. The delivery company physically receives the items and marks the event on the blockchain as delivery is initiated. The delivery company contacts a delivery agent. The delivery agent is modeled to be separate from the delivery company as this model is open to outsourcing the task or sharing economy to take over some of these tasks.

The actual delivery starts with the agent marking the delivery on the blockchain as "started". At this point, the delivery item is in transit. From this point on, the delivery agent can continuously record necessary sensor data. GPS location, temperature, acceleration, and several other pieces of relevant information can be stored and shared on the blockchain. These sensor data can be collected and used for improvements.

When the destination is reached, IoT devices will interact to mark the handover of the goods. There will be a contact initiation between the delivery agent and the home-based IoT device that represent the buyer. This can be a device connected to the home network, which communicates with NFC, and reads the RFID of the goods. At the very least, this device can communicate if this is the correct destination. This IoT utilization can prevent incorrect deliveries and lost packages.

Finally, the buyer will receive the goods, and they may close their part in the process by providing opinions about the experience. These opinions will be stored on the blockchain and will be shared with all participants. Since the blockchain is a reliable source for the originality of the records, even the newest and smallest companies may collect reliable opinion data. The payment can be processed at this point, and the business process instance can be marked as completed.

4.1.6. Conclusion

In this paper, we summarized the issues of the delivery model. The information flow issues are listed and depicted in Figure 37. We have presented a new application area for blockchain technology and a novel framework (BIDAS) to follow while applying this new methodology. In the delivery industry, blockchain technology can be the needed trust provider. From standard parcel delivery to complicated scenarios such as aid delivery, a system to record and maintain tamper-free information is useful. We listed details of these solutions where blockchain technology provides advantages to all participants. A transparent, accessible, and reliable environment benefits all participants.

BIDAS framework guides the implementation of delivery fulfillment using blockchain technology. We propose using blockchain technology to collect the details of the delivery lifecycle where several actors are collaborating. Our framework provides a structured approach towards a blockchain implementation by analyzing the participants, data model, and activities. Transparency of transactions and reliable opinion (word of mouth) data provide advantages to the public.

Autonomous vehicles and delivery methods normally lack the human witnesses on their activities. Blockchain and IoT technologies can compensate for the lack of this witness.

Even though the application of the framework demonstrates the fitness of the framework towards providing a solution, our framework and its blockchain-based delivery model are not yet compared to the competition in terms of costs. The price sensitivity of the customers towards the delivery fees would be a challenge for this framework as the benefits of the blockchain may not justify the cost for every implementation [285]. If the price is the decision criterion, companies will focus on cheaper services and cost-cutting. This is a common challenge faced by all trust-based systems. Privacy and availability are also common challenges facing blockchain implementations. Strong privacy requirements may work against blockchain implementations while transparency and availability are sacrificed. Even if privacy is a determinant factor in the decision, our framework brings trustable monitoring even with limited information.

The next step for our research is the implementation of this BIDAS guided use case with a blockchain platform. Our initial research indicates that Hyperledger is a suitable platform for this implementation. We will take the next steps to define the details of the blockchain data model and implement selected scenarios for evaluating our implementation.

4.2. Blockchain-Based Transparent Disaster Relief Delivery Assurance

After developing the BIDAS framework for creating solutions with blockchain-based delivery assurance, we adopted an aid delivery application to validate our delivery assurance framework. Blockchain-based Aid Delivery Assurance (BADA) application is a complete reflection of the various findings in previous sections of this thesis. BADA is a disaster relief application, including vehicle interaction and delivery assurance. This application is defined with BTTF and designed with BIDAS. By adopting this application, we demonstrated the possibility to deliver aid and use the assurance model of blockchain technology to improve aid delivery service.

4.2.1. Introduction: Call for Humanitarian Aid

Blockchain technology provides benefits that change the way business partners interact. This new way of establishing democratic trust helps business owners to think differently. The structure of participation can now shift from the centralized approach where one party has the authority and responsibility to a collective-effort-based community relying on technologically provided trust.

In what follows, we present a literature survey of issues in the disaster relief and aid industry as a problem definition. We briefly introduce the blockchain technology while highlighting the most impactful benefits followed by a survey of literature about blockchain technology in disaster relief. This survey includes the leading use cases and opportunities of the blockchain technology in this industry. Our main contribution is the design of a blockchain network as the proposed solution that addresses the issues and take advantage of the new features of the blockchain technology. Discussion and future directions related to our solution conclude this paper.

4.2.2. Problem Definition

Disasters happen frequently. In the last 40 years, the United States has had more than 250 weather disasters where the overall costs were at least $1 billion [302]. Disasters are not limited to weather and climate-related catastrophes. Poverty is a disaster [303], and wars are pulling the majority of people down to poverty [304].

4.2.2.1. Poverty, hunger, and refugees

World Vision [305] lists one of the main reasons why people around the world do not have enough food to eat is because of lack-of-money. There are several causes for such poverty. Some of the common causes for not having enough money for obtaining food are diseases, natural disasters, lack of education, and economic opportunities of the environment.

There are an estimated 870 million people [305] in the world who are hungry. One in every eight people does not have enough food while the majority of the world is enjoying technological advancements, economic prosperity, and general comfort.

The Food and Agriculture Organization of the United Nations [306] estimated that 33 percent of the food produced in the world for human consumption gets lost or wasted. This loss means the food we have is enough to feed another 50 percent more of our kind. The same resources indicate that the cereal products wasted in industrial countries alone are more than the entire food production of sub-Saharan Africa. These cereal products alone could have fed approximately half of all hungry people on earth if not wasted.

The causes for this food loss vary. From production to consumption there are several stages of loss. In developed countries, cultural and lifestyle-related causes are plenty. Excessive production due to customer expectation of wide range of products to be available on the shelves, consumers denying products based on appearance quality in the expectation of cosmetic perfection and overall sense of disposing the material if not part of a perfect product view (cutting the crust of toast-bread) are some culture-based reasons of waste [306]. Our habits, lifestyle, and lack of public awareness lead to these significant food losses. It would not be easy to change these factors.

There are several ways to address this problem of one part of the world having access to more than they need while others do not have enough. One of the methods would be acquiring, transporting, and distributing the food directly to the people in need. This supply chain that we

also call food-aid has its problems. They are fueling conflicts by injecting valuable resources where governance is weak. In Afghanistan, Congo, Rwanda, and Somalia, the influx of aid is fueling conflicts [307]. Eighty percent of the food sent to Somalia is estimated to be stolen [308]. Corruption of officials and middleman is an issue. Aid agencies paying bribes to warlords, rebels, or army officials is common [307] [309]. We see that widespread fraud on food aid exists almost everywhere that aid is needed [310]. Bringing food to a region does not contribute to the local economy. It benefits the source region of food. It does not empower or train local people to produce more, either [311].

Refugees are another class of people in need of help. The western world is familiar to see scenes from Africa, where refugees are migrating to neighbor countries due to drought and national disasters. People in this status are living in camps waiting for the food-aid due to insufficient economic condition in the host countries. There are other cases of refugees that are not bound to camps. With the erupting war, millions of Syrians are separated from their homes to become refugees in Turkey and Jordan. Several million of these refugees are residing in Turkish cities [312]. Many tried, some successfully, to continue their search for refugee status in European Union states. Most of these people were not able to carry their assets while running from fast approaching conflict.

4.2.2.2. Cash and related trust issues

It is better to give cash to refugees so that they would purchase their needs in their dignity [313]. They may choose to purchase instead of being fed with common goods. As part of being a human, they may also have preferences. It is only logical to let them choose while the cost of help is similar. Aid can be improved by ending waste and delay of transporting food through distances and giving cash instead [314] [311].

So, when a $2 donation can feed several children, what is the reason for children dying in hunger? For the people who can help others with the means of financial help, the number one reason not to help is the lack of trust [315]. Due to lack of transparency in the means and results of financial aid, donors believe either their contribution is too small to make a change, or issues can not be solved at all [316].

Numbers can be unreliable when spending or consumption is not traceable. In a typical refugee crisis, the receiving state indicating a lump sum amount is less reliable than tracing the distribution of funds and spending electronically.

4.2.2.3. Supply chain issues related to disaster relief

Many people in the world lack food and shelter. Even though the numerical concentration is in third world countries, unexpected events such as disasters can bring even people of developed countries into a position of needing help. Hurricane Katrina (2005) killed 1833 people and left with a damage of $125 billion in the United States [317]. The need for disaster relief can be anywhere in the world.

The supply chain of disaster relief is also dependent on central sources and coordination. Depending on the conditions after the disaster, relief efforts are always open to discussion. The comparison of Hurricane Maria disaster relief provided to Puerto Rico to that provided to mainland states is still a point of contention due to the difference in response activities [318]. Lack of transparency is preventing a clear analysis of the events.

Intermediaries in the disaster relief also introduce a risk of corruption. The lack of transparency leaves the efforts and aid vulnerable to the middleman's decisions [319]. The trust issue caused by this middleman risk discourages contributors from using the donation media provided by centralized relief efforts organizations.

4.2.2.4. New vehicles of disaster relief

Disaster conditions often deteriorate the conditions for conventional vehicles. Floodwaters take time to drain. Mud and debris cover the roads. Fallen trees can be an obstacle for road vehicles. These conditions can remain even after the weather conditions are back to normal. These circumstances are ideal for adoption of a new vehicle of delivery. Drones or Unmanned Aerial Vehicles (UAVs) are already taking part in the humanitarian response efforts around the world [320]. With their abilities such as capturing images and videos, drones can assist the crews for disaster relief.

With the introduction of delivery drones such as Amazon Prime Air [321], there is new utility for drones in aid distribution. Emergency supplies delivery is a good task for a delivery

drone. Considering delivery drones are preparing to deliver ordinary parcels, disaster time vital resources can be distributed with the help of these drones.

Crowdsourcing can be a powerful tool for mobilizing high volume of relief efforts [322]. However, using crowdsourcing without adequate auditing and transparency can cause fraud and result in loss of donors' trust. The monetary gain expected by the contributors as a result of their attendance may lead to misuse and misrepresentation.

4.2.3. How Blockchain Can Help Delivering Disaster Relief

Distributed ledger technology is the emerging new way of keeping records by distributing them to the participants of a network. Peer-to-peer networking is used to scale the reach of these networks so that participants can all maintain and witness the same set of transactions.

Blockchain is a type of distributed ledger where the integrity of the records is protected with the help of advanced cryptographic patterns. Transactions or simply data are bundled into blocks and supported with the metadata that helps to chain the block. Metadata of each block has a tree of hash values that maintain the integrity of the block, and has the hash of the previous block to form the pointer that helps the chain impact.

Blockchain technology can create new opportunities for each industry through its features and capabilities. The literature recognizes the opportunity as a solution to a supply chain problem [323]. Even major software companies focusing on supply chain solutions have acknowledged their interest in a blockchain-based solution to the issue. Defense organizations and military are seeing the blockchain environment as a communication medium for their logistics under extraordinary conditions such as disasters [324]. Blockchain technology can, at the least, make the response process swifter [325].

There are some existing studies about using blockchain technology to keep and validate identity records for refugees [326]. With minimum details, some ideas to use blockchain technology to aid refugees also exist [327]. IBM provides one of the most elaborate reports about using blockchain technology in disaster relief [142] where experts advise extensive use of web/mobile technologies and IoT while leaving details of the blockchain at a high level.

4.2.3.1. Transparency

Blockchain technology enables building a higher level of trust for the interoperability of disaster relief organizations through information sharing [328]. Agents can record an aid delivery and share it with all its details such as GPS coordinates of the aid recipient in Africa, images of sites, and pictures of recipients.

Recording an extensive range of information in an immutable data store would also enable authorities to utilize artificial intelligence technologies for auditing. An AI-based system can recognize duplicates, identify people, and mark suspicious/conflicting data during or after operations.

Global auditing capability will improve trust in the aid ecosystem. An aid organization anywhere in the world can be audited by a higher authority in order to improve its position and brand. Shared truth will help diminish the fraud that takes advantage of the layers of bureaucracy. New transparency and immutability enable audits to be conducted anytime and on untampered data.

The digital environment of a blockchain also has advantages in extreme conditions of the disaster scenario. A refugee or a disaster victim is most likely to be stripped off their documentation. There may not be a proof for identity, but a collection of attributes such as facial features may represent the identity. Where anonymity is seen to be more of a fit at the recipient of the aid or the presenter/donor, blockchain systems can allow that with the use of hash values instead of real values.

Removing the intermediaries results in cutting operational costs that each involved party is spending on their operations. Removing the dependencies also improves the resilience of the services, and increases availability.

4.2.3.2. Cryptocurrency

Cryptocurrency integration can help monetary operations by creating a medium for donations and other monetary transactions. Using Ethereum or another programmable cryptocurrency can provide the ability to use smart contracts for payments. On the other hand, existing cryptocurrencies may not be a good medium for financial aid. Besides their current

volatile state, there are adoption issues on spending with cryptocurrencies. Vendors may not accept it as easy as the local currencies. Local currency usage would be similar to electronic payments.

For the sake of isolating this project from the complexities of an existing cryptocurrency, we can assume at this stage that we will support multiple world currencies, or we will have our currency (DisasterAidCoin). Donations in our blockchain will be able to target a specific region in the world. This zone-limitation will prevent the funds from being accumulated and used for any other reason than the cause. Funds will be available for the services provided by the vendors in that region. This regional boundary can manage the refugee vouchers and coupons as well as the disaster relief donations.

Storing monetary transactions in our blockchain will also help with the requested traceability and transparency. The donors, if they prefer, can trace the destination of their donations. The blockchain system will store tracking data for every transaction of spending. Blockchain provides the ability to audit the spending on the blockchain transactions without the risk of corruption of the data.

4.2.3.3. Automation

Donations and aid usually have a specific target. Donation for a charity is for a specific cause. Donors assume and would like their donations to be spent for the cause they donated for. The same is true for the allowances given to the refugees. These allowances are for the immediate needs and to be spent in a time frame. Smart contracts can handle the automated tasks in a blockchain. If the system represents donations in the form of a smart contract, the smart contract methods can enable the additional characteristics that we need from the donation. Expiry of the funds may be a feature of the smart contract. An alternative solution to this is to embed this expiration login into the cryptocurrency. This way, the cryptocurrency would take care of the different states of the money, such as *active* when in use, *spent* when the funds are spent for the targeted cause, and *expired* when no longer available and returned when the expired money is refunded back to the donor.

4.2.3.4. Timely Reaction

Disaster conditions are different from regular operations. Disaster relief needs to be delivered immediately without intermediaries and bureaucracy slowing it down. An example can

be temporary evacuations of cities due to chemical accidents and hazardous conditions or fire. A modern country that has financial means to help its citizens does not need to take a long time to deliver the necessary coupons or allowances. There should not be an obstacle for the nations to take care of their own. Blockchain technology can help with the speed of distributing and allocating monetary resources. Payments can be instant, and accounting can wait until after the disaster conditions are relieved. Considering most disaster relief efforts highly depend on collected donations, reacting quickly with the help of technology can convince donors to donate more.

4.2.4. Proposed Solution to Disaster Relief

Global Aid industry needs a global backbone to manage transactions transparently and reliably. We propose to develop a blockchain-based aid delivery assurance system (BADA) to store, coordinate and communicate disaster relief efforts immutably on a blockchain-based distributed ledger.

To design BADA, we will use the Blockchain and IoT for Delivery Assurance on Supply Chain (BIDAS) [7]. BIDAS is a delivery assurance framework to provide solutions to the two fundamental problems in the delivery industry, which are “Handover of packages” and “Continuous monitoring”. BIDAS offers a blockchain-based solution to track the handovers and guides the implementation with a pattern to design the solution. BIDAS also enables all intermediary delivery agents and their IoT extensions such as sensors to become a participant of the blockchain.

Our solution follows the delivery assurance steps of BIDAS, which are “Decentralized Communication”, “Enlarged Participation and Information Flow”, “Transparent Delivery Data Model”, “Defined Delivery Activities” and “Process Automation”.

4.2.4.1. Decentralized communication

Like most other businesses with a high number of stakeholders, disaster relief ecosystems are conventionally consisting of central authorities managing the communication. Individuals donate funds and materials to specific organizations. Governments organize disaster relief and manage information traffic. They are the only trustable party in the ecosystem for all contributors. They may collect donations, or they may use their existing funds. They are an absolute authority about the final information about the events of disaster relief. They may share or censor

information according to their organizational principles and direction. Aid agencies may collect donations and organize their own services. Service providers are either providers of material or relief efforts. Coordinated by the authorities, these teams join the relief efforts. Typically, all communication between individual teams is also managed by authorities as depicted in Figure 44.

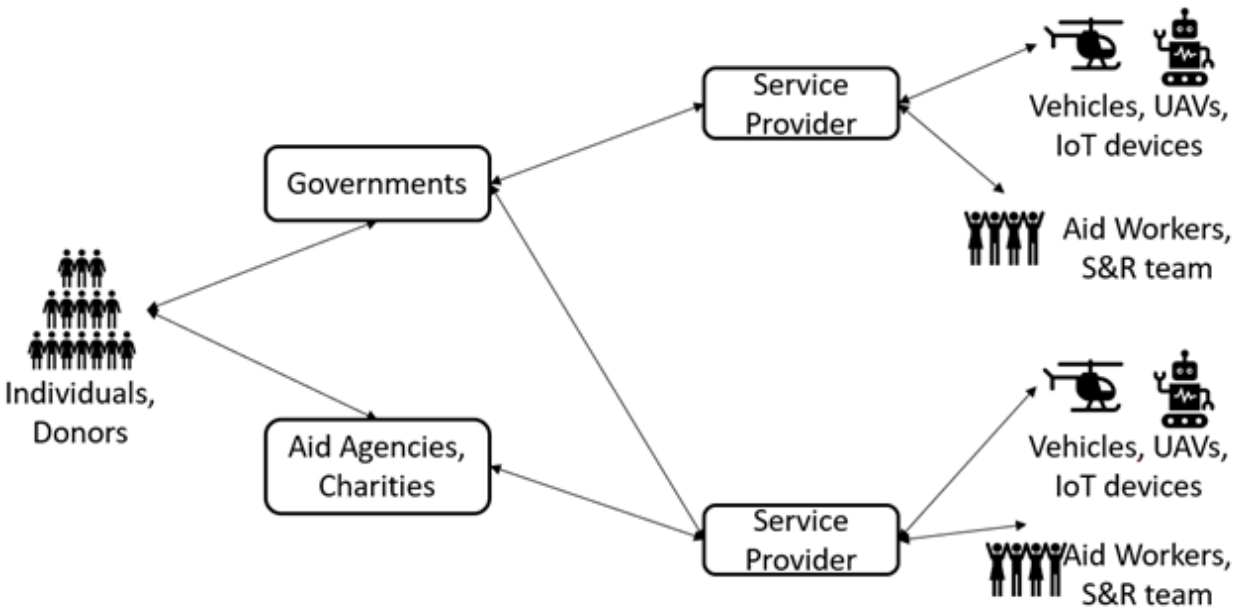


Figure 44- Conventional communication model of stakeholders in disaster relief

The first step of the BIDAS framework is to adopt a decentralized business model. Blockchain networks are distributed. Each node in the network is aware of other nodes in the network, and all nodes collectively form the blockchain. Each node in the network receives a copy of the ledger and can maintain its copy.

The main benefit of such a distributed architecture is the resilience of the network. If any of the nodes are malfunctioning, broken or inaccessible, the rest of the nodes can sustain the operations. Upon restart, each node synchronizes with the rest of the network and becomes up to date by obtaining the latest copy of the ledger. Each participant can decide on the importance of each piece of information without the need for central management. In disaster scenarios, central authorities are often unreachable or too busy to process requests. Central authorities usually are optimized around the ongoing business, and not flexible enough to adapt to drastic changes in the conditions.

Peer to peer decentralized systems eliminate middlemen. Storing transactions in an automatically-shared and tamperproof database eliminates the need for many intermediaries. Legacy operations such as reconciliations are no longer needed as the blockchain networks handle this issue in real-time. Most importantly, the single point of failure is removed from the overall system. Any participant in the blockchain network can be down due to the disaster conditions. This absence does not impact the rest of the network.

Without the middleman, the ecosystem would also retain the associated funds that were transferred to the middlemen for their services as commissions and handling fees. Currently some middlemen significantly decrease the magnitude of the help for their own benefits at the expense of the most vulnerable people. Elimination of the middlemen is also important for fighting with corruption.

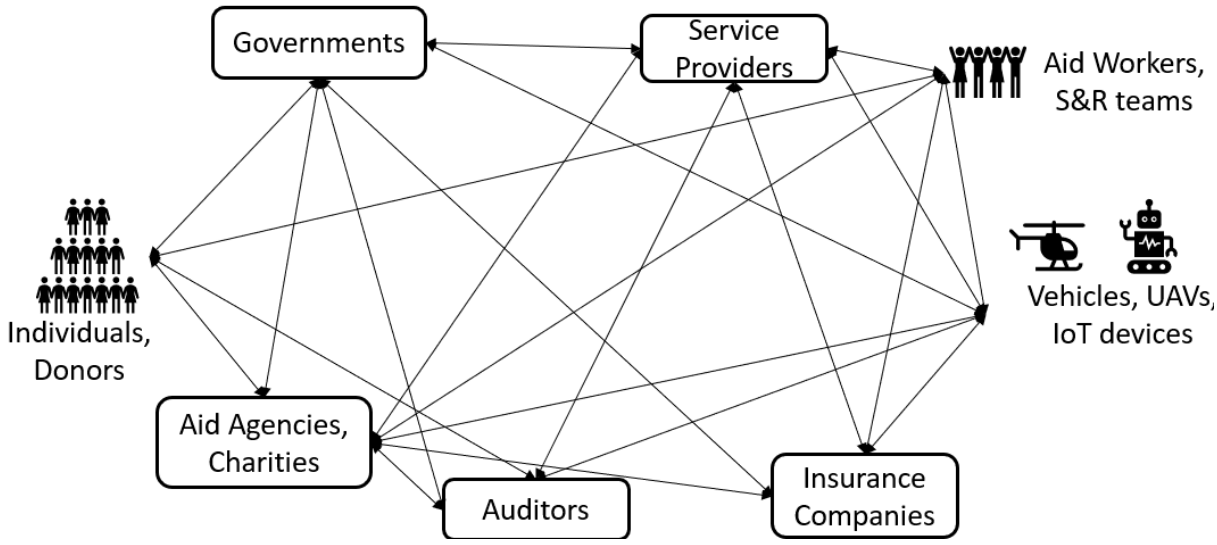


Figure 45- Participants of the blockchain network and new information flow

4.2.4.2. Enlarged participation and information flow

The first step in designing a blockchain system is identifying the stakeholders. Modeling a business with blockchain technology does not change the set of stakeholders. In order to start the process of applying BIDAS, our first step is to identify the stakeholders and actors in the system.

Most stakeholders with technical ability and processing power become participants of the blockchain ecosystem. They either use applications to issue transactions with the system, become a full node in the network by contributing to blockchain lifecycle, or only monitor the system to benefit from the new decentralized information flow, as depicted in Figure 45.

From the functional perspective, individuals are donors and participate in the blockchain system by donating and managing their donation funds over the blockchain. They can also contribute to the overall health of the system by dedicating processing power as a node in the blockchain. How individuals would be represented is a sensitive topic due to the privacy preferences and laws. Blockchain systems enable contributors to choose between having clear identities or staying anonymous.

Aid agencies and charities participate in the blockchain-based aid ecosystem as they collect and manage donations. This platform increases the trustability of these agencies to gain the confidence of the donors. Moreover, according to the assumption that donors would donate more when they can trust their donations will faithfully be channeled to the donation cause, these agencies can collect more donations with the success of this platform.

Participants under the group named service providers can be vendors providing services to refugees or disaster victims. Service providers participate in this blockchain mainly to record their activities and benefit from compensation.

Governments are a natural part of this ecosystem. Governments can coordinate and report their aid activities through this blockchain. Governments investing into this new aid system is necessary for overall adoption. Governments can also provide other services using this system. Distribution of regular aid such as welfare payments to poor people is an example of such use. Using this system will give authorities an advantage in tracking the location of the welfare recipients. Tax agencies can trace the charitable donation by tracking donations and can trace the income of service providers by tracking the spending.

Groundworkers such as S&R teams or refugee aid station workers can be a participant in the system with mobile devices with light operating systems or computers. They are service providers whose service is typically paid by government organizations.

Vehicles such as UAVs and other IoT devices can be a participant if they are playing a role in the delivery of the aid. These devices are typically part of the service provider networks.

Insurance companies are natural participants as they would like to monitor the relief effort related to their liabilities. Since their ability to know the cause of damages and minimize costs of

relief improves their bottom line, these organizations benefit highly from a trustworthy system full of detailed information.

Table 8- List of roles in relief delivery handover 1/2

Party Type	**Initiator**	**Service Intermediary**	**Service Intermediary**	**Service Intermediary**
Owner	A Donor	A Charity	Trucking Company	Air transport company
Actor/ Agent		Charity Warehouse manager	Driver	Airport personnel
Sensor Host		Charity Warehouse system	Truck	Plane, airports
Sensor		Charity Warehouse exit sensors	Barcode Scanner, Truck GPS	Plane loading docks

Table 9- List of roles in relief delivery handover 2/2

Party Type	**Service Intermediary**	**Service Intermediary**	**Receiver**
Owner	Crisis centre	UAV company	Disaster Victim
Actor/ Agent	Crisis managers	UAV Operators	
Sensor Host	Crisis management centre warehouse	UAV	
Sensor	Crisis centre unloading docks	UAV Cameras, GPS	

Auditors and governance organizations such as the United Nations can provide value to this ecosystem by participating. They can audit the integrity of the system by validating the efforts and funds are adequate and expensed ethically.

Besides the list of participants, BIDAS provides guidance on the handover processes in the delivery. It is not always one participant that carries a relief material from the procurement all the way to disaster victim. The interaction model in aid delivery handovers is depicted in Figure 46.

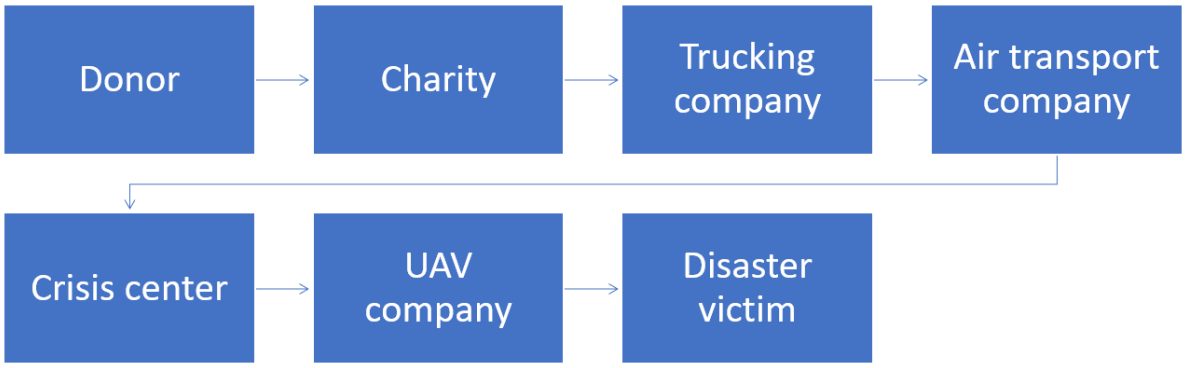


Figure 46- The aid delivery interactions model according to BIDAS

BIDAS recommends recording these handovers in the blockchain. In order to do that, all handover activities are to be discovered as detailed in samples in Table 8 and Table 9. These roles and handover activities are not a restrictive list; however, a successful implementation must start considering known use cases like these. All activities involved in the handover must be detailed as in Table 12.

4.2.4.3. Data Model: Assets and attributes

BIDAS framework recommends some fundamental entities such as Customer, Order, Order Item, Payment, Deliverable, Delivery, Delivery Stage, Delivery Event, Delivery Schedule, Contact Event, Agents (Employees), Sensor Hosts and Sensors. In the disaster relief scenario, some of these elements are named differently. For example, customers in a usual e-commerce-based delivery scenario are named as a victim in a disaster scenario. We make these changes and define our assets and attributes that will reside on the blockchain.

Table 10- Sensor readings

Sensor	**Data**
Charity Warehouse exit sensors	Material tracking information Truck entry and exit information
Barcode Scanner, Truck GPS	Truck load information (material tracking) Truck GPS coordinates
Plane loading docks	Plane load information (material tracking)
Crisis centre unloading docks	Crisis centre material receipt/tracking
UAV GPS	UAV location
UAV Cameras	UAV activity images (image before and after the drop)

BIDAS also guides in adding all sensor readings that are specified in Table 10 and continuous monitoring data into the blockchain. We take this into consideration and add the data elements to our data model.

Table 11- Registries and Attributes

Name	**Attributes**
Donor (registry)	Public-key, Signature Optional: Name(s), Contact Information(s)
Charity / Aid Agency (registry)	Public-key, Signature Optional: Name(s), Contact Information(s)
Service provider (registry)	Public-key, Signature Optional: Name(s), Contact Information(s)
Service (registry)	Service Provider (Public-key), Name/Description, Price, Currency
Delivery Agent (registry)	Type, Service Provider (Public-key), Public-key, Signature

Registration activities are relatively simple. Our solution will have the lists of Donors, Charities, Service Providers, Services, and Delivery Agents. These entities in Table 11 typically have their public key in the system to represent them in the consecutive transactions. They sign their registration to prove that they are registering themselves. The blockchain will include these records, similar to an identity management service. Enhanced security requirements may need these records to be validated by authorities.

Table 12- Transactions and Attributes

Asset Name	**Attributes**
Donation	Donor (Public-key), Charity (Public-key), Amount, Currency, Status (Donation, Expired), Optional: Location, Expiry-date, Original transaction
Aid Handover	Time, From Principal (Address),FromAgent, From Sensor Host, From Sensor, To Principal (Address),To Agent, To Sensor Host, To Sensor, Donation
Service Request	Service Type, GPS Location, Requestor, Status
Delivery	Status (Ordered-InProgress-Completed), ServiceType, GPS-Destination Location, Time, Delivery Principal(Address), Delivery Agent, Delivery Sensor Host, Service, Recipient (Signature) or Proof (Image, sound, ..), Optional: Aid Transactions

The most important transactions in the aid blockchain are the donations, aid handovers and delivery of services as listed in Table 12. Aid transaction such as a donation is a micro currency transfer. However, the transaction record must include the business logic fields. For example, the expiry date and the donation status must exist. If a donation remains unused until the specified time, the transaction will revert by issuing another aid transaction with status expiration. Smart contracts can handle this task of expiration. Delivery is the most complicated transaction that will record the aid delivery. Whether it is a drone dropping a care package accompanied with an image from the drone's camera, or an aid worker distributing blankets to refugees with fingerprints, an extensive list of details are recorded in this transaction to enable an audit. An aid delivery starts by the requestor creating a record on the blockchain. Then when an aid agency, which we generally name as service provider, accepts the delivery, the delivery is re-recorded with a new status: in progress. Multiple in-progress transactions will be on the ledger in case the business requires tracking. Finally, delivery can be marked as completed when the aid is delivered.

Since our blockchain system is custom, it does not have a limitation for the type of attributes. However, the size of data in a peer to peer network may have a performance impact. Therefore, a custom implementation may strategize externalizing files such as images or long strings. Most attributes described here are mandatory as they are assumed to be fundamental. Optional attributes typically are based on the business rules and requirements.

4.2.4.4. Activities and automation

There are many activities in disaster relief use cases. Following the BIDAS framework, we define the handover activities as detailed in Table 13.

Table 13- Handover Activities

Participant	**Activity**
Donor	A donor donates to the charity with the intention to help disaster victims
Charity	A charity procures material or prepares their existing material to be transported to the airport with trucks
Trucking company	A trucking company takes the material from charity and transport to the airport
Air transport company	An air transport company receives the materials from the trucking company and transport them to the destination airport to be delivered to the crisis centre.
Crisis centre	A crisis centre received the material from air transport and prepared them to be distributed.
UAV company	UAV company receives the materials from the crisis centre and delivers them to the victims.

There are other activities that the BIDAS framework prescribes. These activities, such as delivery status changes, the return of the packages, unsuccessful delivery, comments, and sentiments from stakeholders also can be part of the newly designed blockchain.

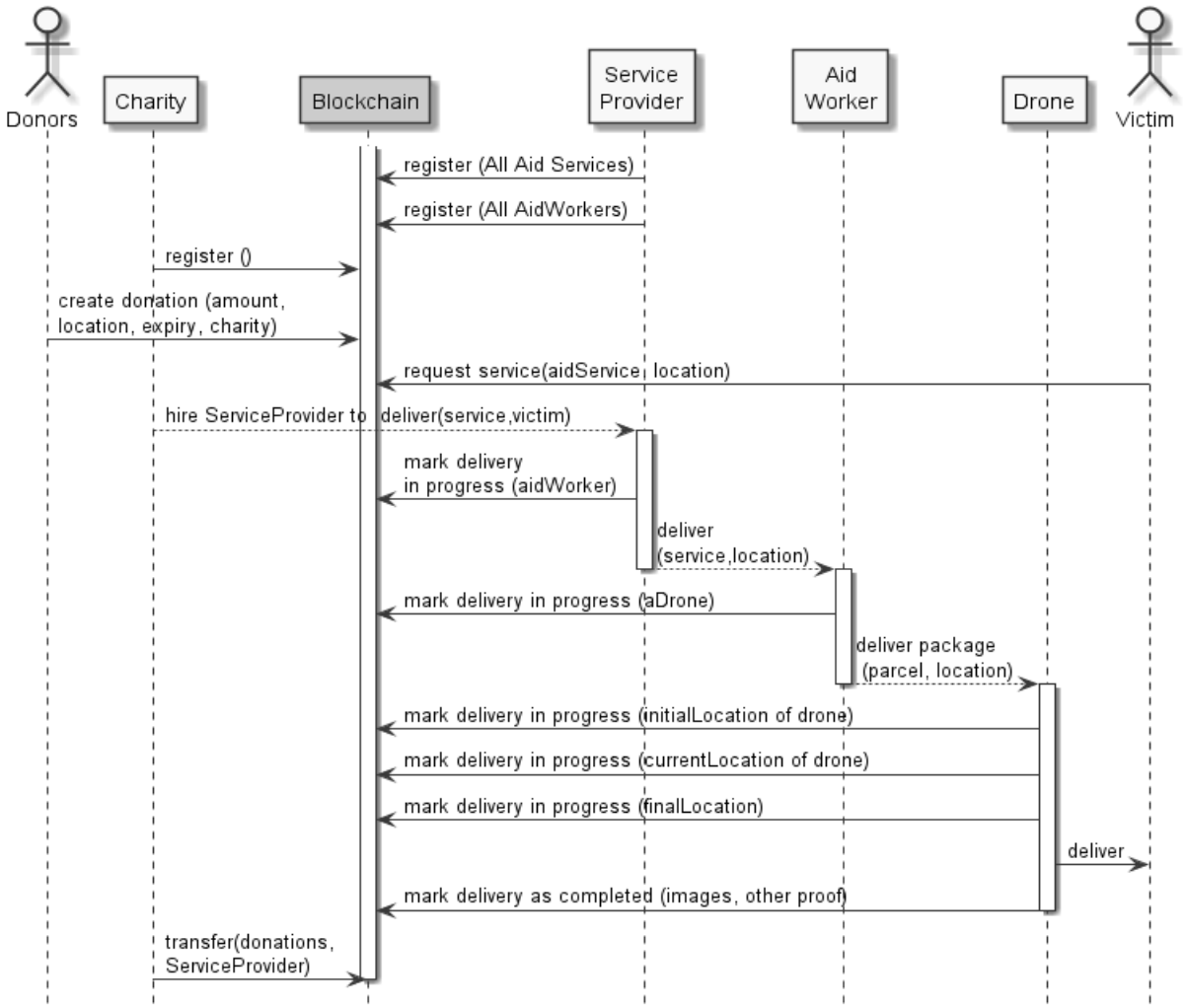


Figure 47- The sequence of steps while delivering services with a drone

In this paper, we do not detail all use cases due to space considerations. We will focus on the use case for the interactions around drone-assisted delivering services in a disaster situation. This sample use case starts with a registration phase where all aid workers, service providers, and charities are registered. If there is a strong governing body, these registrations may be approved as well.

4.2.5. Limitations and Future Direction

In this paper, we introduced a novel use case where the conventional methods can be improved through decentralization with blockchains. We listed the issues with the current model, detailed the advantages of the decentralized model, and offered a solution using blockchain

technology. We applied the BIDAS in order to start our implementation with guidance from a structured framework. We identified a good fit between the framework and our use case.

Like most blockchain implementations, the success of the blockchain ecosystem depends on its adoption. If the blockchain is implemented with the support and acceptance from the majority of significant stakeholders, it can be successful.

The governance of the blockchain system is usually an issue in implementations. Even Bitcoin blockchain has a team that develops the software and maintains the system. Bitcoin has an advantage of uniformity in the usage of the blockchain. In our design, since the blockchain usage may not be uniform in geography, country, and even purpose, a permissioned system is needed. NGOs, government agencies, and countries using this blockchain can contribute to the processing power.

There are many components to be developed for this ecosystem to work. Victims and aid workers need mobile applications to interface with the blockchain. Each mobile application must have the ability to keep a public key. Dependency on a cellular network and mobile phones is a single point of failure. However, with no network in the disaster area, the system will have to drop to an offline processing state where the applications will delay the blockchain interactions until reconnecting to the network. Until this reconnection, mobile devices will have to store the details. Online services such as identification of victims or refugees using face recognition would be unavailable.

The next step in our research is to develop the blockchain system and validate functional requirements listed above as well as non-functional requirements such as response times, scalability, and capacity. We identified Hyperledger to be a suitable platform for the implementation of our blockchain use case.

5. Experimentation

5.1. Experiment Implementation

5.1.1. Disaster Scenario

5.1.1.1. Description of the target disaster scenario

Our experiment evaluates our proposed solution during disaster conditions. We do not have a limitation on the type of disasters where our proposed solution is useful. Most disasters have similar characteristics. They occur suddenly, cause a severe disturbance, inflict pain, and disrupt the lives of a great many people. Disaster relief needs to be agile, quick, in high volume, and through unexpected hard conditions. Since we are focusing on the delivery, conditions we best serve are where there is a disruption on the usual methods of delivery, current delivery channels are unreliable, or where there are potential trust issues.

Several disaster scenarios fit into the descriptions mentioned above. Disasters that happened in the last fifteen years demonstrated the need for better solutions. Even in the leading economies in the world, extreme weather events paralyze the infrastructure and systems. In Canada, Hurricane Hazel, in 1954, killed 81 and left thousands of people homeless [329]. A state of emergency was declared in 2017 when 2,426 Quebec homes were flooded [330]. Don valley river flooded its valley and disrupted life in Toronto in 2017 [331]. In the United States, Hurricane Catrina [332], Hurricane Harvey [333] and Hurricane Maria [334] had shown that even though the aid is ready to be delivered, closed roads and missing personnel prevents immediate relief. We need autonomous and reliable delivery to help people faster and better. In Hurricane Maria, millions of bottles of water remained undelivered [335]. The stockpile of bottles stayed in the airports for months. People and organizations that sent these bottles or funding for the items deserve to know the truth about their contributions. Knowing about the destiny of the aid funds and material, donors can make better decisions next time.

Earthquakes, landslides, tsunamis, floods, forest fires, toxic chemical spills and radiation disasters are all suitable scenarios for our experiment due to the impact on logistics efforts. These disasters either damage infrastructure, block roads, prevent land vehicles from working, preventing people from working, and finally leave victims trapped waiting for aid. While floods are frequent

in North America, nuclear power plant accidents create a similar need for the drone delivery of aid. A nuclear accident prevents reasonable means of delivery. While the issue is recent, emergency personnel would focus on accident-related physical issues such as firefighting. Remaining personnel would be minimal, especially considering the danger of being outdoors without proper equipment.

In our experiment, we model a disaster scenario that is parallel to the examples we presented above. Our experiment assumes the need for drone delivery due to urgency. Our simulation focuses on a hurricane scenario where the flood following the hurricane blocks roads with debris and muddy flood waters. In this case, people are trapped in/on their houses and waiting for emergency supplies. Our proposed solution delivers the supplies and enhances this operation by recording the delivery event into the blockchain. Our proposal also solves the trust issues as part of the overall disaster relief.

5.1.1.2. Crisis centres

For any delivery use case, the source location and destination location are essential entities. Physical delivery in our context is the activity of transporting the deliverable from the source location to the destination location. Since we are focusing on the last mile of the delivery in this use case, our starting points are the crisis centres where drones pick up the aid materials and start the delivery.

There are several alternatives for the crisis centre selection. Our main criteria are the availability of deliverables to arrive at the crisis centre and the availability of drones to take off for deliveries. Under normal conditions, most warehouses would fit into the criteria where trucks would bring the deliverables and a rooftop or parking lot can be used to launch drone operations. However, under disaster conditions, we cannot assume any location is available.

Each province and city have designated emergency gathering locations with a limited set of infrastructure support features such as power generators. Community centres, parks and large parking lots are examples of designated locations that are suitable to become distribution centres. Many government buildings except for fire stations can serve this purpose [336]. Sports fields are also good candidates since they provide open areas with flat grounds.

The second set of possible candidates for our crisis centres are airports. Airports are designed to be air and land transportation hubs. They are built on broad areas, including warehouses and large parking lots. They are almost always first to recover and go back to normal operations for aid to arrive and for people to evacuate. In the aftermath of hurricane Maria, in about 36 hours, San Juan airport was operational [337]. Airports are good candidates as bigger air vehicles bring in people, generators, and aid material while drones use these resources. The main disadvantage of airports had been drone flight restrictions around airports. We can assume the restrictions do not apply during disaster conditions, and drones can fly from some relatively safe areas of the airport.

5.1.1.3. Aid Items

Immediately after a disaster's destructive powers leave the impact area, disaster relief efforts start. Food, drinking water and first aid kits are some of the primary necessities for the survivors. From this list, drinking water is the top item that victims need urgently. Water is the most significant single component of the human body, where 50%–60% of total body mass is water. It has a quick turnover of 2–3 litres. If the loss of water reaches 10–15% of body mass, about 20–30% of total body water, death is the likely outcome. These values mean that two days without water may have lethal consequences. Delivering fresh water is essential. This type of delivery happens using conventional means where applicable. Hurricane Maria had shown us that where the delivery channels are obstructed with debris and floodwaters, having a lot of water in the distribution centres does not bring any benefit. Months after Hurricane Maria, bottled water sent to the island was still sitting at the airports. Despite its value, water is a heavy item to carry. It is not always logistically possible to provide high quantities to a high number of destinations.

Figure 48- Aid items

Instead of providing the water itself, there are alternate ways that can be a more practical solution during disasters such as a flood. The portable filtration kits or personal filtration devices are good choices. We identified the aid items in Figure 48 as most compatible with our delivery scenarios due to their weight and utility. Life-straw [338] filters water, removing bacteria, parasites and microplastics. It is durable and ultralight, weighing only 57 grams. It has years-long shelf-life, and it can be used actively for months. Cleansip [339] is also a similar device but a lot lighter at 9.07 grams with a long shelf-life. Drinkable book [340] is a booklet of water filtering papers that can be used to produce clean water from muddy and dirty water. It is light as 50 grams containing multiple filters in one booklet. We consider other water purification systems and tablets in this category.

5.1.2. Constraints

We understand that all proposed methods related to drone delivery are currently not entirely applicable. In this section, we list these constraints and detail our assumptions related to these inherent limitations.

5.1.2.1. Drone operations - Legislation

There are regulations related to operating UAVs. Canadian Aviation Regulations (CARs) [341] lists the rules for drones that are 25 kg and less. Small drones under 250 grams are reasonably free to use in a line of sight, and at least five-meter distance from people. Certification is mandatory for advanced recreational drones that are heavier than 250 grams [342]. For these advanced drones,

rules are very restrictive, such as the maximum altitude of 90 meters, 75-meter minimum distance from people/buildings, maximum of 500 meters from the operator and a minimum of 9.5 km from airports [343].

Each province has a trespass act governing very likely conflict when a drone is using the airspace above a private property. Some law experts define trespassing as a mere presence of a drone on private property [344]. The same sources especially indicate that the purpose of the drone is irrelevant when there is a conflict in trespassing. Altitude restrictions are defining the airspace of a private property.

Autonomous flights are forbidden in most countries. Some countries, such as the UK, are currently restrictive. However, most restrictive countries have processes in place to issue a permit for significant size experimental autonomous delivery [345]. The list of publicly permissive countries was limited to Costa Rica, Iceland, Italy, Sweden, Norway and UAE in 2017 [346]. Recently more and more countries are granting permits for proven vendors [347].

5.1.2.2. Drone delivery problems

Drone delivery is not widely in practice yet due to some problems related to the nature of this business. First, there is a weather challenge where drones are extra vulnerable due to extensive exposure. Cold weather severely degrades drones' battery capacities. Fog, snow and rain are extreme challenges for drones [348].

Drones' flight range is currently a limitation for drone delivery [349]. Delivery drones need to have extended capabilities to deliver items to long distances and return for re-load. It is arguable that with one charging of batteries, a drone must complete multiple delivery flights in order to become economically viable. Replacing the batteries after each flight would delay the next take-off and decrease the total number of runs. A manual replacement is the default option, but it is the most time-wasting option. If the battery replacement can be automated, the total number of deliveries would increase.

Another concern is the safety of the drones. Drone delivery needs enhanced drones with price tags that are higher than recreational drones. These expensive pieces of equipment can be vulnerable to physical attacks, abuse including shooting [21], theft or theft by finding.

Connectivity is the next major problem [350]. Both for the management of the delivery operations and the safety of the delivery operations, a delivery drone needs to be connected. Connectedness is key to normal operations. For mobile networks that enable such connectedness, 5G technology is the hope. Network providers see the opportunity to boost the utility of drones and started to prepare for it [351]. With the superior qualities of 5G, such as minimal latency and more than 100 times faster data speeds [352], drones are expected to provide several more services besides flying. Better coordination of drone fleets through takeoff and landing speeds up the operations.

While looking forward to a world with drones handling delivery operations, we are aware that the safety concerns have to be handled, and possible issues have to be resolved. These potential issues include accidents such as a drone hitting electric wires and cause a fire. Drones crashing on the sky is possible with the saturation of the number of drones and concentration of operations in certain areas. Drones becoming an obstacle to other air vehicles is the most common concern at the moment, but it is also possible that drones become a concern for land vehicles on a highway and cause accidents. When drones are loaded with deliveries, additional issues such as falling drones or packages may become a concern [353].

For our experiment, we considered the above-listed limitations. We assume legislation is changed towards enabling the technology. We assumed that the value of our proposed disaster recovery solution also helps legislators justify the changes on flight rules. Disaster conditions needs to be treated according to the realities of extra ordinary circumstances.

We assume drones are protected from harm, and the flight safety including public safety is achieved with technological enhancements. Even in disaster conditions there can be people targeting the delivery drones in order to steal their load or for the salvage value or drone parts. We considered such a loss as part of our failure rates in our experiment analysis.

We assumed network technologies enable continuously connected drones exchange data at seamless speeds with the introduction of 5G technologies. However, even if the drones are not continuously connected our blockchain system would still serve its purpose. There would be differences in the timeliness of the data. Continuous connectivity enables drones to do continuous monitoring and real time interaction capabilities. Without real time interaction, all communication would be postponed until the drone is in returned to its base. Our experiment analyses both cases.

Battery technologies that enable extended flight time and the long range of the drones are essential assumptions about the drone delivery experiment. Our detailed analysis concludes our experiments with calculations related to the battery technology and range.

As a conclusion, since our proposed blockchain solution is flexible and the blockchain technology in general open to change and improvements, current assumptions do not constitute any permanent incompatibility with the future changes.

5.1.3. Systems modelling

5.1.3.1. Communication model

We modelled the aid delivery ecosystem of Blockchain-Based Transparent Disaster Relief Delivery Assurance to a blockchain system for our experiment. Participants of our network are depicted in the figure below.

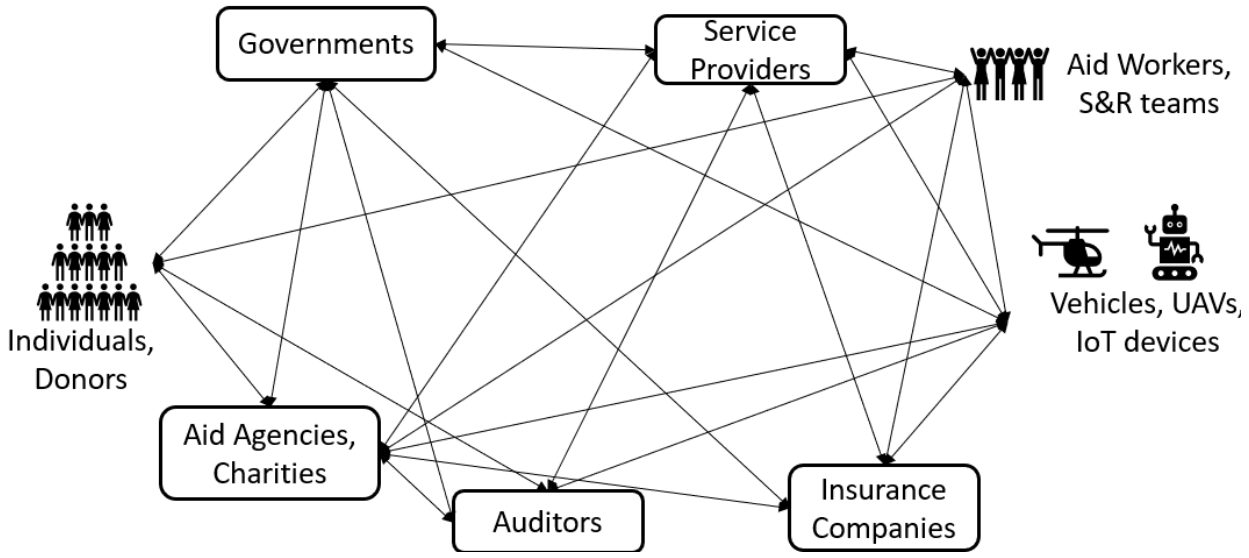


Figure 49 - Participants of the blockchain network and new information flow

As part of an aid blockchain, Government, Aid Agencies, Auditors, Insurance Companies and Service Providers collaborate. For a permissioned blockchain, the number of members does not significantly contribute to quality. More members mean more information flows to our blockchain. Since we created the air blockchain for the reliable collection of information, more information is beneficial.

5.1.3.2. Data model

Below is the list of the record structures in our main aid delivery blockchain as per BADA. We use these record structures to add information to our blockchain. Entities in the data model are represented as JSON objects in the smart contracts. When a client issues a transaction, all the information related to this transaction is sent to the blockchain node. When the blockchain receives the transaction, the smart contract engine of the blockchain identifies the transaction type, and the execution is forwarded to the corresponding smart contract code. The smart contract first creates JSON objects corresponding to the information in the transaction. Then smart contract entities are stored in the blockchain in their JSON representation.

Each entity we used in the aid blockchain is detailed in the following subsections. Entity representations are in Go language. Capital letter usage on some naming vs others is part of the Go language scope rules. Each entity is represented with a struct that is similar to a class definition in most object-oriented languages. Each field is defined by its name, its type and other annotation tags. Each line describes one field. JSON tags are also provided for each entity for the smart contract libraries to operate on the fields as needed.

5.1.3.2.1. Service Request

Service request entity represents a service that had been requested by victims or any other organization that is aware of the need for aid delivery. With the assumption that the victims have a network connection, it is possible for them to create their own service requests. A more probable case of service request creation would be either aid agencies or disaster management agencies to create these records. Each record includes the type of service that is requested, coordinates of the destination, status and timestamps.

```
type ServiceRequest struct {
	Status string `json:"status"`
	ServiceType string `json:"servicetype"`
	DestinationLongitude string `json:"destinationlongitude"`
	DestinationLatitude string `json:"destinationlatitude"`
	Timestamp string `json:"timestamp"`
}
```

5.1.3.2.2. Donation

In our aid ecosystem, a donation entity represents the information coming with each donation. Each donation record includes the donor who donated, the charity, amount, currency, status and timestamp. We included other constraints for a donation record, such as consent for the donation to be used for a service in a specific geographic region. The target region of the donation is represented with the coordinates specified in this record. This measure can help prevent the donation from being used outside of the intended destination. An expiry date attribute is also provided to mark the timeframe of the donation. Each donation must be spent before the provided expiry date, or the donation would be cancelled. This measure can help enforce the donation to be spent within the expected timelines instead of postponing.

```
type Donation struct {
	Donor string `json:"donor"`
	Charity string `json:"charity"`
	Amount int `json:"amount"`
	Currency string `json:"currency"`
	Status string `json:"status"`
	DestinationLongitudeStart string `json:"destinationlongitudestart"`
	DestinationLatitudeStart string `json:"destinationlatitudestart"`
	DestinationLongitudeEnd string `json:"destinationlongitudeend"`
	DestinationLatitudeEnd string `json:"destinationlatitudeend"`
	Timestamp string `json:"timestamp"`
	Expiry string `json:"expiry"`
}
```

5.1.3.2.3. Aid Handover

BIDAS framework models the delivery events as a series of handovers. For our aid delivery scenario, AidHandover structure is used to record these handover events. The aid materials that are going to a destination would be handed from one member to another in the blockchain system. The handover can be happening in person or it can happen autonomously using the sensors. The record intends to store all possible information related to the actors involved in this event.

```
type AidHandover struct {
	Timestamp string `json:"timestamp"`
	DestinationLongitude string `json:"destinationlongitude"`
	DestinationLatitude string `json:"destinationlatitude"`
	AidItemId string `json:"aiditemid"`
	FromPrincipal string `json:"fromprincipal"`
	FromAgent string `json:"fromagent"`
	FromSensorHost string `json:"fromsensorhost"`
	FromSensor string `json:"fromsensor"`
	ToPrincipal string `json:"toprincipal"`
	ToAgent string `json:"toagent"`
	ToSensorHost string `json:"tosensorhost"`
	ToSensor string `json:"tosensor"`
	Donation string `json:"donation"`
}
```

5.1.3.2.4. Delivery

Delivery records represent the delivery in the last-mile. In our application, drones deliver the aid items to the destination coordinates. Delivery events such as state of the delivery and completion of the delivery can be recorded to the blockchain. All these records create a trace of how a specific donation is used. A delivery proof can be attached to a donation to further convince the stakeholders on the delivery of the aid. Drones add this proof of delivery to the delivery record.

```
type Delivery struct {
	Status string `json:"status"`
	ServiceType string `json:"servicetype"`
	DestinationLongitude string `json:"destinationlongitude"`
	DestinationLatitude string `json:"destinationlatitude"`
	Timestamp string `json:"timestamp"`
	AidItemId string `json:"aiditemid"`
	DeliveryPrincipal string `json:"deliveryprincipal"`
	DeliveryAgent string `json:"deliveryagent"`
	DeliverySensorHost string `json:"deliverysensorhost"`
	Recipient string `json:"recipient"`
	Proof string `json:"proof"`
	Donation string `json:"donation"`
}
```

5.1.3.2.5. Monitoring Events

Monitoring of the IoT events is a significant additional value provided by our blockchain. Delivery operations are a chain of handover events. Since the modern implementation of handovers and interactions involve a significant amount of IoT devices, a structure to record the observations is needed.

We created the below entity to record the observations from the monitoring devices. This entity contains attributes to record the key information on the delivery event and add the readings from the devices in a flexible structure where the type and value of the readings are provided.

```
type DeliveryMonitoring struct {
        DestinationLongitude string `json:"destinationlongitude"`
        DestinationLatitude string `json:"destinationlatitude"`
        Timestamp string `json:"timestamp"`
        AidItemId string `json:"aiditemid"`
        DeliveryPrincipal string `json:"deliveryprincipal"`
        DeliveryAgent string `json:"deliveryagent"`
        DeliverySensorHost string `json:"deliverysensorhost"`
        CurrentLongitude string `json:"currentlongitude"`
        CurrentLatitude string `json:"currentlatitude"`
        OtherMonitoringType string `json:"othermonitoringtype"`
        OtherMonitoringValue string `json:"othermonitoringvalue"`
}
```

5.1.4. Simulation Design

There are several online disaster databases. We identified that there are detailed records of disasters in the literature. Public Safety Canada [354] has the Canadian Disaster Database that contains disaster information related to more than a thousand disasters.

The types of disasters we want to simulate are where people are scattered to a geographical area and delivery for aid is needed. Hurricane and flood are practical examples of our use case.

5.1.4.1. Limitations

There are no specific and detailed datasets for the locations of the disaster victims at times of flooding and similar disasters. Some victims evacuate their homes, some victims move to higher grounds, some return to their homes and many gather together to join forces against possible dangers. Due to the lack of data, we decided to start from a superset. We then identify the aid target area. Finally, in the designated target area, we include all addresses into our delivery destination list.

5.1.4.2. Delivery targets superset

Ideal data for experimenting with the delivery assurance as part of disaster relief would be the data detailing where disaster victims are located during a major disaster. This data would show how victims are scattered, how they gather, where they wait for aid, and what the group demographics are. Such data would help us correctly simulate the delivery of the care package to the right location with coordinates, deliver a precise amount of aid, and prevent any waste. However, such data does not exist. Without the coordinates of disaster victims, and demographics, we have to use simulation in order to conduct our tests.

We need a superset of target locations to be used as delivery destinations. For this purpose, we use the Open Addresses [355] dataset. Open addresses are a global dataset for addresses. Data in this dataset consists of a list of addresses with longitude, latitude, street number, street name and the city. Addresses are incomplete with missing elements such as postal code, but this dataset provides us with the minimum data that we need for conducting our simulation.

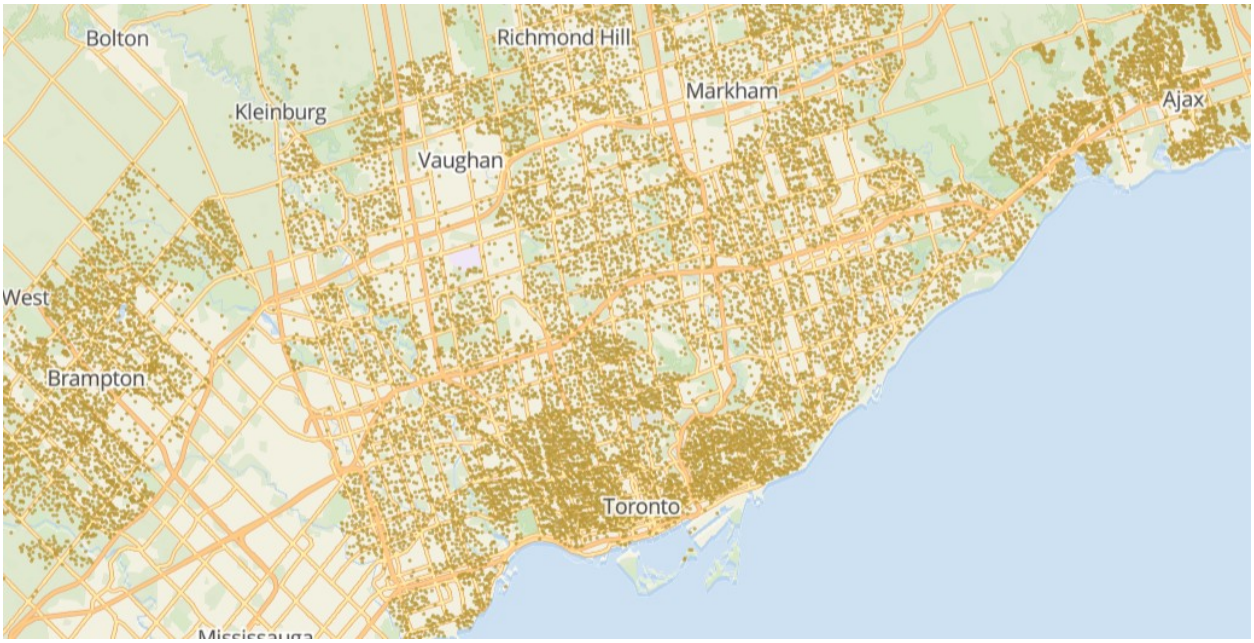


Figure 50- Open Addresses Dataset Toronto Addresses

Sample data from the Open Addresses dataset is shown below to demonstrate the data precision, types, and completeness.

Table 14- Sample data from the initial dataset

LON	LAT	NUMBER	STREET	UNIT	CITY	DISTRICT	REGION	POSTCODE	ID	HASH
-79.5443	43.593789	22	Lloyd George Ave		Etobicoke					4609176c08c67d96
-79.5435	43.5934445	3	Lloyd George Ave		Etobicoke					8acf99afdb870ad6
-79.5436	43.5936221	7A	Lloyd George Ave		Etobicoke					239c832319e298e7
-79.5466	43.5962026	58	Foch Ave		Etobicoke					2bb9aab1d601c207
-79.5464	43.5959935	54	Foch Ave		Etobicoke					c33e434ceba1c9fb
-79.5466	43.5963137	60	Foch Ave		Etobicoke					f037b9cfaead8162

5.1.4.3. The delivery targets data model

We created a relational database system (RDBS) in order to work on the addresses. For this purpose, we procured a Microsoft Azure environment. In this environment, we create an MS SQL Server database.

In this RDBMS instance, we created a database schema to store, enrich and use the data. Our main table that we load the delivery targets is called ADDRESSES. Its attributes are listed in table below. Toronto addresses are loaded and counted to be 525,545 addresses. Durham region addresses are counted to be 235,587.

ADDRESSES (dbo)

Column Name	Condensed Type	Nullable
AddressId	int	No
LON	decimal(12, 9)	Yes
LAT	decimal(12, 9)	Yes
NUMBER	varchar(128)	Yes
STREET	varchar(128)	Yes
UNIT	varchar(128)	Yes
CITY	varchar(128)	Yes
DISTRICT	varchar(128)	Yes
REGION	varchar(128)	Yes
POSTCODE	varchar(128)	Yes
ID	varchar(128)	Yes
HASH	varchar(128)	Yes
Elevation	decimal(6, 2)	Yes
SimulationId	int	Yes

Figure 51- Addresses Table

In order to load the data from its source (CSV files) to the SQL tables, we created a data ingestion pipeline for loading the addresses from the source to the database. We used the Azure Data Factory for this task. Steps of these operations are provided on GitHub [356].

5.1.4.4. Data enrichment application

Data cleansing is a big part of the analysis of big data systems. We continued with enriching and cleaning the data according to our planned tests. For our Toronto tests, we modelled the flood in the Toronto area. In order to simulate the rise of the water and calculate the impact area, we decided to use the elevation. The elevation attribute was not included in the Open Addresses dataset. We decided to add this data to our dataset.

JAWG [357] is an interactive map provider. They also provide APIs to serve map data. We created an application to read the Toronto addresses and add the elevation data. This application goes through the ADDRESSES table in the database, and for each record, it calls the JAWG API. After parsing the API response, the application extracts the elevation data from the JSON payload and writes it to the database to the same table. The application code is provided on GitHub [358].

5.1.4.5. Disaster Victims Determination

From this superset of all destinations, we choose the target for each disaster. In order to find a suitable set of destinations, we work on a model that creates a limited number of destinations. Closure of the main roads is a factor in defining the flood area. When the main roads are closed, alternative delivery channels such as drone delivery can be used as replacement.

Our flood simulation took place as follows. Using Google Earth, we increased the water body around Toronto to 190 meters. This high value is determined by testing the impact of different values for the purposes of simulation. Our aim is to limit the number of delivery destinations to a manageable amount and simulate the conditions that make conventional means of delivery not possible.

We gradually increased the waters and observed the impact of the flood on the Toronto map as follows. When the waters were raised 180 meters as in Figure 52, we observed a large area of land was above water. When we raised this number gradually, we observed around 190 meters as in Figure 53, there is a smaller land that is suitable for our experiment. This figure also shows how the main roads are flooded and alternative disaster relief efforts are not possible. We also supported the suitability with number of addresses we have in our database that is located in this survival map. At each increase, we tested the visuals and the elevation values to check whether we

reach a practical dataset of disaster victims. When we reached 200 meters as in Figure 54, we observed the land mass we cover is small for the load tests we are targeting.

Figure 52- Toronto Flood - 180 meters

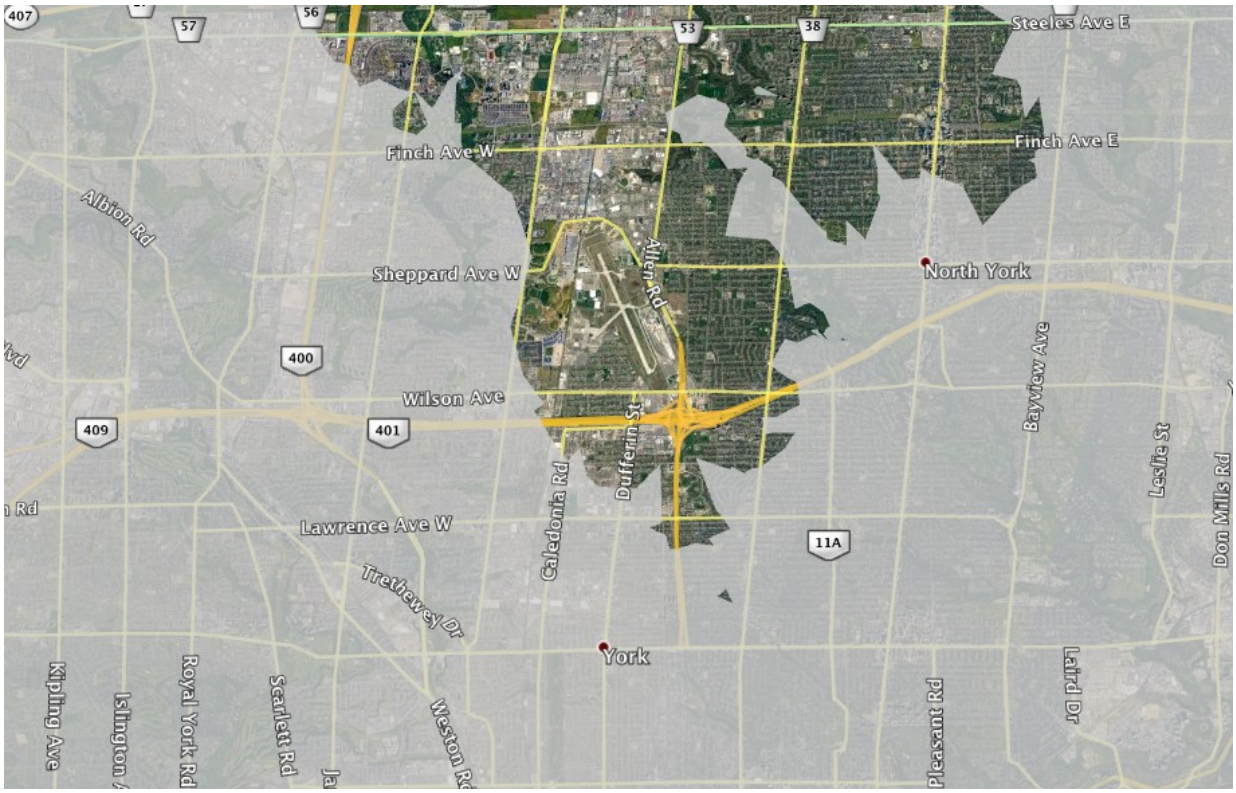


Figure 53- Toronto Flood – 190 meters

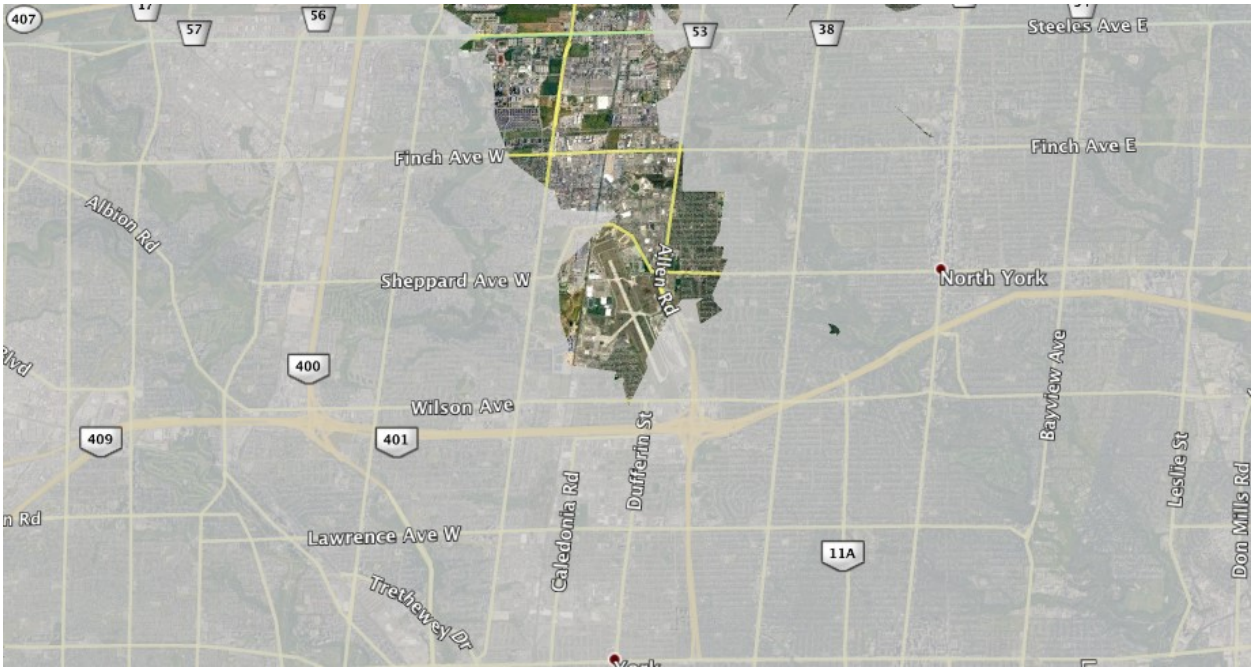


Figure 54- Toronto Flood - 200 meters

By querying our database, we found out that the following number of addresses in Toronto is above water. The disaster victims are determined to be the following number of addresses. From 190 meters criteria we identified a total of 17546 addresses inhabitable as detailed in Table 15.

Table 15- Number of addresses for each 10 meters

Elevation Min (>)	**Elevation Max (<=)**	**Number of addresses**
200m	…	516
190m	200m	17018
180m	190m	47279
170m	180m	52337
160m	170m	64408
150m	160m	60120
0	150m	283855

Detail of the per meter change in the number of addresses are provided in Table 16.

Table 16- Number of addresses for each one meter

Elevation Min (>)	**Elevation Max (<=)**	**Number of addresses**
195m	196m	1348
194m	195m	1558
193m	194m	2054
192m	193m	2739
191m	192m	3112
190m	191m	3770
189m	190m	3958
188m	189m	3888
187m	188m	4277
186m	187m	4567
185m	186m	4962

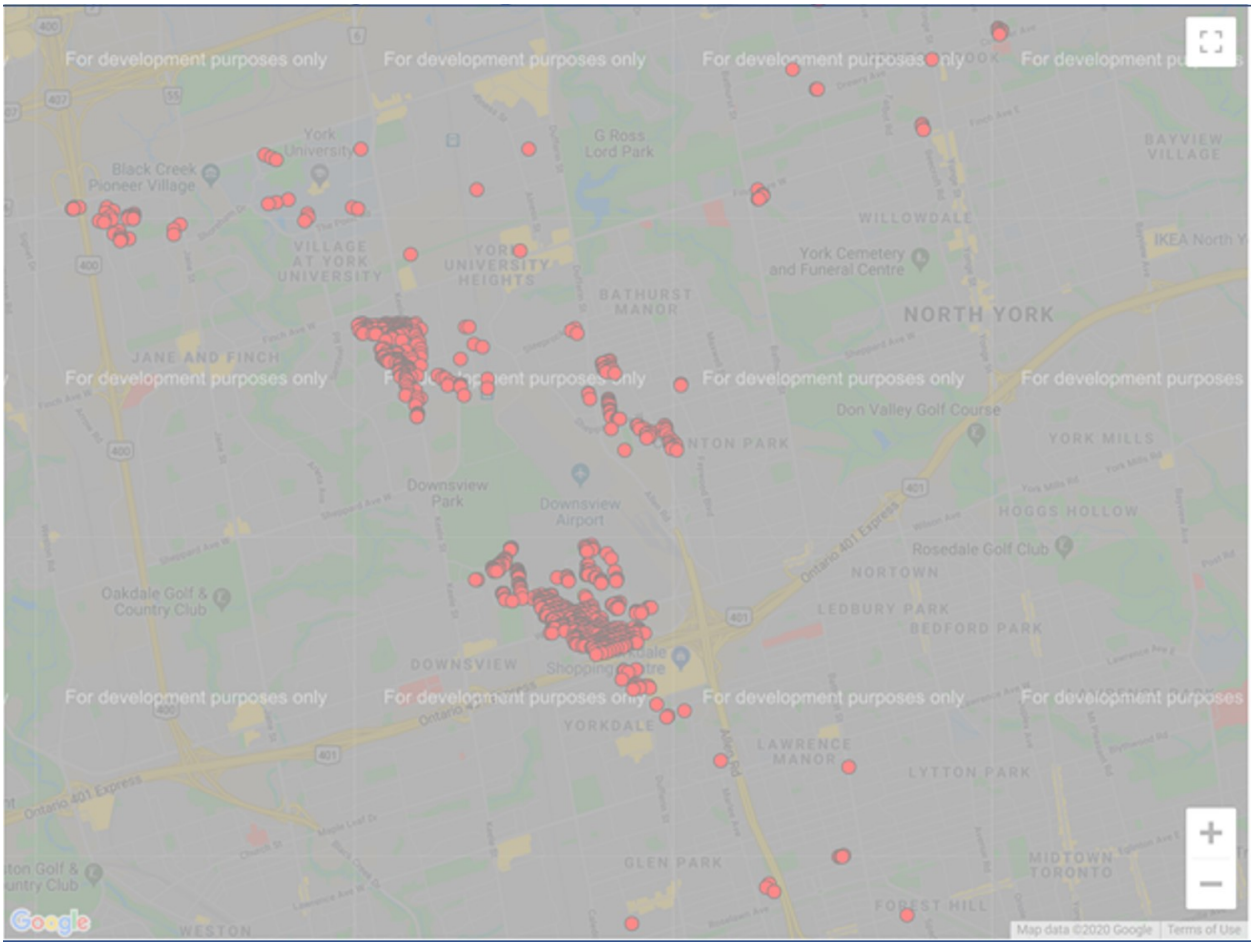


Figure 55- Map view of delivery targets in Toronto Flood

We plotted some of our delivery targets on to a map [359] and validated the locations are mainly around Downsview Park, which has a small airport, hangars, storage locations and a large park.

5.1.4.6. Crisis Centres

Under normal conditions, we cannot operate drones from airports. However, previous flood examples indicate that the aid is often accumulating in airports and need to be distributed from there. We acknowledge the fact that we cannot fly from Downsview airport. Meanwhile, there is a large park and warehouse establishment in close proximity to the airport. Therefore, we designate the Downsview park as the distribution and crisis centre. We store the aid materials, run our operations and distribute the aid from the Downsview Park.

5.1.4.7. Service Provider - UAV Company

UAV companies are service providers. They are a member of the blockchain system. They are members of the blockchain network, and they also handle blockchain-related tasks that are not handled by drones. They coordinate drones, schedule tasks and manage the physical characteristics of the autonomous operations such as handle the loading of the drones or other mechanical maintenance tasks.

In the simulation, we developed a java application to represent the UAV company. This Java application is managing the scheduling and coordination of the UAVs.

5.1.4.8. UAV

UAVs carry out the delivery operations autonomously. While the operations are in progress, UAVs communicate to the blockchain and issue transactions for the information that they are programmed to add to the blockchain.

There are multiple categories of UAVs. In our experiment we are mainly interested in the UAVs that can deliver aid with by taking frequent trips between the crisis centres and the delivery destinations. Racing drones are the fastest drones in this category reaching to 260kms/hr [360]. There are several examples of delivery drones flying up to 100km of distance with 100km/hr speed [361]. Although there are faster drones with longer range, we can assume these values are our base for the calculations.

In the simulation java application, each UAV is represented with a separate thread. Threads are executed simultaneously in the java virtual machine (JVM), and each receives their task from the UAV company.

The UAV simulation application includes the majority of the simulation logic as the success and failure logic for the deliveries are coded in the UAV applications as drone-based factors. Drone-based factors include drone failure, such as a drone that fails and gets lost during the operations. Some drones are programmed to try to reach far away delivery points, and can not come back to the base successfully. The rate for failure is assumed to be 1%-3%. Each drone picks a delivery task and marks it into the blockchain. During the delivery operation, it creates its IoT conditional monitoring records. When the delivery operation is completed, the UAV creates the delivery completion transaction. Finally, UAV returns home, and the mission is accomplished.

5.1.5. Implementation of the Blockchain

5.1.5.1. Blockchain provider and specifics

There were 861 blockchains as of May 2019 [362]. Most of these blockchains were part of the cryptocurrency boom and created as specific products serving specific purposes. As the underlying product fails, blockchains also disappear [362]. The blockchain council indicates the blockchains that are developed as platforms. These blockchain platforms provide infrastructure to people who would like to develop their own projects by utilizing underlying libraries and algorithms.

In order to conduct our experiment, we need to develop our blockchain application on a blockchain platform. Among top blockchain platforms, Ethereum is the most popular one. Its public nature attracts most blockchain projects as the only blockchain or a blockchain that they can write anchor information beside their private blockchain. Hyperledger Fabric is the most popular permissioned blockchain. The world's top enterprises openly support this blockchain. It is a production-ready blockchain for enterprises. R3 Corda is another popular blockchain mainly known by its financial focus and its institutional users from financial markets.

We chose Hyperledger Fabric since Ethereum is a public blockchain system that is not suitable for the privacy requirements that may be required for our projects. R3 Corda is used by financial applications, but our application requires a more flexible data model. Our blockchain application does not meet the requirement to have complex validation logic.

Hyperledger Fabric is a permissioned blockchain implementation. Besides functioning as a simple blockchain, its key features include the ability to create channels to segregate blockchain transactions and running smart contracts that can be developed in Go/JavaScript/Java languages. Operating with a multi-channel model enables the clients of this blockchain to have private transactions. Most businesses need to use the blockchain system to store data in three different privacy levels. The first one is public data. Public data includes operational attributes such as data and no-knowledge attributes such as hash values. The second level of privacy is semi-private data. Participants may choose to share some transaction information that helps facilitate other advantages. For example, an insurance blockchain may enable participants to see which cars are insured. This sharing helps participants with their own business transactions. The last category of

information is the private information such as price that only participants involved in the business transaction have to know.

Hyperledger Fabric network consists of nodes that may have different roles. These blockchain nodes are called peers. All peers retain a copy of the ledger. Some peers are configured to run smart contracts. Others may be only focusing on transaction processing and commit operations. The separation of code execution from the transaction processing is called the endorsement pattern. Endorsement means that multiple peers would run the chain code and endorse the results with their signature. With these endorsements, the blockchain system can accept and commit the results. Once the transaction is validated, the ordering service includes it to the next block and communicates the block to the networks for consensus. Each next block is cut by reaching a certain number of transactions or a timeout. Ordering service in Hyperledger Fabric is a plug and play system that can be replaced with leading industry systems such as Kafka and Zookeeper.

5.1.5.2. Programming language

Smart contracts in Hyperledger space are called chain code. Chain code applications use the defined ledger APIs to access the shared state in order to run the business logic defined by the application developers. For developing smart contracts, there are alternatives provided by the Hyperledger Fabric. Go language is the default choice, and it is the natural language for the Hyperledger. Google engineers created Go language. Creators of Go language intended to create a language that is not slow like Python and not complicated like java. Go language is developed with multi-threaded environments in mind where old languages mainly focus on memory economy. Go system has great simplicity, to be built and tested quickly.

Go language has some useful features that are compliant with the philosophy of blockchain, for example the compiler errors are thrown for unused variables. Blockchain technology is a medium that distributes values and applications to several participants in the network and not wasting any memory is essential.

5.1.5.3. Number of Members

Each member of the blockchain is an independent server. Each member runs the blockchain software and communicates with the other members to conduct blockchain transactions. For the

sake of limiting the related expenses, we limited members in the blockchain. We created a total of four peers. These four members are a good representation of four different roles in the blockchain application. Service providers are the only mandatory blockchain member.

5.1.5.4. Block Size

Block size is an essential factor in blockchain operations. Each block is created with a predefined number of transactions or a predefined time frame. If there is a high number of drones, there would be a high number of transactions created simultaneously. Large throughput of transactions is dependent on the block creation capacity.

5.1.5.5. Channels and Security

Channels are logical separators between the different lines of businesses. Each disaster would have its own channel separating the participants and rules from other disasters. Channels are the scope of security and business rules. For our experiment, we created a channel named "aid channel." Users are registered, and roles are assigned on a specific channel.

5.1.5.6. Resources (CPU, Memory)

We used three computers in our experiment. Blockchain application is installed and configured on two Linux based computers while the application testing the system was running at a third Linux based computer. CPU for these computers are Intel Core i7 and each has 2GB RAM.

5.1.5.7. Transaction Size

The transaction limit in the Hyperledger is 99 MB by default. Our record structure is minimal, and this limit is not a significant factor in our tests.

5.2. Load Testing

We repeated our tests and collected data in order to understand the blockchain behaviour and the capacity of the blockchain network we constructed. During the tests, we assumed that all drones are clients for our system and drones are using our system by continuously issuing delivery event transactions. No time is wasted at the flight of delivery. These tests assume an instant delivery. These tests reveal the ideal concurrent clients for our system, and we observe the maximum throughput we can reach with the current setup.

We completed sixty tests in this category to record the impact of changes in the test variables towards the overall system performance.

5.2.1. Throughput

We run our tests for each combination of the test variables. For each combination, we completed one thousand deliveries and collected data. We also repeated our tests with several high numbers of loads and observed very comparable results.

5.2.1.1. Distribution with block size set to ten and block timeout set to two

In order to understand the impact of our test variables, our first major test is to accomplish the same amount of work with a different number of concurrent clients. We collected the change in the throughput value with respect to the changing number of concurrent clients. For the entire test, the block size is kept as ten, and the timeout is kept as two.

The diagram below shows the result of this experiment. It indicates that where the throughput in number of Transactions Per Second (TPS) is the performance benchmark, the lowest performance is observed where there is not enough activity. When there is only one drone issuing transactions, each transaction is waiting for the block to be completed. Since one client means one transaction, the transaction is packaged in a block only with the block timeout, which is 2 seconds. This behaviour is observed even when there are nine concurrent clients. Nine clients are connected at the same time and each issue one transaction. Therefore, a total of nine transactions are created, and all wait for the timeout of the block.

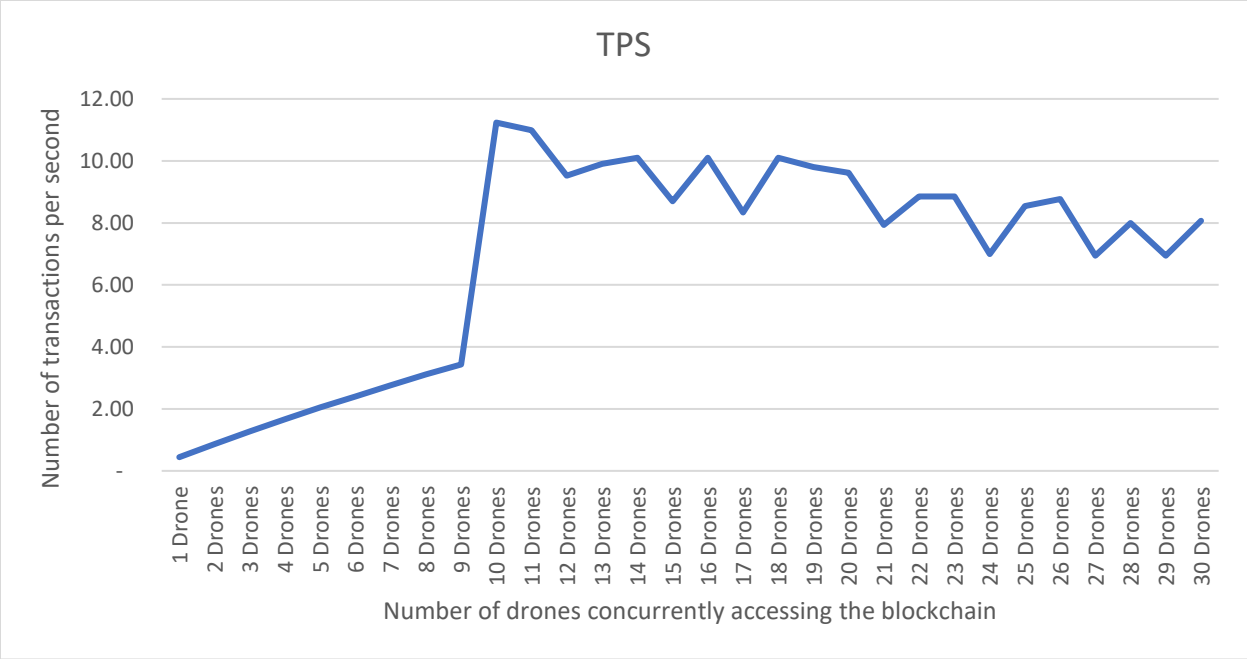


Figure 56- Performance (TPS) vs # of concurrent clients

When the number of concurrent clients reaches the block size, then the behaviour of the blockchain system changes and blocks are issued as soon as the number is reached. Therefore, any number of concurrent clients above the block size presents a good performance number. From the findings, we can conclude that the best performance is reached when the number of concurrent clients is the same as the block size. When the concurrent number of clients exceeds this number, then some clients are serviced with the current block immediately, but some other clients wait for the next block.

The diagram shows a decline in the performance with an increasing number of concurrent users after the number exceeds the block size. There are two reasons for such a decline. First is the line-up. When there are twenty clients trying to issue transactions at the same time, the first ten transactions are packaged in the same block, and the next ten transactions are packaged in the next block. Even though the decline in performance is not high, there is still an added waiting time for the owners of the second set of ten transactions. This line up is suspected to decrease performance. The second reason is suspected to be the simulation software. Simulation of multiple concurrent clients is done using thread programming. However, since the software is running on the common CPU, the increasing thread numbers are sharing the same resources and may slow the system down in thread context switches.

5.2.1.2. When the block size = # of drones

Since we discovered that the peak performance could be accomplished with the number of concurrent clients to be the same as the number of transactions bundled in a block, we continue to observe the statistics in different settings. The diagram below shows the system performance where the block size variable and the number of concurrent clients is the same. Our experiment indicates that the performance peaks where the number of concurrent clients and the block size is twenty. This type of peaks is often related to the infrastructure capabilities such as network and hardware. When the number of concurrent access exceeds the healthy capacity of the system, clients form queues and servers split their capacity between managing the queue and processing requests. Clogging of the system makes processors make high numbers of context switching, which slows down the processing and reduces the TPS performance.

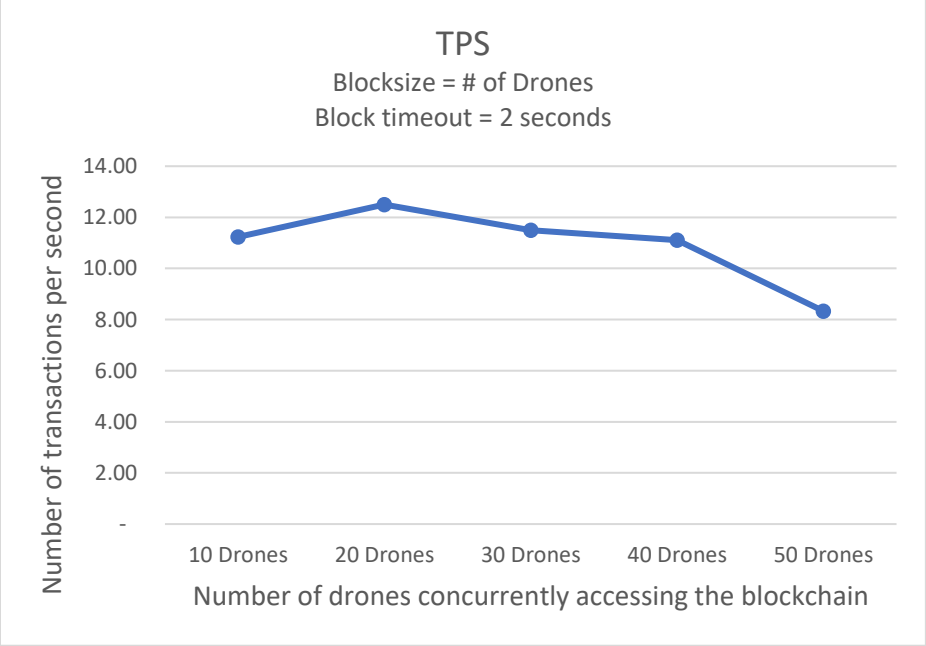


Figure 57- Performance (TPS) where the block size = concurrent clients

5.2.1.3. Block size vs increasing number of clients

In order to demonstrate the full impact of changes in the test variables, we included the graphs showing the performance of our system for each tested block size. The below graphs show how the peak performance of the system for each block size change is related to the number of

concurrent clients. For each network setting below, the peak performance is accomplished when the block size is set to be the same value as the number of concurrent clients.

When the block size of the blockchain is set to 20 transactions, we observed the peak performance where 20 drones were accessing to the blockchain concurrently. The variation of the performance with respect to changing concurrent clients is shown in Figure 58.

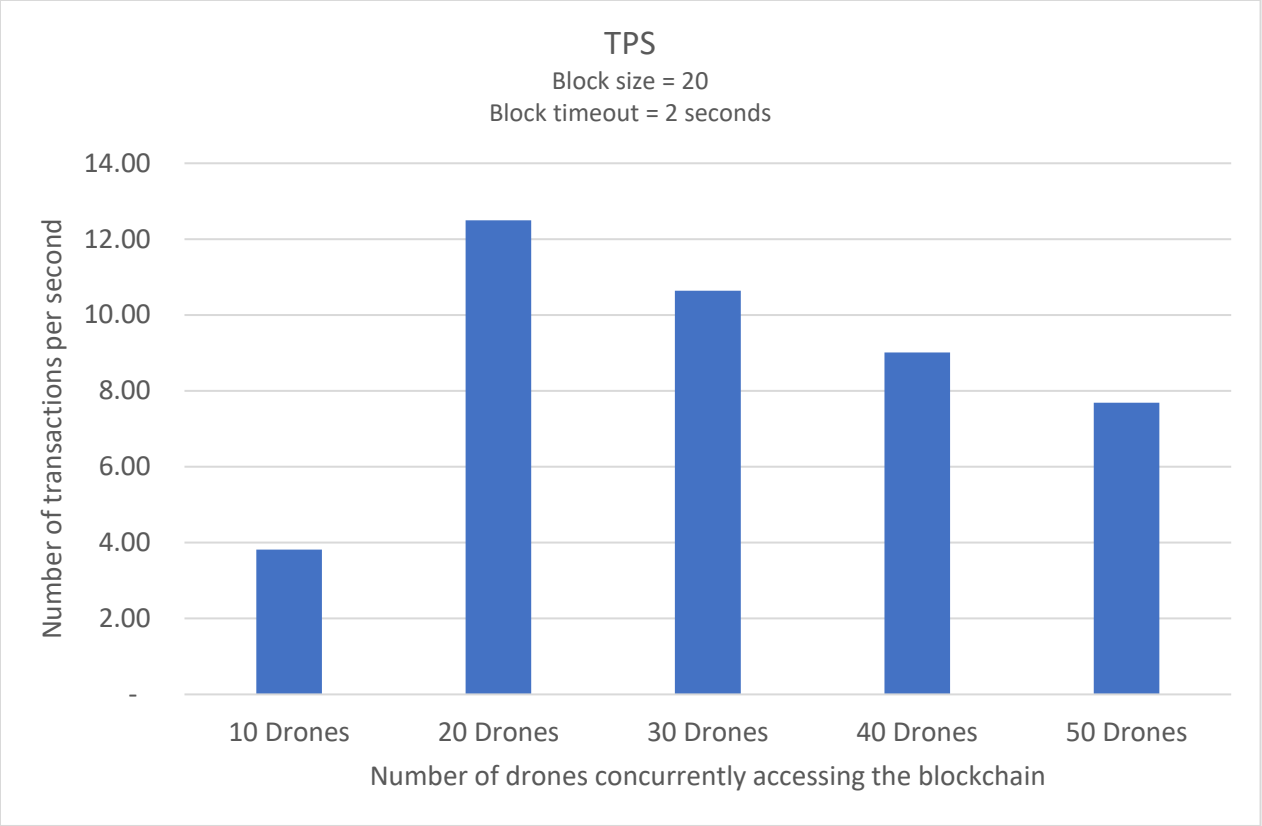


Figure 58- Performance (TPS) with increasing concurrency (block size = 20)

When the block size of the blockchain is adjusted to 30 transactions, we observed the peak performance at the experiment where 30 drones were accessing to the blockchain concurrently. The variation of the performance with respect to changing concurrent clients is shown in Figure 59 .

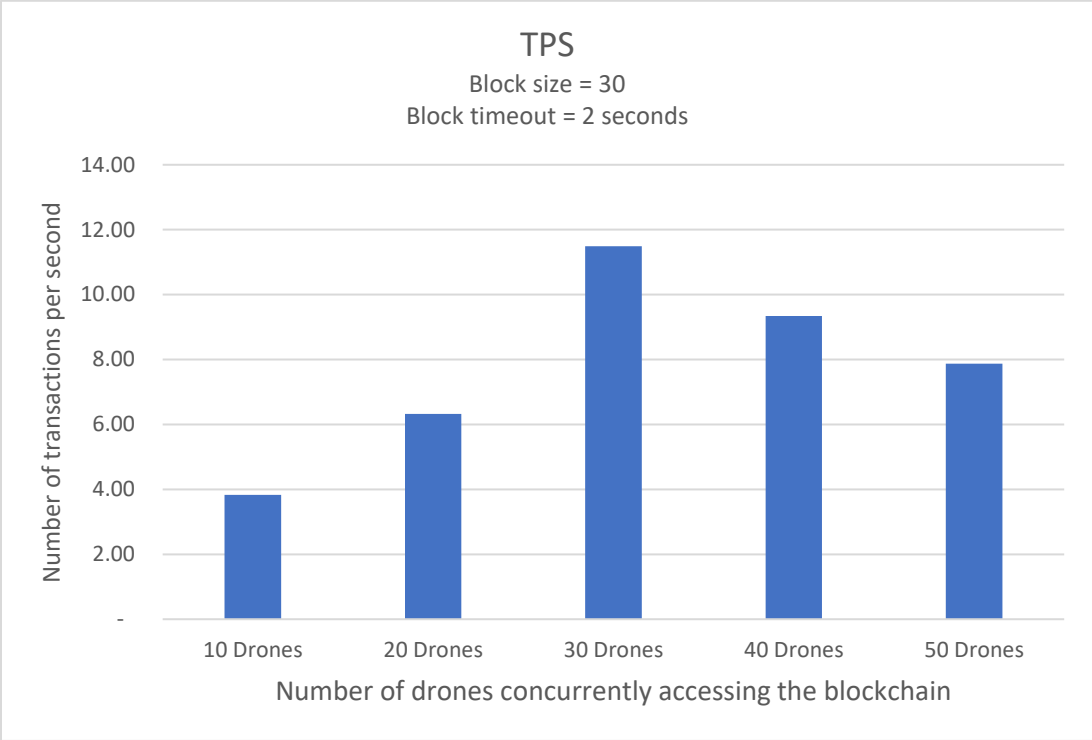


Figure 59- Performance (TPS) with increasing concurrency (block size = 30)

Figure 60 and Figure 61 are included in order to show that this observation is uniform. When the block size of the blockchain is adjusted to 40 transactions or 50 transactions, we observed the peak performance at the experiment where number of drones accessing to the blockchain concurrently was equal to the number of transactions that form a block.

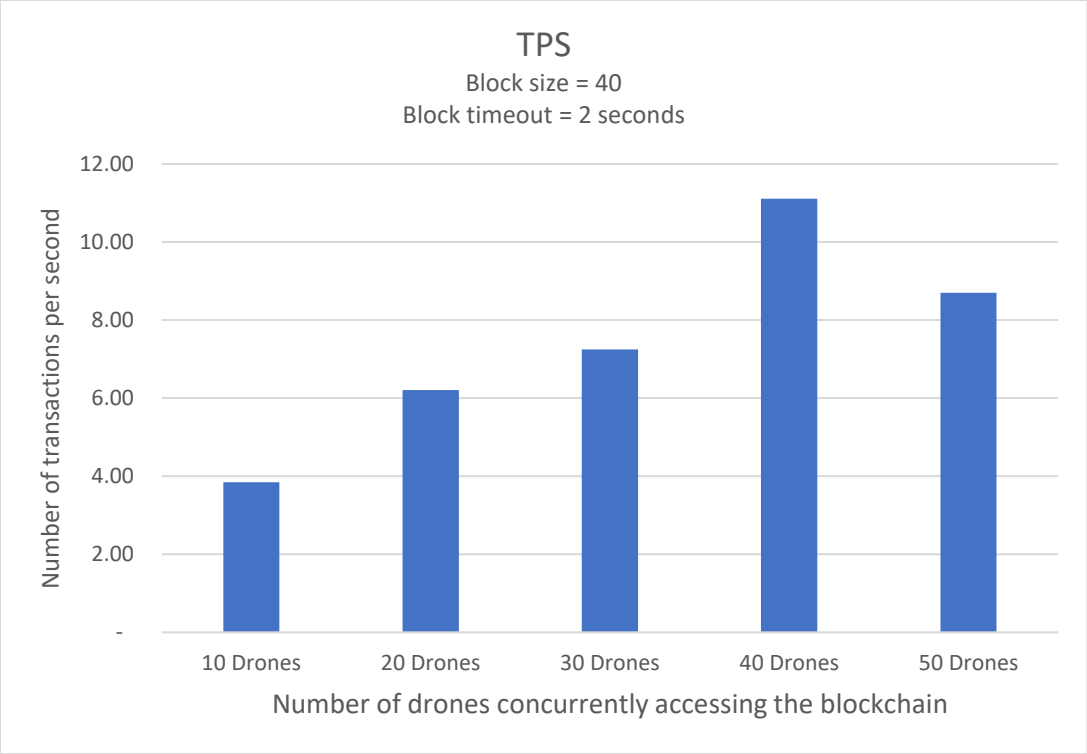


Figure 60- Performance (TPS) with increasing concurrency (block size = 40)

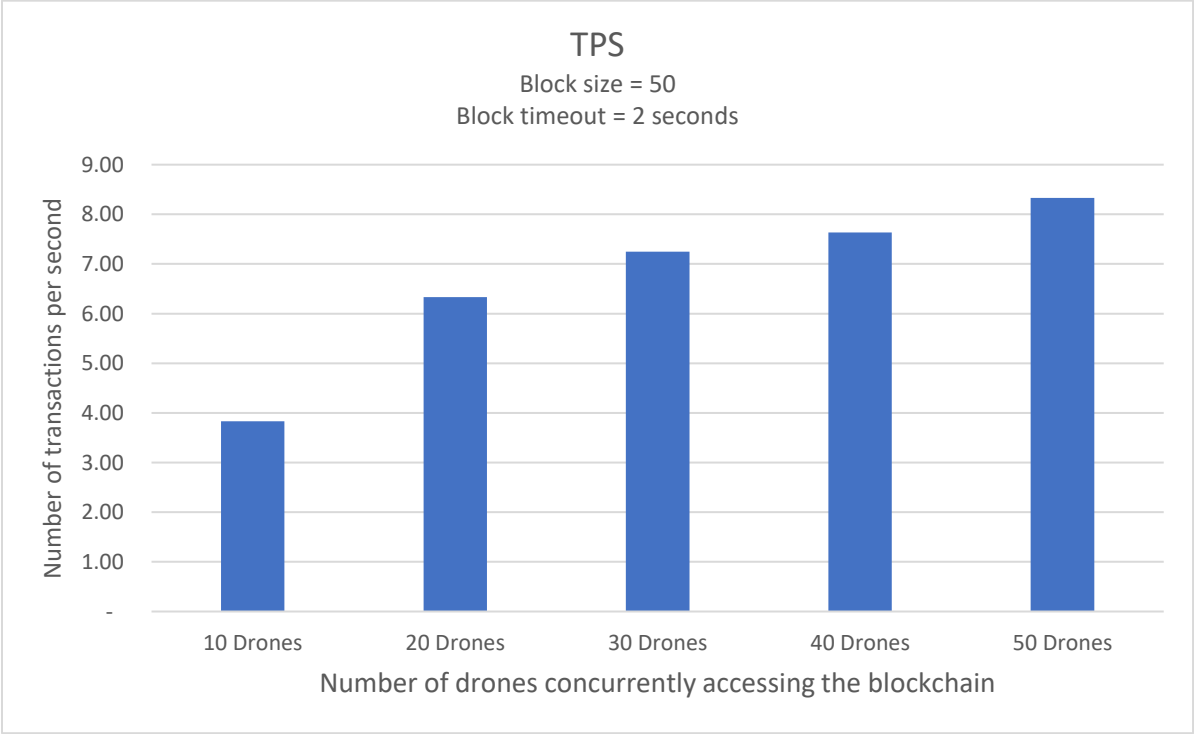


Figure 61- Performance (TPS) with increasing concurrency (block size = 50)

What we have found in this analysis indicates that the blockchain systems have their difference with other client-interaction based systems such as web servers. In this experiment we clearly demonstrated the client delay and peak performance requirements for the blockchain systems. Since block size and the block timeout parameters define the transaction completion for each client issuing their transactions in a time frame, the number of concurrent clients equal to the block size maximizes the throughput.

5.2.1.4. Overall distribution

The diagram below is a summary of the variety of the settings we tested as part of our load testing. The labels in the X-axis indicate the number of concurrent clients, block size and the timeout value for block creation. The number after 'D' designates the number of concurrent clients. The number after 'B' designates the block size for the blockchain network. The number after 'T' is the block creation timeout value.

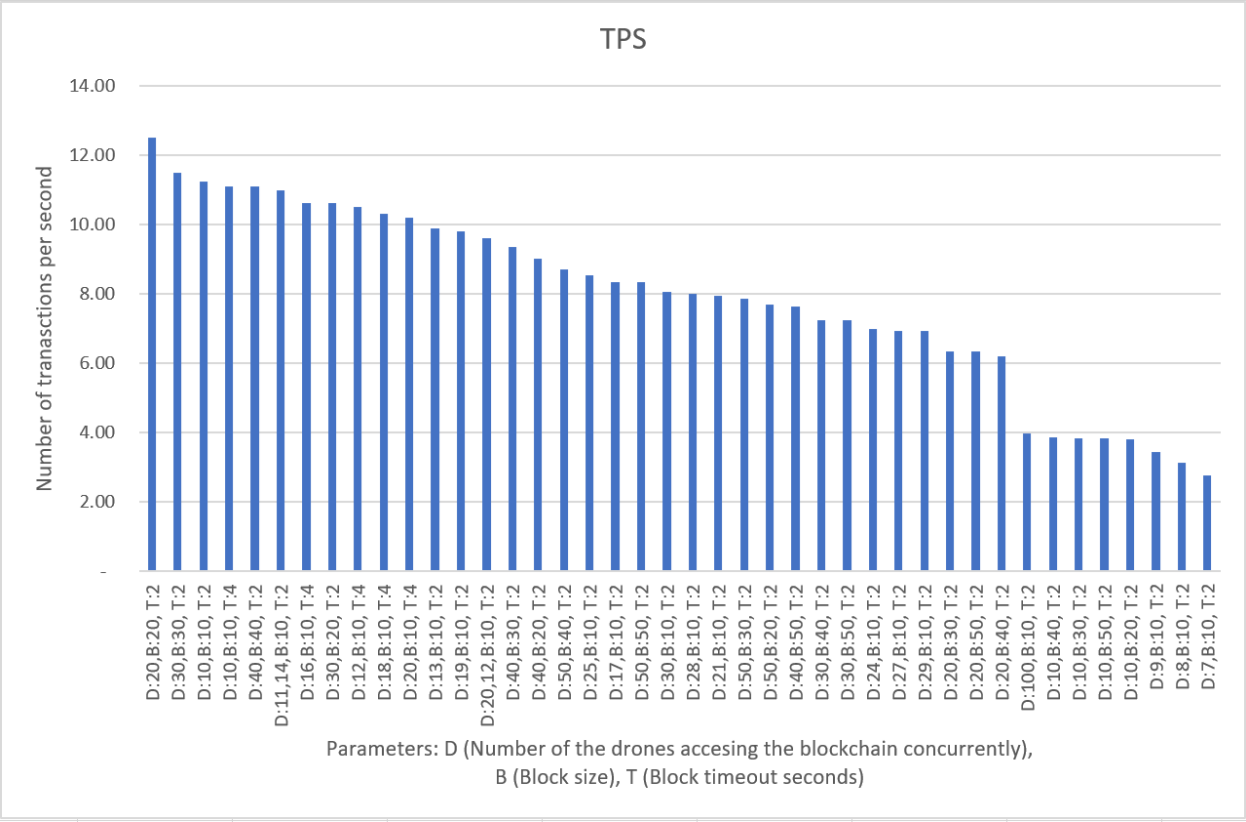


Figure 62- Summary of the performance metrics for all load test experiments

5.2.2. Latency

During our experiments, we collected several statistics, including the latency for each concurrent client. Latency in blockchain transactions is the amount of time a client is waiting from sending a transaction to the blockchain until successful completion of the transaction. Until a transaction is added to a block, our blockchain does not return a successful response. The diagram below displays a summary of these values. While the number of concurrent clients increases, the latency increases. Clients wait for more for each transaction where there is an increasing number of concurrent clients. Each client waits more than three times in the 50 concurrent clients, and the maximum of this wait time may be more than five times the maximum wait time where there are ten concurrent clients. We believe the simulation application also has an impact on this value to enlarge as 50 threads using the same set of resources would diminish the performance of the system.

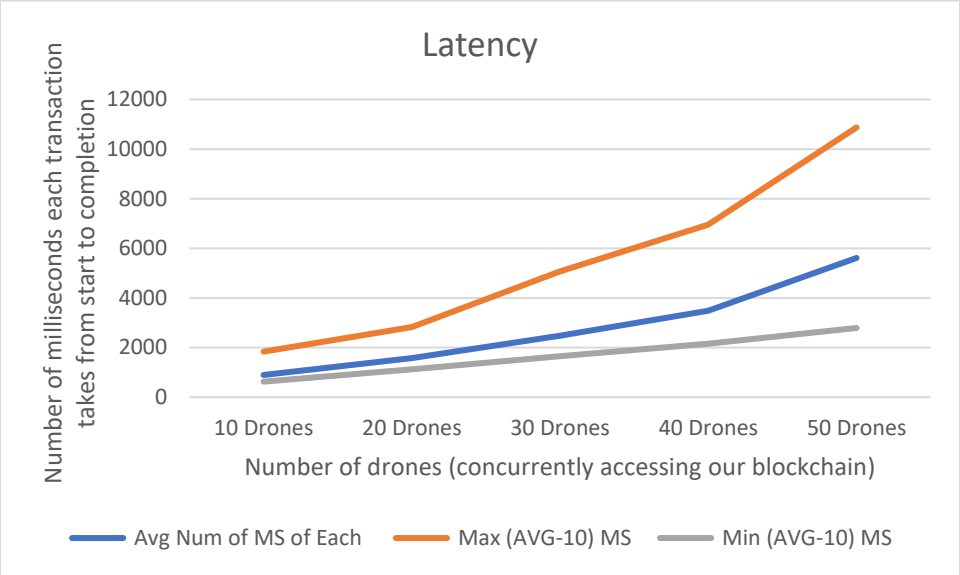


Figure 63- Latency on the system where number of concurrent clients = block size

In the drone flight scenario, each drone spending an increasing amount of time to conduct blockchain transactions certainly is not desired. However, considering the total amount of time each drone will spend flying, loading the drones and changing batteries, even the maximum value of ten seconds is not high.

We analyzed the latency for our system to find out the configuration that would result in the observation of peak performance. Below is a diagram that analyses latency changes with the

change of the number of concurrent clients. The increase in the number of concurrent clients shows an unusual behaviour around the point where the number of concurrent clients is close to the block size. (For this graph the block size is 10). However, overall, there is a steady increasing trend for the average, minimum and maximum values. As the blockchain network creates its blocks for the clients, more clients issuing transactions means more clients are waiting. Two factors are essential in our load test. First, all clients are continuously issuing transactions. As they finish one transaction, they immediately issue the next one. Moreover, the next factor is the simulation software managing the clients with threads. These threads are sharing resources and cycles from the same resources.

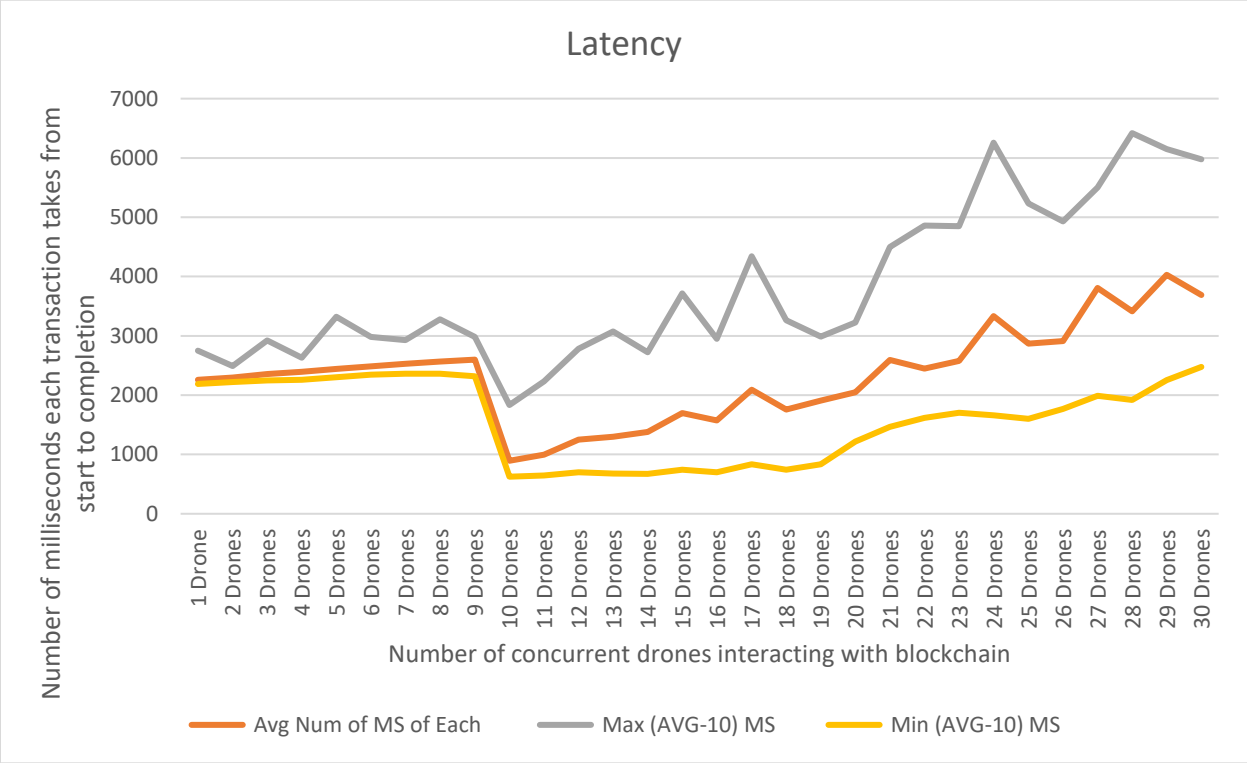


Figure 64- Latency change with growing number of clients

5.2.3. Conclusion of the Load Tests

We calculated earlier that we need to deliver items to 17546 different addresses for our aid distribution scenario. From the load testing perspective, we adopt this large number ignoring whether the physical delivery is possible or not. For these addresses, we run the blockchain simulation with its peak performance settings of twenty concurrent clients with a block size of twenty. Twenty concurrent clients can represent twenty drones delivering items in an instant and immediately continue on their next deliveries without any flight, loading, battery replacement or downtime.

Completing all deliveries took 22 minutes and 43 seconds. Each transaction took 77.68 milliseconds, achieving 12.87 transactions per second.

This performance indicates that if each drone would issue a blockchain transaction for each delivery, approximately 23 minutes of this operation will be spent on blockchain operations. These results show that the blockchain-related additional time cost is insignificant. Blockchain technology does not bring any additional cost to the overall system in terms of performance.

With an assumption of each drone completing each delivery task in 10 minutes, the per delivery weight of a one message blockchain transaction is 0.012947%. Issuing 77 blockchain transactions for each delivery would make the blockchain transaction time cost to increase to 1% of overall delivery.

The average distance to a delivery target is 8.2 km, and the return trip is 16.4 km. With the assumption that each drone can fly 100km/hr, completing each delivery task will average to 4.8 minutes, the per delivery weight of a one message blockchain transaction is 0.027%. Issuing 37 blockchain transactions for each delivery would make the blockchain transaction time cost to increase to 1% of overall delivery. These figures indicate that issuing aid delivery transactions on a blockchain network is possible.

5.3. Physical Delivery Projections

Our load testing proved that the blockchain technology could be a backend for the aid delivery, and we can store records that assure the delivery in an immutable system. Our simulations can be projected to the events of physical delivery. However, several factors need to be considered. We will review these factors and calculate the time needed to deliver the planned aid in our experiment.

5.3.1. Performance Analysis Results

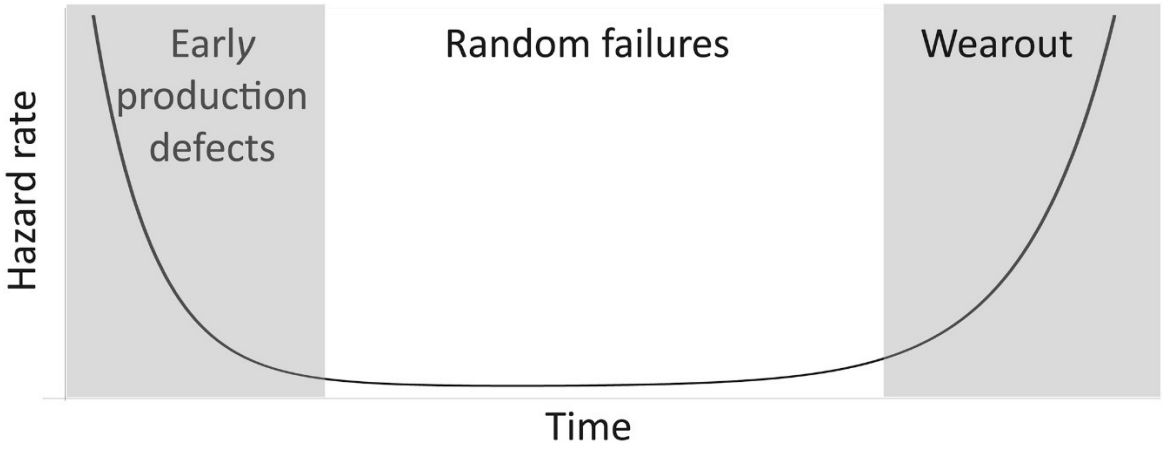
Results of the performance analysis is summarized in Table 17. When we analyze the distances from our crisis centre to the delivery targets, we calculated the average distance to delivery targets as 8.2 km. The farthest address is 18494 meters away from our crisis centre. The total distance to be flown is 143339831 meters. Approximately 143340 km. This number is 3.58 times the earth's circumference. If each drone would make a single delivery at each time, the total distance becomes 286680 km. With 100km/hr drone speed, this distance would translate to 2868 hours of UAV flight. With 100 drones, our planned aid mission concludes in approximately 28.7 hours. Two hundred drones would reduce the time to approximately 14.4 hours. Since each UAV will fly approximately 4.8 minutes to serve average distance, one drone would create one transaction every 4.8 minutes. One hundred drones will need a throughput of 0.35 TPS, and two hundred drones would need 0.69 TPS. Alternatively, the peak performance of 12.87 TPS would serve approximately 3707 drones with one message per delivery scenario.

Table 17- Summary of findings

Experiment Findings	**Value**	**Comments**
Average distance of delivery targets	8200 meters	
The farthest address	18494 meters	
The total distance to be flown	143,339,831 meters	3.58 times the earth's circumference
Number of deliveries at each mission	1	
Drone speed	100km/hr	
Total flight hours	2868 hours	
Number of drones planned	200	
Total time of mission	28.7 hrs with 100 drones 14.4 hrs with 200 drones	
Performance requirement	0.35 TPS for 100 drones 0.69 TPS for 200 drones	
Expected time for each transaction per drone	4.8 minutes	
Maximum number of drones for our blockchain	3707 drones	

5.3.2. Physical Failures

Reliability engineering literature indicates that complex components and systems failures can be represented with a bathtub curve [363] as in Figure 65. These complex components and systems fail in greater rates at the beginning of their utilization as low-quality components with defects fail fast. After the initial usage, for a long period of usage, the failure rate is lowest as failures are limited to random failures. We assume the initial quality control tests and initialization procedures eliminate the dead-on-arrival equipment. Therefore, we will start our process with the low probability of having a failure. We will increase the probability towards the wear-out period.



[363]

Figure 65- Bathtub curve of the drone failures

Table 18 is a categorization of the addresses that we deliver aid with distances to the crisis centres. We also added possible failure ratios in order to estimate the number of failures. The literature includes a wide range of failure numbers. For each UAV one failure is foreseen for each 1000 hours of flight [364]. We translate this number to be 0.1% failure rate for each one-hour flight. This is our random rate of failure in the bathtub curve. After 14000 meters of flight range we start increasing the probability exponentially, as shown in the below table. The percentage of failures is a factor in the total time of completion for all of the delivery jobs. Excessive failures also can result in failure of overall delivery tasks. However, the total number of failures has no impact on the blockchain load. Whether new UAVs would be started, or the operations would continue with fewer drones are operational decisions. The impact on the blockchain system is either the same, or would result in less load. The below table estimates 70 failures throughout the entire delivery process. If there are 200 drones to start, only 130 of them can survive. All these numbers are in our acceptable ranges.

Table 18- Failure rate distribution estimation

Distance (d) from our crisis centre	**# of delivery destinations**	**Estimated failure rate**	**# of failure**
d<12000	11459	0.1%	12
12000=<d<13000	304	0.1%	1
13000=<d<14000	363	0.1%	1
14000=<d<15000	736	0.2%	2
15000=<d<16000	546	0.4%	3
16000=<d<17000	2314	0.8%	19
17000=<d<18000	1687	1.6%	27
18000=<d	137	3.2%	5

We also analyzed the impact of battery changes. The battery change operations have no impact on the blockchain system performance. However, they can be considered a factor in calculating the total time it will take to complete the disaster relief. The table presented below details the analysis that indicates 5586 battery changes would be needed until the end of the entire delivery operation, considering each battery supports only 100 km of flight. This number seems operationally and logistically challenging. We consider this challenge as the inherent challenge of drone flights. The total number of batteries to replace is proportional to the total flight distance. As a summary, this number is not a factor that has an impact on the blockchain solution.

Distance (d) from our crisis centre	**# of delivery destinations**	**# of flights with a single battery**	**# of battery changes**
d<12000	11459	4	2865
12000=<d<13000	304	3	102
13000=<d<14000	363	3	121
14000=<d<15000	736	3	246
15000=<d<16000	546	3	182
16000=<d<17000	2314	2	1157
17000=<d<18000	1687	2	844
18000=<d	137	2	69

6. Conclusion and Future Work

In this thesis, we have designed an implementation framework for blockchain-based delivery assurance. Whether it is a classic implementation of parcel delivery or a modern implementation by drone delivery or aid delivery as disaster relief, our implementation framework guides the implementation to inject trust into the business processes using blockchain distributed ledger technology. We identified and implemented a specific application scenario of the delivery assurance framework, which is a blockchain-based aid delivery assurance.

While solving the blockchain-based aid delivery problem, we answered our research questions. We provided a framework to guide us on using blockchain technology to solve problems. This framework defined steps that we should follow. We provided a framework for analyzing whether the designed blockchain-based solution is financially viable and acceptable. This framework defines the criteria and points of view. We analyzed the security and automation aspects of blockchain technology. We defined methods to automate business operations in a blockchain and the steps to take about the security aspect of our implementation.

We focused on disaster recovery and provided use cases showing disaster recovery is a suitable target for blockchain implementations. We detailed the value that blockchain brings to disaster recovery efforts and services. As our aid delivery scenario uses autonomous vehicles, we defined the value proposition of blockchain technology for the services provided by autonomous vehicles.

Our main contribution is a framework that guides blockchain technology use in the delivery industry. The techniques to model delivery business as a blockchain and the steps of this process are detailed in this thesis. The role blockchains play in assuring delivery is detailed through the analysis.

For our application scenario of aid delivery assurance, we implemented the required blockchain solution using Hyperledger technology. We experimented with the ability of this solution to address the capacity and capability concerns. Our load tests and analysis results have shown us that our blockchain functions correctly and has a high capacity in specific configurations. With these load testing results and identified performance metrics, we have analyzed the chosen experiment domain with the disaster scenario where we defined our aid items. We identified a

superset of the delivery targets and enriched this data with attributes that helped us with different disaster scenarios. We have created a specific disaster scenario of a flood in Toronto, ON, which helped us define the specific target delivery destinations. We plotted these specific targets on a map, identified our crisis centre, and simulated the aid delivery. We have shown that the blockchain technology provides the assurance infrastructure to the autonomous vehicle-based delivery service.

Our experiment has shown that achieving high throughput numbers is possible. We identified the configurations that provided the highest throughput. We also identified the latency values at each configuration. We have concluded that the performance metrics in the result of this experiment is sufficient for running a large aid delivery. From a throughput perspective, our aid delivery blockchain implementation has the capacity to accomplish the large number of deliveries we targeted. From a latency perspective, we have proven that the latency we would introduce to the system is negligible compared to the duration of the physical operation. We also showed that UAV failures, as well as the battery changes, do not pose a risk on our blockchain implementation.

Our simulation has focused on blockchain technology with its benefits and capabilities. We have listed our limitations, constraints and dependencies. Most significant constraints were identified around the maturity of autonomous delivery and network connectivity. We have conducted our experiment with the note indicating these concerns are addressed with realistic assumptions.

Our simulation includes a flood scenario where used realistic assumptions on several factors in order to design our experiment. All our assumptions are shared as part of this thesis. Future research may build on our assumptions or improve them where more precise data is available.

Our simulation study validates the applicability of our framework and the solution we created using the framework. Further, the validation we received from an industry expert strongly suggests that a solution developed with our framework is applicable in industry.

Our work improves the aid delivery processes with the addition of assurance using the immutable records of the blockchain technology. Where there are multiple untrusting stakeholders, blockchain technology is a recipe for cryptography-based trust injection over distributed records.

Several new projects can be developed to follow our work. Drones surveying the disaster scenes while delivering the packages would be a great benefit to the stakeholders. Rescue teams, insurance companies, governments and the public can benefit from this extra information. This way, we have an intelligently recreated map of the disaster area, which is usually different than the map from pre-disaster times. Destroyed bridges, as well as newly formed rubble bridges, are good examples of notable variations between the before and after disaster maps.

With AI, drones can recognize the existence of people and deliver aid for these people. Future work can improve targeting and rerouting to alternate targets with AI-based decisions.

In our study, we observed that the performance metrics of the blockchain application are optimum when there is a stream of transactions coming to the blockchain platform that will not create a queue of clients, and that will not be too small compared to the expected flow. This performance peak can be accomplished by planning the delivery events in order to create a desired inflow of transactions. Since most of the variables for the flights such as distance and speed are known, aim of the scheduling process would be eliminating peaks. If the drones would be assigned to tasks that would create events in a uniform distribution, the load on the system would be uniform, and the performance would be maximum. A scheduler can be developed for the blockchain applications that will schedule the UAV flights and assign destinations in order to optimize the performance of the blockchain.

Another future direction of our work is to create a framework that can guide the implementation of our disaster delivery blockchain solution to other cities. Disaster management offices in each city can plan for the recovery of the next possible disaster including the implementation of our proposed solution. In our experiment we identified an area with 17546 addresses to be serviced with 200 drones in 14.4 hours. Planning can account for the values we identified towards calculation of the resources, timelines and coverage of the next disaster recovery.

Bibliography

[1] S. Meiklejohn, "Top Ten Obstacles along Distributed Ledgers Path to Adoption," *IEEE Security & Privacy,* vol. 16, no. 4, pp. 13 - 19, 2018.

[2] M. Demir, O. Turetken and A. Mashatan, "An Enterprise Transformation Guide for the Inevitable Blockchain Disruption," *IEEE Computer (Accepted),* © 2020 IEEE. Reprinted, with permission.

[3] M. Demir, O. Turetken and A. Ferworn, "A Financial Evaluation Framework for Blockchain Implementations," in *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC © 2019 IEEE. Reprinted, with permission, 2019.

[4] M. Demir, M. Alalfi, O. Turetken and A. Ferworn, "Security Smells in Smart Contracts," in *IEEE International Conference on Software Security and Reliability (QRS)*, Sofia, Bulgaria © 2019 IEEE. Reprinted, with permission, 2019.

[5] M. Demir, A. Mashatan, O. Turetken and A. Ferworn, "Utility Blockchain for Transparent Disaster Recovery," in *IEEE Electrical Power and Energy Conference (EPEC)*, Toronto,ON © 2019 IEEE. Reprinted, with permission, 2018.

[6] M. Demir, O. Turetken and A. Ferworn, "Blockchain Based Transparent Vehicle Insurance Management," in *Sixth International Conference on Software Defined Systems (SDS*, Rome, Italy © 2019 IEEE. Reprinted, with permission, 2019.

[7] M. Demir, O. Turetken and A. Ferworn, "Blockchain and IoT for Delivery Assurance on Supply Chain (BIDAS)," in *IEEE Big Data 2019- IoT Big Data and Blockchain (IoTBB'2019)*, Los Angeles, California © 2019 IEEE. Reprinted, with permission, 2019.

[8] M. Demir, O. Turetken and A. Ferworn, "Blockchain-Based Transparent Disaster Relief Delivery Assurance," in *IEEE SysCon 2020 (Accepted)*, Montreal, QC © 2020 IEEE. Reprinted, with permission, 2020.

[9] D. O. Manz and T. W. Edgar, "Science and Cyber Security," in *Research Methods for Cyber Security*, Syngress, 2017, pp. 33-62.

[10] N. Kishore and P. Raina, "Parallel cryptographic hashing: Developments in the last 25 years," *Cryptologia,* vol. 43, no. 6, pp. 504-535, November 2019.

[11] F. Ablayev and M. Ablayev, "On the Concept of Cryptographic Quantum Hashing," *Arxiv,* no. 1509.01268, 2015.

[12] S. Garfinkel, "https://www.technologyreview.com/s/402961/fingerprinting-your-files/," MIT Technology Review, 4 August 2004. [Online]. Available: https://www.technologyreview.com/s/402961/fingerprinting-your-files/.

[13] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," [Online]. Available: https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf. [Accessed 9 February 2019].

[14] Microsoft, "Get-FileHash," Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-6. [Accessed 06 11 2019].

[15] "Public key cryptography," IBM, [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7pkey.html. [Accessed 9 February 2019].

[16] "What Is a Digital Signature?," Comodo Certification Authority, [Online]. Available: https://www.instantssl.com/https-tutorials/digital-signature.html. [Accessed 9 February 2019].

[17] "Digital signatures," IBM, [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7dsign.html. [Accessed 9 February 2019].

[18] P. Baran, "On Distributed Communications Series. I. Introduction to Distributed Communications Networks," RAND, [Online]. Available: https://www.rand.org/pubs/research_memoranda/RM3420/RM3420-chapter1.html. [Accessed 9 February 2019].

[19] I. Lee, "CIS 505: Software Systems," 2007. [Online]. Available: https://www.cis.upenn.edu/~lee/07cis505/Lec/lec-ch1-DistSys-v4.pdf. [Accessed 31 October 2019].

[20] SolarWinds, "Centralized Networks vs Decentralized Networks," 30 November 2018. [Online]. Available: https://www.solarwindsmsp.com/blog/centralized-vs-decentralized-network.

[21] A. Bartoli, M. Dohler, A. Kountouris and D. Barthel, "Advanced security taxonomy for machine-to-machine (M2M) communications in 5G capillary networks," in *Machine-to-machine (M2M) Communications*, WP, 2015, pp. 207-226.

[22] A. C. Regan and R. Chen, "Vehicular ad hoc networks," in *Vehicular Communications and Networks*, WP, 2015, pp. 29-35.

[23] X. Chen, R. Tharmarasa and T. Kirubarajan, "Multitarget Multisensor Tracking," in *Academic Press Library in Signal Processing*, Elsevier, 2014, pp. 759-812.

[24] J. Hall and e. al, "A Survey of Worldwide Censorship Techniques," Network Working Group, 25 May 2018. [Online]. Available: https://tools.ietf.org/id/draft-hall-censorship-tech-05.html.

[25] H. Partz, "Major Content Delivery Network Introduces Decentralized Content Gateway," Cointelegraph, 18 September 2018. [Online]. Available: https://cointelegraph.com/news/major-content-delivery-network-introduces-decentralized-content-gateway.

[26] A. Parker, "Cloudflare goes InterPlanetary - Introducing Cloudflare's IPFS Gateway," Cloudflare , 17 September 2018. [Online]. Available: https://blog.cloudflare.com/distributed-web-gateway/.

[27] D. Mullins, H. Whitehouse and Q. D. Atkinson, "The Role Of Writing And Recordkeeping In The Cultural Evolution Of Human Cooperation," Evolution Institute, 3 July 2013. [Online]. Available: https://evolution-institute.org/the-role-of-writing-and-recordkeeping-in-the-cultural-evolution-of-human-co/.

[28] R. Kuhn, D. Yaga and J. Voas, "Rethinking Distributed Ledger Technology," *Computer,* vol. 52, no. 2, pp. 68-72, 2019.

[29] D. Burkhardt, M. Werling and H. Lasi, "Distributed Ledger," in *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Stuttgart, 2018.

[30] WorldBank, "Blockchain & Distributed Ledger Technology (DLT)," WorldBank, 12 April 2018. [Online]. Available: https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt.

[31] H. Garcia-Molina and R. K. Abbott, "Reliable distributed database management," *Proceedings of the IEEE,* vol. 75, no. 5, pp. 601-620, May 1987.

[32] R. G. Brown, "On Distributed Databases and Distributed Ledgers," 8 November 2016. [Online]. Available: https://gendal.me/2016/11/08/on-distributed-databases-and-distributed-ledgers/.

[33] S. Brakeville and B. Perepa, "Blockchain basics: Introduction to distributed ledgers," IBM, 1 June 2019. [Online]. Available: https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/.

[34] L.-D. Ibanez, E. Simperl, F. Gandon and H. Story, "Redecentralizing the Web with Distributed Ledgers," *IEEE Intelligent Systems,* vol. 31, no. 1, pp. 92-95, 2017.

[35] S. Popov, "The Tangle," 01 October 2017. [Online]. Available: https://iota.org/IOTA_Whitepaper.pdf. [Accessed 10 October 2017].

[36] S. Park and H. Kim, "DAG-Based Distributed Ledger for Low-Latency Smart Grid Network," *Energies ,* vol. 12, no. 18, p. 3570, 2019.

[37] M. Hearn, "Corda: A distributed ledger," 29 November 2016. [Online]. Available: https://docs.corda.net/_static/corda-technical-whitepaper.pdf. [Accessed 31 12 2017].

[38] J. Young, "Cryptocurrency still a long journey ahead," Cointelegraph, 24 September 2017. [Online]. Available: https://cointelegraph.com/news/cryptocurrency-still-a-long-journey-ahead.

[39] C. Blenkinsop, "Blockchain's Scaling Problem, Explained," ConinTelegraph, 22 August 2018. [Online]. Available: https://cointelegraph.com/explained/blockchains-scaling-problem-explained.

[40] M. Walport, "Distributed Ledger Technology: beyond block chain," 19 January 2016. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[41] S. Underwood, "Blockchain Beyond Bitcoin," *Communications of the ACM,* vol. 59, no. 11, pp. 15-17, 2016.

[42] N. Chowdhury, Inside Blockchain, Bitcoin, and Cryptocurrencies, Auerbach Publishers, Incorporated , 2019.

[43] V. Buterin, "Merkling in Ethereum," 15 November 2015. [Online]. Available: https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/. [Accessed 6 February 2018].

[44] M. Belotti, N. Božić, G. Pujolle and S. Secci, "A Vademecum on Blockchain Technologies: When, Which and How," *IEEE Communications Surveys & Tutorials,* 2019.

[45] A. Chepurnoy, M. Larangeira and A. Ojiganov, "Rollerchain, a Blockchain With Safely Pruneable Full Blocks," 23 August 2016. [Online]. Available: https://arxiv.org/pdf/1603.07926.pdf.

[46] E. Palm, O. Schelén and U. Bodin, "Selective Blockchain Transaction Pruning and State Derivability.," in *Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018.

[47] Y. Yang, "Blockchain data accepted as evidence in legal complaint filed by short video app Douyin," South China Morning Post, 13 September 2018. [Online]. Available: https://www.scmp.com/tech/policy/article/2163914/blockchain-data-accepted-evidence-legal-complaint-filed-short-video-app.

[48] "Blockchain and Evidence Records — A Match Made In Tamper Proof Heaven," veridocglobal, 21 April 2019. [Online]. Available: https://medium.com/@veridocglobal/blockchain-and-evidence-records-a-match-made-in-tamper-proof-heaven-1c7e8ab1ad9c.

[49] J. Palfreyman, "Proving Provenance with Blockchain," IBM, 17 March 2016. [Online]. Available: https://www.ibm.com/blogs/insights-on-business/government/proving-provenance-with-blockchain/.

[50] R. Lons, "From the "Genesis Block" to Tim Draper's big buy: A History of Bitcoin," *PandoDaily,* 2014.

[51] M. Vidrih, "What Is a Block in the Blockchain?," Medium, 29 December 2018. [Online]. Available: https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373.

[52] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf. [Accessed 10 October 2017].

[53] E. Duffield and D. Diaz, "Dash: A Privacy-Centric Crypto-Currency," [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper. [Accessed 31 12 2017].

[54] S. Gauld, F. v. Ancoina and R. Stadler, "The Burst Dymaxion -An Arbitrary Scalable, Energy Efficient and Anonymous Transaction Network Based on Colored Tangles," 27 December 2017. [Online]. Available: https://www.burst-coin.org/wp-content/uploads/2017/07/The-Burst-Dymaxion-1.00.pdf. [Accessed 31 December 2017].

[55] W. Ren, J. Hu, T. Zhu, Y. Ren and K.-K. R. Choo, "A flexible method to defend against computationally resourceful miners in blockchain proof of work," *Information Sciences,* vol. Information Sciences, pp. 161-171, 2020.

[56] V. Durnev, D. Murin, V. Sokolov and D. J. Chalyy, "On Some Approaches to the Solution of the "Useful Proof-of-Work for Blockchains" Task," *Automatic Control and Computer Sciences,* vol. 52, no. 7, p. 880–884, 2018.

[57] N. Shi, "A new proof-of-work mechanism for bitcoin," *Financial Innovation,* vol. 2, no. 31, 2016.

[58] Y. Xu and Y. Huang, "MWPoW: Multiple Winners Proof of Work Protocol, a Decentralisation Strengthened Fast-Confirm Blockchain Protocol," *Security and Communication Networks,* 2019.

[59] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," *IEEE Access,* vol. 7, pp. 85727-85745, 2019.

[60] E. Deirmentzoglou, G. Papakyriakopoulos and C. Patsakis, "A Survey on Long-Range Attacks for Proof of Stake Protocols," *IEEE Access,* vol. 7, pp. 28712-28725, 2019.

[61] S. Dziembowski, S. Faust, V. Kolmogorov and K. Pietrzak, "Proofs of Space," [Online]. Available: https://eprint.iacr.org/2013/796.pdf. [Accessed 19 January 2018].

[62] https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/, "Consensus Algorithms in Blockchain," Geeksforgeeks, [Online]. Available: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/. [Accessed 25 November 2019].

[63] D. Massessi, "Public Vs Private Blockchain In A Nutshell," CoinMonks, 12 December 2018. [Online]. Available: https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f.

[64] N. Kobie, "How much energy does bitcoin mining really use? It's complicated," 2 December 2017. [Online]. Available: http://www.wired.co.uk/article/how-much-energy-does-bitcoin-mining-really-use. [Accessed 6 February 2018].

[65] A. Malanov, "Why blockchain is not such a bad technology," 28 September 2017. [Online]. Available: https://www.kaspersky.com/blog/good-good-blockchain/19575/. [Accessed 6 February 2018].

[66] J. Chen, "Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks," *ACM SIGBED Review,* vol. 15, no. 5, pp. 22-28 , 2018.

[67] D. Yafimava, "What are Consortium Blockchains, and What Purpose do They Serve?," Blockchain insights, 15 January 2019 . [Online]. Available: https://openledger.info/insights/consortium-blockchains/.

[68] M. Beedham, "Here's the difference between 'permissioned' and 'permissionless' blockchains," Hard Fork, 5 November 2018. [Online]. Available: https://thenextweb.com/hardfork/2018/11/05/permissioned-permissionless-blockchains/.

[69] https://hyperledger-fabric.readthedocs.io/en/latest/, "Welcome to Hyperledger Fabric," IBM, [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/. [Accessed 3 February 2018].

[70] "Best Practices for Running a Permissioned Blockchain Network in a Regulated Production Environment," Consensys, 8 October 2019. [Online].

[71] R. Nagpal, "17 blockchain platforms — a brief introduction," Medium, 12 April 2017. [Online]. Available: https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b.

[72] L. Feng, H. L. Zhang and S. Sun, "System architecture for high-performance permissioned blockchains," *Frontiers of Computer Science ,* 2018.

[73] N. Kolokotronis, K. Limniotis, S. Shiaeles and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," *IEEE Consumer Electronics Magazine,* vol. 8, no. 3, pp. 28-34, 2019.

[74] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with Accountable Mixes," Princeton , [Online]. Available: https://wws.princeton.edu/faculty-research/research/item/mixcoin-anonymity-bitcoin-accountable-mixes. [Accessed 2 December 2019].

[75] Y. Cao, Y. Li, Y. Sun and S. Wang, "Decentralized Group Signature Scheme Based on Blockchain," in *2019 International Conference on Communications, Information System and Computer Engineering (CISCE)*, Haikou, China, 2019.

[76] L. Wang, X. Shen, J. Li, J. Shao and Y. Yang, "Cryptographic primitives in blockchains," *Journal of Network and Computer Applications,* vol. 127, pp. 43-58, 2019.

[77] L. Malina, J. Hajny, P. Dzurenda and S. Ricci, "Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions," in *15th International Joint Conference on e-Business and Telecommunications*, Porto, Portugal, 2018.

[78] B. Wang, J. Sun, Y. He, D. Pang and N. Lu, "Large-scale Election Based On Blockchain," *Procedia Computer Science,* vol. 129, p. 234, 2018.

[79] R. Zhang and R. Xue, "Security and Privacy on Blockchain," *ACM Computing Surveys,* vol. 52, no. 3-51, p. 34, 2019.

[80] A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao and D. Zheng, "Efficient and privacy-preserving traceable attribute-based encryption in blockchain," *Annals of Telecommunications,* vol. 74, no. 7, pp. 401-411, 2019.

[81] I. Eyal, A. E. Gencer, E. G. Sirer and R. v. Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," in *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16)*, Santa Clara, CA, 2016.

[82] T. McConaghy, R. Marques, A. Mu¨ller, D. D. Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare and A. Granzotto, "BigchainDB: A Scalable Blockchain Database," [Online]. Available: https://mycourses.aalto.fi/pluginfile.php/378362/mod_resource/content/1/bigchaindb-whitepaper.pdf. [Accessed 1 March 2019].

[83] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng and J. Yu, "Direct Acyclic Graph based Blockchain for Internet of Things: Performance and Security Analysis," 25 May 2019. [Online]. Available: https://arxiv.org/abs/1905.10925.

[84] J. Kan, S. Chen and X. Huang, "Improve Blockchain Performance using Graph Data Structure and Parallel Mining," 31 October 2018. [Online]. Available: https://arxiv.org/pdf/1808.10810.pdf.

[85] C. Blenkinsop, "'Free Transactions Cleared in Five Seconds': Platform to Help Businesses Use Blockchain," cointelegraph, 7 November 2018. [Online]. Available: https://cointelegraph.com/news/free-transactions-cleared-in-five-seconds-platform-to-help-businesses-use-blockchain.

[86] Stellar, "Why is Stellar better than what exists?," Stellar.org, [Online]. Available: https://www.stellar.org/overview#why-is-stellar-better-than-what-exists. [Accessed 15 December 2019].

[87] HIMSS, "Blockchain performance throughput and scalability," HIMSS, [Online]. Available: https://www.himss.org/blockchain-performance-throughput-and-scalability. [Accessed 15 December 2019].

[88] "Technology Meant to Make Bitcoin Money Again Just Went Live," 15 March 2018. [Online]. Available: http://fortune.com/2018/03/15/bitcoin-lightning-network-technology/. [Accessed 28 April 2018].

[89] L. Mearian, "Sharding: What it is and why many blockchain protocols rely on it," ComputerWorld, 28 January 2019. [Online]. Available: https://www.computerworld.com/article/3336187/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html.

[90] RaidenNetwork, "Raiden - Fast, cheap, scalable token transfers for Ethereum," Raiden Network, [Online]. Available: https://github.com/raiden-network/raiden/?fref=ts. [Accessed 15 December 2019].

[91] M. Dalton, "Shades Of Plasma: The Many Faces Of Ethereum's Scaling Solution," CryptoBriefing, 13 July 2019. [Online]. Available: https://cryptobriefing.com/shades-plasma-ethereum-scaling/.

[92] "Blockchain speeds & the scalability debate," Blocksplain, 28 February 2018. [Online]. Available: https://blocksplain.com/2018/02/28/transaction-speeds/.

[93] E. Government, "Estonian blockchain technology," [Online]. Available: https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf. [Accessed 5 March 2019].

[94] Quorum, "What is Quorum?," JP Morgan, [Online]. Available: https://www.jpmorgan.com/global/Quorum#section_1320553510217. [Accessed 1 March 2019].

[95] "Blockchain for financial services: Bring trust, simplicity and efficiency to financial transactions with IBM Blockchain," [Online]. Available: https://www.ibm.com/blockchain/financial-services/. [Accessed 6 February 2018].

[96] G. Magyar, "Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management," in *IEEE 30th Neumann Colloquium (NC)*, Budapest, Hungary, 2017.

[97] M. Chanson, E. Fleisch, A. Bogner and F. Wortmann, "Blockchain as a Privacy Enabler: An Odometer Fraud Prevention System," in *UBICOMP/ISWC '17*, MAUI, HAWAII, 2017.

[98] N. Bore, S. Karumba, J. Mutahi, S. S. Darnell, C. Wayua and K. Weldemariam, "Towards Blockchain-enabled School Information Hub," in *In Proceedings of the Ninth International Conference on Information and Communication Technologies and Development (ICTD '17)*, New York, 2017.

[99] "Blockchain for supply chain," [Online]. Available: https://www.ibm.com/blockchain/supply-chain/. [Accessed 6 Februrary 2018].

[100] C. Sullivan and E. Burger, "E-residency and blockchain," *Computer Law & Security Review,* vol. 33, no. 4, pp. 470-481, 2017.

[101] "BC Diploma Homepage," BC Diploma, [Online]. Available: https://www.bcdiploma.com/. [Accessed 14 February 2019].

[102] N. Zhu, "How to create certificates on the Ethereum blockchain," Medium, 21 Jul 2018. [Online]. Available: https://medium.com/coinmonks/how-to-create-certificates-on-the-ethereum-blockchain-part-1-45564fd29595.

[103] F. Al-Turjman, Cognitive Sensors and IoT : Architecture, Deployment, and Data Delivery, CRC Press LLC, 2017.

[104] W. C. Adams, "The Internet of Things and the Connected Person," Wired, 2014. [Online]. Available: The Internet of Things and the Connected Person. [Accessed 22 November 2019].

[105] A. Banafa, Secure and Smart Internet of Things (IoT) : Using Blockchain and AI, River Publishers, 2018.

[106] D. Deloach and B. Berman, "Why Smart City Development Relies on Relationships," Government-echnology-Future Structure, 16 September 2016. [Online]. Available: https://www.govtech.com/fs/infrastructure/Why-Smart-City-Development-Relies-on-Relationships.html.

[107] J. Compton, "How Blockchain Could Revolutionize The Internet Of Things," Forbes, 27 June 2017. [Online]. Available: https://www.forbes.com/sites/delltechnologies/2017/06/27/how-blockchain-could-revolutionize-the-internet-of-things/#3437a95d6eab.

[108] A. Grizhnevich, "IoT architecture: building blocks and how they work," ScienceSoft, [Online]. Available: https://www.scnsoft.com/blog/iot-architecture-in-a-nutshell-and-how-it-works. [Accessed 22 November 2019].

[109] M. Vena, "Privacy remains a big issue in today's smart home," Venture Beat, 15 May 2019. [Online]. Available: https://venturebeat.com/2019/05/15/privacy-remains-a-big-issue-in-todays-smart-home/.

[110] B. K. Alese, "Consumer Trust Model in Online Transaction," *International Journal of Computer Applications* , vol. 72, no. 17, 2013.

[111] A. Panarello, N. Tapas, G. Merlino and F. Longo, "Blockchain and IoT Integration: A Systematic Survey," *Sensors,* vol. 18, no. 2575, 2018.

[112] N. Fotiou and G. C. Polyzos, "Smart contracts for the Internet of Things: opportunities and challenges," 23 January 2019. [Online]. Available: https://arxiv.org/pdf/1901.10582.pdf.

[113] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things Journal,* vol. 5, no. 4, pp. 1184-1195, 2018.

[114] A. Banafa, "IoT and Blockchain: Challenges and Risks," 9 October 2019. [Online]. Available: https://ahmedbanafa.blogspot.com/2017/10/iot-and-blockchain-challenges-and-risks.html?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq.

[115] A. Dorri, S. S. Kanhere and R. Jurdak, " Towards an Optimized BlockChain for IoT," in *Second International Conference on Internet-of-Things Design and Implementation*, New York, NY, 2017.

[116] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and privacy," *arXiv,* 2017.

[117] L. Kelly, "Transparency is the Cure to Blockchain's Shady Reputation," The Crypto, 2 August 2019. [Online]. Available: https://medium.com/crypto/transparency-is-the-cure-to-blockchains-shady-reputation-343a8c465a2e.

[118] M. M. R. M. S. H. M. A. Rahman, E. Hassanain, M. F. Alhamid and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," *IEEE Access,* vol. 7, pp. 18611-18621, 2019.

[119] "Supply chain management," IBM, [Online]. Available: https://www.ibm.com/topics/supply-chain-management. [Accessed 30 November 2019].

[120] K. Hill, "5 Innovative Technologies To Improve Supply Chain Management," Innovation Enterprise, [Online]. Available: https://channels.theinnovationenterprise.com/articles/5-innovative-technologies-to-improve-supply-chain-management. [Accessed 1 December 2019].

[121] B. Marr, "How Blockchain Will Transform The Supply Chain And Logistics Industry," Forbes, 23 March 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#3b6f408c5fec.

[122] M. Nakasumi, "Information Sharing for Supply Chain Management Based on Block Chain Technology," in *IEEE 19th Conference Business informatics*, Thessaloniki, Greece, 2017.

[123] E. Hofmann, U. M. Strewe and N. Bosia, Supply Chain Finance and Blockchain Technology : The Case of Reverse Securitisation, Springer, 2017.

[124] "Unblocking blockchain for shipping," Hellenic shipping news, 17 October 2018. [Online]. Available: https://www.hellenicshippingnews.com/unblocking-blockchain-for-shipping/.

[125] N. Kshetri, "Blockchains and International Business," *IT Professional,* vol. 21, no. 4, pp. 8-13, 2019.

[126] TradeLens, "TradeLens home page," TradeLens, [Online]. Available: https://www.tradelens.com/. [Accessed 1 December 2019].

[127] "Chinese Blockchain Company Targets Maritime Silk Road," Maritime Executive, 21 August 2018. [Online]. Available: https://www.maritime-executive.com/article/chinese-blockchain-company-targets-maritime-silk-road.

[128] K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," *IEEE Access,* p. 17465–17477, 2017.

[129] J. Astill, R. A. Dara, M. Campbell, J. M. Farber, E. D. G. Fraser, S. Sharif and R. Y. Yada, "Transparency in food supply chains: A review of enabling technology solutions," *Trends in Food Science & Technology,* vol. 91, pp. 240-247, 2019.

[130] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *13th International Conference on Service Systems and Service Management (ICSSSM)*, 2016 .

[131] S. Kamble, A. Gunasekaran and H. Arha, "Understanding the Blockchain technology adoption in supply chains-Indian context," *International Journal of Production Research ,* pp. 2009-2033, 2018.

[132] "The TrustChain Initiative," TrustChain , [Online]. Available: https://www.trustchainjewelry.com/. [Accessed 1 December 2019].

[133] S. Figorilli, F. Antonucci, C. Costa, F. Pallottino and L. Raso, "A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain," *Sensors,* vol. 18, no. 9, 2018.

[134] S. A. Abeyratne and R. P. Monafared, "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger," *International Journal of Research in Engineering and Technology ,* vol. 05, no. 09, p. 1–10, 2016.

[135] J. A. Ligon and P. D. Thistle, "Information Asymmetries and Informational Incentives in Monopolistic Insurance Markets," *The Journal of Risk and Insurance,* vol. 63, no. 3, pp. 434-459, 1996.

[136] H. Wu, Z. Li, B. King, Z. B. Miled, J. Wassick and J. T. ., "A Distributed Ledger for Supply Chain Physical Distribution Visibility," *Information ,* vol. 8, no. 4, p. 1–18, 2017.

[137] H. Wu, "A distributed blockchain ledger for supply chain," Purdue University, Ann Arbor, 2017.

[138] T. Bocek, B. B. Rodrigues, T. Strasser and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Lisbon, 2017.

[139] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 858-880, 2019.

[140] C. Bégue, "Trust Your Supplier (TYS)," IBM, [Online]. Available: https://www.ecianow.org/assets/docs/GIPC/IBMTrustYourSupplier%20for%20ECIA%20v2.pdf. [Accessed 2 December 2019].

[141] E. Johnson, "Skepticism of Maersk-IBM's TradeLens hit bigger blockchain questions," JOC, 13 August 2018. [Online]. Available: https://www.joc.com/technology/skepticism-maersk-ibm's-tradelens-hit-bigger-blockchain-questions_20180813.html.

[142] P. Mohan, "Disaster Management Solution, Part 1: Cloud, IoT, and blockchain," IBM, 9 December 2017. [Online]. Available: https://developer.ibm.com/articles/disaster-management-using-blockchain-iot/.

[143] H. R. Hasan and K. Salah, "Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters," *IEEE Access,* vol. 6, pp. 46781-46793, 2018.

[144] X. Liang, J. Zhao, S. Shetty and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Baltimore, MD, 2017.

[145] K. Park, K. Cho, D. Han, T. Kwon and S. Pack, "Proof of Delivery in a Trustless Network," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Seoul, Korea (South, 2019 .

[146] H. R. Hasan and K. Salah, "Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts," *IEEE Access,* vol. 6, pp. 65439-65448, 2018.

[147] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services," *Computers,* vol. 8, no. 58, 2019.

[148] F. Tian, ""A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things," in *13th International Conference Service Systems and Service Management (ICSSSM)*, 2017.

[149] R. v. Hoek, "Exploring blockchain implementation in the supply chain : Learning from pioneers and RFID research," *International Journal of Operations & Production Management ,* vol. 39 , no. 6/7/8, pp. 829-859 , 2019.

[150] M. Dobrovnik, D. M. Herold, E. Fürst and S. Kummer, "Blockchain for and in Logistics: What to Adopt and Where to Start," *Logistics,* vol. 2, no. 3, 2018.

[151] M. C. Lacity, "Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality," *MIS Quarterly Executive,* no. 17, pp. 201-222, 2018.

[152] P. Traugott, "Ethereum (ETH) working on a lot of small updates while we wait for the big ones to be announced," 29 July 2018. [Online]. Available: https://captainaltcoin.com/ethereum-eth-working-on-a-lot-of-small-updates-while-we-wait-for-the-big-ones-to-be-announced/.

[153] H. Partz, "Privacy Altcoin Zcash Announces First Network Update, 'Not Expected' To Be A Fork," 3 March 2018. [Online]. Available: https://cointelegraph.com/news/privacy-altcoin-zcash-announces-first-network-update-not-expected-to-be-a-fork.

[154] A. Fernández, "Urgent update and technical issues at Ethereum," 15 October 2017. [Online]. Available: https://bitcoiner.today/en/urgent-update-and-technical-issues-at-ethereum/.

[155] M. @. Veriday, "Is Blockchain Right for You? Bridging the Legacy Gap," 23 November 2017. [Online]. Available: https://www.veriday.com/blog/blockchain-right-bridging-legacy-gap/.

[156] B. Marr, "The 5 Big Problems With Blockchain Everyone Should Be Aware Of," 19 February 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#2b9e879e1670.

[157] R. McMillan, "The inside story of Mt. Gox, BitCoin's $460 million disaster," 3 March 2014. [Online]. Available: https://www.wired.com/2014/03/bitcoin-exchange/. [Accessed 9 February 2018].

[158] S. Gupta and T. Mondal, "HfS Blueprint Report: Enterprise Blockchain Services," November 2017. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=82013282USEN.

[159] A. B. Pedersen, M. Risius and R. Beck, "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies," *MIS Quarterly Executive,* no. Forthcoming, 2019.

[160] "Cross border supply chain solution," [Online]. Available: https://www.ibm.com/blockchain/use-cases/. [Accessed 10 February 2018].

[161] L. Pawczuk, R. Massey and J. Holdowski, "Deloitte's Global Blockchain Survey 2019," 2019. [Online]. Available: https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf.

[162] J. Cuomo, "Introducing the next-gen platform for enterprise blockchain," IBM, 18 June 2019. [Online]. Available: https://www.ibm.com/blogs/blockchain/2019/06/introducing-the-next-gen-platform-for-enterprise-blockchain/.

[163] V. Tabora, "Databases and Blockchains, The Difference Is In Their Purpose And Design," 4 August 2018. [Online]. Available: https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b.

[164] S. Meunier, "Blockchain technology — a very special kind of Distributed Database," 29 December 2016. [Online]. Available: https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118.

[165] N. Bauerle, "What is the Difference Between a Blockchain and a Database?," [Online]. Available: https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database. [Accessed 28 June 2019].

[166] B. Ibryam, "The next integration evolution — blockchain," 05 02 2019. [Online]. Available: https://techcrunch.com/2019/02/05/blockchain-as-integration-evolution/.

[167] J. Chenard, "How Blockchain is Reinventing Business Process Management," HyperLedger, 12 June 2018. [Online]. Available: https://www.hyperledger.org/blog/2018/06/12/how-blockchain-is-reinventing-business-process-management.

[168] M. Hooper, "Top five blockchain benefits transforming your industry," IBM, 22 February 2018. [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/.

[169] Z. Li, Q. Lu, S. Chen, Y. Liu and X. Xu, "A Landscape of Cryptocurrencies," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Seoul, South Korea, 2019.

[170] T. Brewster, "Exclusive: Hackers Take Control Of Giant Construction Cranes," Forbes, 15 January 2019. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2019/01/15/exclusive-watch-hackers-take-control-of-giant-construction-cranes/#4e1344f61d0a.

[171] J. P. Bender, K. Burchardi and N. Shepherd, "Capturing the Value of Blockchain," Boston Consulting Group, 9 April 2019. [Online]. Available: https://www.bcg.com/en-ca/publications/2019/capturing-blockchain-value.aspx.

[172] Y. Vilner, "The Year Of Blockchain And Sharing Economy's Intersection," Forbes, 20 July 2018. [Online]. Available: https://www.forbes.com/sites/yoavvilner/2018/07/20/the-year-of-blockchain-and-sharing-economys-intersection/#1534087f4c28.

[173] S. Warren, C. Wolff and N. Hewett, "Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction," World Economic Forum , 8 April 2019. [Online]. Available:

https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction.

[174] D. Noah, "8 Documents Required for International Shipping," 10 January 2018 . [Online]. Available: https://www.shippingsolutions.com/blog/documents-required-for-international-shipping.

[175] J. Colaco, S. Chatterjeev, A. Watson and V. Singla, "Blockchain in Insurance," Deloitte.ca, [Online]. Available: https://www2.deloitte.com/ca/en/pages/financial-services/articles/blockchain-in-insurance.html. [Accessed 31 May 2019].

[176] "Minimum Requirements," Bitcoin.org, [Online]. Available: https://bitcoin.org/en/full-node#minimum-requirements. [Accessed 1 June 2019].

[177] J. Connell, "How Much Does it Cost to Run a Full Bitcoin Node?," 23 February 2017 . [Online]. Available: https://news.bitcoin.com/cost-full-bitcoin-node/.

[178] J. Bloomberg, "Don't Let Blockchain Cost Savings Hype Fool You," Forbes, 24 February 2018. [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2018/02/24/dont-let-blockchain-cost-savings-hype-fool-you/#7713f0fb5811.

[179] N. Szabo, "Formalizing and Securing Relationships on Public Networks," 1 September 1997. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/548/469.

[180] "Solidity, the Contract-Oriented Programming Language," [Online]. Available: https://github.com/ethereum/solidity. [Accessed 10 November 2018].

[181] "Ethereum," [Online]. Available: https://github.com/ethereum. [Accessed 10 November 2018].

[182] M. Ghafari, P. Gadient and O. Nierstrasz, "Security Smells in Android," in *IEEE 17th International Working Conference on Source Code Analysis and Manipulation (SCAM)*, Shanghai, 2017.

[183] I. Thomson, "Parity: The bug that put $169m of Ethereum on ice? Yeah, it was on the todo list for months," 16 November 2017. [Online]. Available: https://www.theregister.co.uk/2017/11/16/parity_flaw_not_fixed/.

[184] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali and R. Hierons, "Smart contracts vulnerabilities: a call for blockchain software engineering?," in *International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Campobasso, 2018.

[185] B. Jiang, Y. Liu and W.K.Chan, "ContractFuzzer: Fuzzing Smart Contracts for Vulnerability Detection," 2018. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1807/1807.03932.pdf.

[186] L. Luu, D.-H. Chu, H. Olickel, P. Saxena and A. Hobor, "Making Smart Contracts Smarter," in *ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, New York, NY, USA, 2016.

[187] V. Chia, P. Hartel, Q. Hum, S. Ma, G. Piliouras, D. Reijsbergen, M. v. Staalduinen and P. Szalachowski, "Rethinking Blockchain Security: Position Paper," 12 June 2018. [Online]. Available: https://arxiv.org/abs/1806.04358.

[188] P. Tsankov, A. Dan, D. Drachsler, A. Gervais, F. Bünzli and M. Vechev, "Securify:PracticalSecurityAnalysisofSmartContracts," 24 August 2018. [Online]. Available: https://arxiv.org/pdf/1806.01143.pdf.

[189] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko and Y. Alexandrov, "SmartCheck:Static Analysis of Ethereum Smart Contracts," in *WETSEB'18*, Gothenburg, Sweden , 2018.

[190] "Ethereum Wiki," [Online]. Available: https://github.com/ethereum/wiki/wiki/Safety#timestamp-dependence. [Accessed 10 November 2018].

[191] "When can BLOCK HASH be safely used for a random number? When would it be unsafe?," Stack Exchange, 1 April 2016. [Online]. Available: https://ethereum.stackexchange.com/questions/419/when-can-blockhash-be-safely-used-for-a-random-number-when-would-it-be-unsafe/427#427.

[192] "Solidity Documentation," [Online]. Available: https://solidity.readthedocs.io/en/develop/security-considerations.html. [Accessed 10 November 2018].

[193] "Inline assembly 30 times speedup," [Online]. Available: https://www.reddit.com/r/ethereum/comments/4f3lbt/solidity_stringutils_library/d25kzb5/. [Accessed 10 November 2018].

[194] "Recommendations for Smart Contract Security in Solidity," Consensys, [Online]. Available: https://consensys.github.io/smart-contract-best-practices/recommendations/#lock-pragmas-to-specific-compiler-version. [Accessed 2018 November 2018].

[195] "Ethereum Smart Contract Best Practices," Consensys, [Online]. Available: https://consensys.github.io/smart-contract-best-practices/known_attacks/#dos-with-unexpected-revert. [Accessed 10 November 2018].

[196] "Why are self destructs used in contract programming?," Ethereum, 24 September 2018. [Online]. Available: https://ethereum.stackexchange.com/questions/315/why-are-selfdestructs-used-in-contract-programming.

[197] "Throw vs. Return," 16 November 2016. [Online]. Available: https://ethereum.stackexchange.com/questions/10046/throw-vs-return.

[198] S. McKie, "Solidity Learning: Revert(), Assert(), and Require() in Solidity, and the New REVERT Opcode in the EVM," 27 September 2017. [Online]. Available: https://medium.com/blockchannel/the-use-of-revert-assert-and-require-in-solidity-and-the-new-revert-opcode-in-the-evm-1a3a7990e06e.

[199] "MinerOne Smart Contracts Security Analysis," 28 February 2018. [Online]. Available: https://minerone.io/doc/SmartDec-MinerOne-Security-Audit.pdf.

[200] "SWC-129," [Online]. Available: https://smartcontractsecurity.github.io/SWC-registry/docs/SWC-129. [Accessed 10 11 2018].

[201] "Learn X in Y minutes Where X=Solidity," [Online]. Available: https://learnxinyminutes.com/docs/solidity/. [Accessed 10 November 2018].

[202] "Solidity Visibility and Getters," BitDegree, [Online]. Available: https://www.bitdegree.org/learn/solidity-visibility-and-getters/#Solidity_Visibility_and_Getters_Main_Tips. [Accessed 10 November 2018].

[203] P. Vessenes, "The ERC20 Short Address Attack Explained," 06 April 2017 . [Online]. Available: https://vessenes.com/the-erc20-short-address-attack-explained/.

[204] D. Hoyte, "Submission to the Underhanded Solidity Coding Contest," 21 September 2017. [Online]. Available: https://github.com/Arachnid/uscc/tree/master/submissions-2017/doughoyte.

[205] R. Wilson, "Blockchain applications in energy trading," 2016. [Online]. Available: https://www2.deloitte.com/uk/en/pages/energy-and-resources/articles/blockchain-applications-in-energy-trading.html. [Accessed 2018 April 28].

[206] C. Martin, "How Blockchain Is Threatening to Kill the Traditional Utility," Bloomberg Technology, 9 April 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-04-09/blockchain-latest-death-knell-of-an-old-school-utility-model. [Accessed 28 April 2018].

[207] E. R. Sanseverino, M. L. D. Silvestre, P. Gallo, G. Zizzo and M. Ippolito, "The Blockchain in Microgrids for Transacting Energy and Attributing Losses".

[208] K. Mannaro, A. Pinna and M. Marchesi, "Crypto-Trading: blockchain-oriented energy market," in *AEIT International Annual Conference*, 2017.

[209] M. Sabounchi and J. Wei, "Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)* , 2017.

[210] M. E. Peck and D. Wagman, " Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain," *IEEE Spectrum,* vol. 54, no. 10, pp. 56-61, 2017.

[211] R. Leonard, "Enerport a new blockchain energy trading project launched," 15 March 2018. [Online]. Available: https://irishtechnews.ie/enerport-a-new-blockchain-energy-trading-project-launched/. [Accessed 28 April 2018].

[212] "Power Ledger is the world leading peer-to-peer marketplace for renewable energy," PowerLedger, [Online]. Available: https://powerledger.io/. [Accessed 28 April 2018].

[213] "TEPCO looks to the transformative potential of blockchain by investing in Electron, a UK energy technology company," 19 January 2018. [Online]. Available: http://www.tepco.co.jp/en/announcements/2018/1473674_15434.html. [Accessed 28 April 2018].

[214] "Welcome to the Future of Energy," GridPlus, [Online]. Available: https://gridplus.io/. [Accessed April 2018].

[215] "Enerchain P2P Trading Project," Enerchain, 29 May 2017. [Online]. Available: https://enerchain.ponton.de/index.php/21-enerchain-p2p-trading-project. [Accessed April 2018].

[216] "Blockchain-based green energy trading platform," WePower, [Online]. Available: https://wepower.network/#. [Accessed 24 April 2018].

[217] "Endesa and Gas Natural Fenosa complete first blockchain energy trade transaction in Spain," Endesa, 6 February 2018. [Online]. Available: https://www.endesa.com/en/press/news/d201802-endesa-and-gas-natural-fenosa-complete-first-blockchain-energy-trade-transaction-in-spain.html. [Accessed 28 April 2018].

[218] G. Zizzo, E. R. Sanseverino, M. G. Ippolito, M. L. D. Silvestre and P. Gallo, "A Technical Approach to P2P Energy Transactions in Microgrids," *IEEE Transactions on Industrial Informatics,* 2018 (Early Access).

[219] M. Mihaylov, S. Jurado, K. Van Moffaert, N. Avellana and A. Nowe, "NRG-X-change a novel mechanism for trading of renewable energy in smart grids," in *Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems*, 2014.

[220] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," *IEEE Transactions on Dependable and Secure Computing,* 2016 (Early Access).

[221] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao and C. Lin, "Applying blockchain technology to decentralized operation in future energy internet," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)* , 2017.

[222] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, 2017.

[223] J. Basden and M. Cottrell, "How Utilities Are Using Blockchain to Modernize the Grid," Harward Business Review, 23 March 2017. [Online]. Available: https://hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid. [Accessed 28 April 2018].

[224] "How blockchain technology could reshape Utilities businesses," Bearing Point, [Online]. Available: https://www.bearingpoint.com/fr-fr/blogs/blog-energie/how-blockchain-technology-could-reshape-utilities-businesses/. [Accessed 28 April 2018].

[225] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Transactions on Industrial Informatics,* vol. 13, no. 6, pp. 3154-3164, 2017.

[226] M. Orcutt, "How Blockchain Could Give Us a Smarter Energy Grid," MIT Technology Review, 16 October 2017. [Online]. Available: https://www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid/. [Accessed 2018 April 2018].

[227] F. Imbault, M. Swiatek, R. d. Beaufort and R. Plana, "The green blockchain: Managing decentralized energy production and consumption," in *2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, 2017.

[228] P. Danzi, M. Angjelichinoski, Č. Stefanović and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," in *2017 IEEE International Conference on Smart Grid Communications* , 2017.

[229] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang and L. Sun, "A Blockchain based Truthful Incentive Mechanism for Distributed P2P Applications," *IEEE Access,* 2018 (Early Access).

[230] G. Dutsch and N. Steinecke, "Blockchain Technology in Energy," PWC, July 2017. [Online]. Available: https://www.pwc.com/gx/en/industries/energy-utilities-resources/publications/blockchain-technology-in-energy.html. [Accessed 28 April 2018].

[231] "Select Ontario Electricity Provider," energyrates.ca, [Online]. Available: http://energyrates.ca/select-ontario-electricity-provider/?prefix=M2N. [Accessed 29 April 2018].

[232] R. Skowronski, "On the applicability of the GRIDNET protocol to Smart Grid environments," in *2017 IEEE International Conference on Smart Grid Communications* , 2017.

[233] A. Unterweger, F. Knirsch, C. Leixnering and D. Engel, " Lessons Learned from Implementing a Privacy-Preserving Smart Contract in Ethereum," in *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018.

[234] Electrical Safety Authority, [Online]. Available: https://www.esasafe.com/toronto. [Accessed 2018].

[235] "Toronto Hydro Service Repair Notice," Toronto Hydro , [Online]. Available: http://www.torontohydro.com/sites/electricsystem/business/connections/Documents/Service%20Repair%20Notice_CAF.PDF . [Accessed 28 April 2018].

[236] B. Lorica, "How big data and AI will reshape the automotive industry," 20 July 2017 . [Online]. Available: https://www.oreilly.com/ideas/how-big-data-and-ai-will-reshape-the-automotive-industry.

[237] "The 2017 EU Industrial R&D Investment Scoreboard," European Commission, 2017. [Online]. Available: http://iri.jrc.ec.europa.eu/scoreboard17.html.

[238] "Mobility Open Blockchain Initiative," [Online]. Available: https://www.dlt.mobi/. [Accessed 10 November 2018].

[239] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan and K. Ren, "A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks," *IEEE Network,* pp. 1 - 9, 2018, (Early Access).

[240] X. Huang, C. Xu, P. Wang and H. Liu, "LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem," *IEEE Access,* vol. 6, pp. 13565 - 13574, 2018.

[241] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics,* 2017, (Early Access).

[242] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," *IEEE Communications Magazine,* vol. 55, no. 12, pp. 119 - 125, 2017.

[243] N. H. Kim, S. M. Kang and C. S. Hong, "Mobile charger billing system using lightweight Blockchain," in *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2017.

[244] M. Pustišek, A. Kos and U. Sedlar, "Blockchain Based Autonomous Selection of Electric Vehicle Charging Station," in *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, 2016.

[245] M. Grosch, "Impact study of mileage fraud with used cars & Adaptability of the Car-Pass model in other EU countries," 2010. [Online]. Available: https://www.car-pass.be/files/article_files/file/7/crm%20study%20final%20report.pdf. [Accessed 28 April 2018].

[246] "Protect European consumers against odometer manipulation Massive fraud in most of Europe should no longer be tolerated," 6 October 2014. [Online]. Available: http://www.fiaregion1.com/wp-content/uploads/2017/05/joint_appeal_against_odometer_manipulation_final.pdf. [Accessed 28 April 2018].

[247] K. L. Brousmiche, T. Heno, C. Poulain, A. Dalmieres and E. B. Hamida, "Digitizing, Securing and Sharing Vehicles Life-cycle Over a Consortium Blockchain: Lessons Learned," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018.

[248] N. Lasla, M. Younis, W. Znaidi and D. B. Arbia, "Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018.

[249] Z. Yang, K. Zheng, K. Yang and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017.

[250] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang and Z. Zhang, "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," *IEEE Transactions on Intelligent Transportation Systems,* pp. 1 - 17, 2018 (Early Access).

[251] M. Singh and S. Kim, "Crypto trust point (cTp) for secure data sharing among intelligent vehicles," in *2018 International Conference on Electronics, Information, and Communication (ICEIC)*, 2018.

[252] C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri and S. Jha, "B-FICA: BlockChain based Framework for Auto-insurance Claim and Adjudication," 16 June 2018. [Online]. Available: https://arxiv.org/abs/1806.06169.

[253] M. Cebe, E. Erdin, K. Akkaya, H. Aksu and S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," *IEEE Communications Magazine,* vol. 56, no. 10, pp. 50 - 57, 2018.

[254] "Criminal Penalties for Using Fake Proof of Insurance," 14 June 2013. [Online]. Available: https://www.carsdirect.com/car-insurance/criminal-penalties-for-using-fake-proof-of-insurance.

[255] Joseph Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," 14 January 2016. [Online]. Available: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf. [Accessed 10 November 2018].

[256] R. Gevaers, E. V. d. Voorde and T. V. lslander, "Cost Modelling and Simulation of Last-mile Characteristics in an Innovative B2C Supply Chain Environment with Implications on Urban Areas and Cities," *Procedia - Social and Behavioral Sciences,* vol. Volume 125 , pp. 398-411, 2014.

[257] E. Coupland and F. Pierce, "The 'last mile' problem, by Parcel2Go," Supply Chain Digital, 4 November 2013. [Online]. Available: https://www.supplychaindigital.com/logistics/last-mile-problem-parcel2go. [Accessed 27 October 2019].

[258] Y. Vakulenko, P. Shams, D. Hellström and K. Hjort, "Service innovation in e-commerce last mile delivery: Mapping the e-customer journey," *Journal of Business Research,* vol. 101, pp. 461-468, 2019.

[259] M. Hochstenbach, C. Notteboom, B. Theys and J. D. Schutter, "Design and Control of an Unmanned Aerial Vehicle for Autonomous Parcel Delivery with Transition from Vertical Take-off to Forward Flight –

VertiKUL, a Quadcopter Tailsitter," *International Journal of Micro Air Vehicles,* vol. 7, no. 4, pp. 395-405, 2015.

[260] Accenture, "World Economic Forum: Digital Transformation of Industries - Logistics Industry," January 2016. [Online]. Available: http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-logistics-industry-white-paper.pdf. [Accessed 27 October 2019].

[261] A. Lee, "JD.coms autonomous delivery vehicles will take to streets of Tianjin," South China Morning Post, 19 January 2018. [Online].

[262] "Domino's Pizza Is Testing Autonomous Delivery Vehicles," Newstex Finance & Accounting Blogs, 17 June 2019. [Online].

[263] "Robomart home page - Self driving stores," Robomart, [Online]. Available: https://robomart.co/. [Accessed 16 July 2019].

[264] C. Swedberg, "DropTag Knows When a Package Has Been Handled With Care," RFID Journal, 12 February 2013. [Online]. Available: https://www.rfidjournal.com/articles/view?10411/2.

[265] "Overview of Condition Based Monitoring (CBM)," inspectioneering, [Online]. Available: https://inspectioneering.com/tag/condition+based+monitoring. [Accessed 16 July 2019].

[266] D. Sheynin, "The Last Mile: How Data Analytics In The Cloud Is Improving Parcel Delivery," Forbes, 3 January 2017. [Online]. Available: https://www.forbes.com/sites/rackspace/2017/01/03/the-last-mile%E2%80%AFhow-data-analytics-in-the-cloud-is-improving-parcel-delivery/#19e411d219d5.

[267] A. Milano, "Walmart Wants Blockchain to Make Shipping 'Smarter'," 2 March 2018. [Online]. Available: https://www.coindesk.com/walmart-using-blockchain-tech-make-shipping-smarter.

[268] C. R. D. Meijer, "Blockchain and package tracking: a win-win situation!," 11 June 2017 . [Online]. Available: https://www.finextra.com/blogposting/14167/blockchain-and-package-tracking-a-win-win-situation.

[269] cryptoninjas, "How the 'Last Mile' problem is being solved by Blockchain," 1 August 2018. [Online]. Available: https://www.cryptoninjas.net/2018/08/01/how-the-last-mile-problem-is-being-solved-by-blockchain/.

[270] Pierbridge, "5 Reasons Blockchain Will Transform the Parcel Shipping Industry," 27 December 2017 . [Online]. Available: https://pierbridge.com/news/2017/5-reasons-blockchain-will-transform-the-parcel-shipping-industry.html.

[271] ShipChain, "The end-to-end logistics platform of the future: trustless, transparent tracking.," [Online]. Available: https://shipchain.io/. [Accessed 30 October 2019].

[272] Nextpakk, "Nextpakk-Reinventing The Logistics of Life," [Online]. Available: https://s3.amazonaws.com/nextpakk-assets/docs/pakka-ico-whitepaper.pdf. [Accessed 30 October 2019].

[273] VoltTech, "Last Mile Delivery & Logistics Company," [Online]. Available: https://volttech.io/. [Accessed 30 October 2019].

[274] Precision, "Could Blockchain Revlutionize Parcel Shipping?," [Online]. Available: https://www.fedex.com/content/dam/fedex/us-united-states/Compatible-Solutions/images/2019/Q2/Could_Blockchain_Revolutionize_Parcel_Shipping_V2_50457811.pdf. [Accessed 30 October 2019].

[275] PitneyBowes, "What's Happening in the World of Shipping: Blockchain tech, FedEx's latest acquisition and the Uber for shipping," PitneyBowes, [Online]. Available: https://www.pitneybowes.com/us/shipping-and-mailing/case-studies/whatshappeningintheworldshippingweekofjune13th2016.html. [Accessed 30 October 2019].

[276] A. Broring, S. K. Datta and C. Bonnet, "A Categorization of Discovery Technologies for the Internet of Things," in *Proceedings of the 6th International Conference on the Internet of Things*, Stuttgart, Germany, 2016.

[277] M. Samaniego and R. Deters, "Using Blockchain to Push Software-Defined IoT Components Onto Edge Hosts," in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*, Blagoevgrad, Bulgaria, 2016.

[278] J. Sun, J. Yan and K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financial Innovation,* vol. 2, no. 1, p. 26, 2016.

[279] S. M. I. W. H. Li Da Xu and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics,* vol. 10, no. 4, 2014.

[280] C. H. Liu, B. Yang and T. Liu, "Efficient naming, addressing and profile services in Internet-of-Things sensory environments," *Ad Hoc Networks,* vol. 18, pp. 85-101, 2014.

[281] F. Paganelli, S. Turchi and D. Giuli, "A Web of Things Framework for RESTful Applications and Its Experimentation in a Smart City," *IEEE Systems Journal,* vol. 10, no. 4, 2016.

[282] V. Pureswaran and P. Brody, "Device democracy - Saving the future of the Internet of Things," [Online]. Available: http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/. [Accessed 19 May 2019].

[283] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access,* vol. 4, pp. 2292-2303, 2016.

[284] C. M., M. Löffler and R. Roberts, "The Internet of Things," March 2010. [Online]. Available: https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things.

[285] M. Joerss, J. Schröder, F. Neuhaus, C. Klink and F. Mann, "Parcel delivery - The future of last mile," September 2016. [Online]. Available: https://www.mckinsey.com/~/media/mckinsey/industries/travel%20transport%20and%20logistics/our%20insights/how%20customer%20demands%20are%20reshaping%20last%20mile%20delivery/parcel_delivery_the_future_of_last_mile.ashx.

[286] A. Dorri, S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home.," in *IEEE International Conference on Pervasive Computing and Communications Workshops*, Kona, HI, 2017.

[287] "Pitney Bowes Parcel Shipping Index Reports Global Parcel Shipping Reaches $279 Billion in Revenue," Business Insider, 28 August 2018. [Online]. Available: https://markets.businessinsider.com/news/stocks/pitney-bowes-parcel-shipping-index-reports-global-parcel-shipping-reaches-279-billion-in-revenue-1027489736.

[288] S. A. Ross, "The Economic Theory of Agency: The Principal's Problem," *The American Economic Review,* vol. 63, no. 2, pp. 134-139, 1973.

[289] "Agency Theory," SevenPillarsInstitute, [Online]. Available: https://sevenpillarsinstitute.org/ethics-101/agency-theory-2/. [Accessed 15 November 2019].

[290] S. Fayezi, A. O'Loughlin and A. Zutshi, "Agency theory and supply chain management: a structured literature review," *Supply chain management: An international journal,* vol. 17, no. 5, p. 556–570, 2012.

[291] S. P. Shapiro, "Agency Theory," *Annual Review of Sociology,* vol. 31, pp. 263-284, 2005.

[292] L. Obbayi, "Computer Forensics: Chain Of Custody," Infosec, [Online]. Available: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/#gref. [Accessed 10 10 2019].

[293] M. J. McGrath and C. N. Scanaill, "Sensing and Sensor Fundamentals," in *Sensor Technologies*, Springer, 2014, pp. 12-50.

[294] Schema.org, "ParcelDelivery," [Online]. Available: https://schema.org/ParcelDelivery. [Accessed 30 October 2019].

[295] databaseanswers, "Database Answers," [Online]. Available: http://www.databaseanswers.org/data_models/package_delivery_service/index.htm. [Accessed 30 October 2019].

[296] adrm, "Parcel & Mail Delivery," [Online]. Available: http://www.adrm.com/ind-parcel-mail-delivery.shtml. [Accessed 30 October 2019].

[297] E. Drkušić, "A Mail Delivery Company Data Model," 1 November 2017. [Online]. Available: https://www.vertabelo.com/blog/a-mail-delivery-company-data-model/.

[298] B. Williams, "Conceptual Data Model for Delivery System," Database Answers, [Online]. Available: http://www.databaseanswers.org/data_models/package_delivery_service/index.htm. [Accessed 10 July 2019].

[299] jsonld, "JSON for Linking Data," [Online]. Available: https://json-ld.org/. [Accessed 30 October 2019].

[300] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa and P. Fraga-Lamas, "Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring," *Sensors,* vol. 19, no. 15, 2019.

[301] B. Buhler and A. Pharand, "The New Delivery Reality - Achieving High Performance in the Post and Parcel Industry," Accenture, 2016. [Online]. Available: https://www.accenture.com/_acnmedia/PDF-42/Accenture-The-New-delivery-Reality-HP-Post-and-Parcel-research-2016.pdf.

[302] NOAA, "Billion-Dollar Disasters: Calculating the Costs," NOAA', [Online]. Available: https://www.ncdc.noaa.gov/monitoring-references/dyk/billions-calculations. [Accessed 20 September 2019].

[303] S. Bulling, "Poverty causes disasters and disasters cause poverty," Thomson Reuters Foundation, 9 May 2011. [Online]. Available: http://news.trust.org//item/20110509085300-aey1c.

[304] "Syria's war: 80% in poverty, life expectancy cut by 20 years, $200bn lost," The Guardian, 12 March 2015 . [Online]. Available: https://www.theguardian.com/world/2015/mar/12/syrias-war-80-in-poverty-life-expectancy-cut-by-20-years-200bn-lost.

[305] "Why are so many people in the world hungry?," World Vision Australia , [Online]. Available: https://www.worldvision.com.au/global-issues/work-we-do/famine/why-are-so-many-people-in-the-world-hungry. [Accessed 23 January 2018].

[306] FAO, "SAVE FOOD: Global Initiative on Food Loss and Waste Reduction," United Nations, [Online]. Available: http://www.fao.org/save-food/resources/keyfindings/en/. [Accessed 23 January 2018].

[307] P. Adams, "Why Food Aid Fuels International Conflict," Huffington Post, Toronto, 2014.

[308] J. Perlez, "Somalia Aid Workers Split on Troops," *The New York Times,* 27 November 1992.

[309] P. van den Dool, "Fourteen reasons not to give," *NRC Handelsblad,* 04 August 2011.

[310] N. Nunn and N. Qian, "US Food Aid and Civil Conflict," *American Economic Review,* vol. 104, no. 6, pp. 1630-66, 2014.

[311] C. Kenny, "Give Poor People Cash," *The Atlantic,* 25 September 2015.

[312] WorldBank, "Turkey's Response to the Syrian Refugee Crisis and the Road Ahead," December 2015. [Online]. Available: http://documents.worldbank.org/curated/en/583841468185391586/pdf/102184-WP-P151079-Box394822B-PUBLIC-FINAL-TurkeysResponseToSyrianRefugees-eng-12-17-15.pdf.

[313] J. Flaherty, "Is Cash Better Than Food Aid for Refugees?," 1 March 2017. [Online]. Available: http://now.tufts.edu/articles/cash-better-food-aid-refugees. [Accessed 30 January 2018].

[314] D. Green, "Ending world hunger is possible – so why hasn't it been done?," *The Guardian,* 15 February 2012.

[315] C. Green, "Charities hit by a lack of trust," 10 April 2018. [Online]. Available: https://www.charitydigitalnews.co.uk/2018/04/10/charities-hit-lack-trust-infographic/.

[316] TLYCS, "Ten Reasons Why People Don't Donate to Charity," The Life You Can Save (TLYCS) , [Online]. Available: https://www.thelifeyoucansave.org/learn-more/common-objections-to-giving. [Accessed 19 September 2019].

[317] CNNlibrary, "Hurricane Katrina Statistics Fast Facts," 23 August 2013. [Online]. Available: https://www.cnn.com/2013/08/23/us/hurricane-katrina-statistics-fast-facts/index.html.

[318] C. Montoya-Galvez, "Study: Puerto Rico received slower, less "generous" federal disaster aid than Texas, Florida," CBC News, 22 January 2019. [Online]. Available: https://www.cbsnews.com/news/study-puerto-rico-received-slower-less-generous-federal-disaster-aid-than-texas-florida/.

[319] J. S. Sorensen and E. Meyer, "How corruption slows disaster recovery," The conversation, 5 June 2018. [Online]. Available: http://theconversation.com/how-corruption-slows-disaster-recovery-96832.

[320] P. Meier, "Humanitarian in the sky: drones for disaster response," Virgin.com, [Online]. Available: https://www.virgin.com/virgin-unite/business-innovation/humanitarian-sky-drones-disaster-response. [Accessed 19 September 2019].

[321] "Amazon Prime Air," Amazon, [Online]. Available: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011. [Accessed 19 September 2019].

[322] M. T.Riccardi, "The power of crowdsourcing in disaster response operations," *International Journal of Disaster Risk Reduction,* vol. 20, pp. 123-128, 2016.

[323] R. J. Bowman, "Emergency Response to Natural Disasters: Blockchain to the Rescue," SupplyChainBrain, 20 March 2019. [Online]. Available: https://www.supplychainbrain.com/articles/29495-emergency-response-to-natural-disasters-blockchain-to-the-rescue.

[324] W. Suberg, "US Defense Dept. Wants to Use Blockchain to Improve Disaster Relief," CoinTelegraph, 27 December 2018. [Online]. Available: https://cointelegraph.com/news/us-defense-dept-wants-to-use-blockchain-to-improve-disaster-relief.

[325] D. Akilo, "U.S. Military Explores Blockchain for Disaster Relief," Business Blockchain HQ, 31 December 2018. [Online]. Available: https://businessblockchainhq.com/business-blockchain-news/us-military-explores-blockchain-for-disaster-relief/.

[326] AIDF, "Blockchain could transform identification and aid processes for refugees," AIDF, 16 March 2018. [Online].

[327] J. McIsaac, J. Brulle, J. Burg, G. Tarnacki, C. Sullivan and R. Wassel, "Blockchain Technology for Disaster and Refugee Relief Operations," in *WADEM Congress on Disaster and Emergency Medicine*, 2019.

[328] J. Rohr, "Blockchain For Disaster Relief: Creating Trust Where It Matters Most," SAP-Digitalist Magazine, 23 November 2017. [Online]. Available: https://www.digitalistmag.com/improving-lives/2017/11/23/blockchain-for-disaster-relief-creating-trust-where-it-matters-most-05527536.

[329] TRCA, "The History of Flood Control in the TRCA," [Online]. Available: http://www.trca.on.ca/dotAsset/18310.pdf. [Accessed 10 January 2020].

[330] R. Lau, "Flooding ravages municipalities across Quebec," GLOBAL NEWS, 8 May 2017. [Online]. Available: https://globalnews.ca/news/3434281/in-photos-flooding-ravages-municipalities-across-quebec/.

[331] DHTorontoStaff, "Toronto's most vulnerable areas for flooding," Daily Hive, 5 May 2017. [Online]. Available: https://dailyhive.com/toronto/toronto-flood-areas-2017.

[332] HurricaneScience, "Katrina Impacts," HurricaneScience, [Online]. Available: http://www.hurricanescience.org/history/studies/katrinacase/impacts. [Accessed 10 January 2020].

[333] K. Z. a. J. A. Arelis R. Hernández, "Texas faces environmental concerns as wastewater, drinking water systems compromised," Washington Post, 3 September 2017. [Online]. Available: https://www.washingtonpost.com/news/post-nation/wp/2017/09/03/trump-administration-wants-to-tie-harvey-recovery-aid-to-debt-ceiling-legislation/.

[334] A. Jenkins, "All of Puerto Rico's International Airports Are Closed Due to Hurricane Maria Devastation," Fortune, 21 September 2017. [Online]. Available: https://fortune.com/2017/09/21/hurricane-maria-puerto-rico-airports-closed/.

[335] D. Wolfe, "Watch while boxes of water bottles languish in Puerto Rico following Hurricane Maria," Quartz, 13 September 2018. [Online]. Available: https://qz.com/1388550/watch-while-boxes-of-water-bottles-languish-in-puerto-rico-following-hurricane-maria/.

[336] VaughanEmergencyPlanningWorkingGroup, "Evacuation re-entry plan," Vaughan Emergency Planning Working Group , August 2009. [Online]. Available: https://www.vaughan.ca/cityhall/emergency_planning/General%20Documents/Evacuation%20Re-Entry%20Plan.pdf. [Accessed 10 January 2020].

[337] R. Meyer, "What's Happening With the Relief Effort in Puerto Rico?," The Atlantic, 4 October 2017 . [Online]. Available: https://www.theatlantic.com/science/archive/2017/10/what-happened-in-puerto-rico-a-timeline-of-hurricane-maria/541956/.

[338] LifeStraw, "LifeStraw," LifeStraw, [Online]. Available: https://www.lifestraw.com/collections/featured/products/lifestraw. [Accessed 10 January 2020].

[339] CleanSip, "What is Clean Sip?," My Clean Sip, [Online]. Available: http://www.mycleansip.com/about/. [Accessed 10 January 2020].

[340] "Folia Filters™ are the world's most affordable water filter," Folia Filters, [Online]. Available: https://www.foliawater.com/foliafilterpapers. [Accessed 10 January 2020].

[341] GovernmentOfCanada, "Remotely Piloted Aircraft Systems," Government Of Canada, [Online]. Available: https://laws-lois.justice.gc.ca/eng/regulations/SOR-96-433/FullText.html#s-900.01. [Accessed 10 01 2020].

[342] GovernmentOfCanada, "Flying your drone safely and legally," Government Of Canada, [Online]. Available: https://www.tc.gc.ca/en/services/aviation/drone-safety/flying-drone-safely-legally.html. [Accessed 10 January 2020].

[343] M. J. Lem and J. W. Lem, "Drone Law," Build-ing, 3 September 2019. [Online]. Available: https://building.ca/feature/drone-law/.

[344] M. McNabbon, "Pay Attention to This One: Can You Be Sued for Flying a Drone Over Private Property? The Next Draft of that Tort Law," DroneLife, 19 March 2019. [Online]. Available: https://dronelife.com/2019/03/19/can-you-be-sued-for-flying-a-drone-over-private-property-the-next-draft-of-that-tort-law/. [Accessed 10 January 2020].

[345] N. Kobie, "Droning on: the challenges facing drone delivery," Alphr, [Online]. Available: https://www.alphr.com/the-future/1004520/droning-on-the-challenges-facing-drone-delivery. [Accessed 10 January 2020].

[346] T. Jones, "International Commercial Drone Regulation and Drone Delivery Services," Rand Corporation, 2017.

[347] P. Butterworth-Hayes, "Regulator approves Drone Delivery Canada trial flights of urban delivery system," Unmanned Airspace, 5 August 2018. [Online]. Available: https://www.unmannedairspace.info/uncategorized/regulator-approves-drone-delivery-canada-trial-flights-urban-delivery-system/.

[348] R. Enderle, "The 5 Most Pressing Problems With Drone Delivery," Tech Buzz, 10 June 2019. [Online]. Available: https://www.technewsworld.com/story/86060.html.

[349] C. Matyszczyk, "Judge rules man had right to shoot down drone over his house," C-net, 28 October 2015. [Online]. Available: https://www.cnet.com/news/judge-rules-man-had-right-to-shoot-down-drone-over-his-house/.

[350] M. Tuerk, "Fixing Amazon's Drone Delivery Problem," Forbes, 16 May 2019. [Online]. Available: https://www.forbes.com/sites/miriamtuerk/2019/05/16/fixing-amazons-drone-delivery-problem/#1db099794d37.

[351] G. Paul, "Verizon wants to become the first carrier to use its 5G network to connect 1 million drone flights," Business Insider, 30 December 2019. [Online]. Available: https://www.businessinsider.com/verizon-highlights-5g-drone-opportunity-2019-12.

[352] Gemalto, "Introducing 5G networks –Characteristics and usages," Gemalto, February 2016. [Online]. Available: https://www.gemalto.com/brochures-site/download-site/Documents/tel-5G-networks-QandA.pdf.

[353] R. Korman, "What is 'safe enough' for drone deliveries?," The seattle times, 22 February 2019. [Online]. Available: https://www.seattletimes.com/business/boeing-aerospace/what-is-safe-enough-for-drone-deliveries/.

[354] PublicSafetyCanada, "The Canadian Disaster Database," PublicSafety Canada, [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/cndn-dsstr-dtbs/index-en.aspx. [Accessed 18 December 2019].

[355] Openaddresses, "The free and open global address collection," Openaddresses, [Online]. Available: https://openaddresses.io/. [Accessed 10 January 2020].

[356] M. Demir, "Steps of Data Ingestion," [Online]. Available: https://github.com/m-demir/DeliveryAssurance/StepsOfDataIngestion.

[357] JAWG, "Interactive maps for your business," JAWG, [Online]. Available: https://www.jawg.io/en/. [Accessed 10 Jan 2020].

[358] M. Demir, "Elevation Application," [Online]. Available: https://github.com/m-demir/DeliveryAssurance/elevation.

[359] copypastemap, "Create a MAP straight from Excel!," copypastemap, [Online]. Available: http://www.copypastemap.com/map.php.

[360] L. M. Segarra, "This Racing Drone Just Set a Guinness World Speed Record," Fortune, 14 July 2017. [Online]. Available: https://fortune.com/2017/07/14/fastest-drone-guinness-world-record/.

[361] F. Corrigan, "Drones For Deliveries From Medicine To Post, Packages And Pizza," DroneZon, 19 December 2019. [Online]. Available: https://www.dronezon.com/drones-for-good/drone-parcel-pizza-delivery-service/.

[362] BitDegree, "Did You Know There are 861 Blockchains?," BitDegree, 15 May 2019. [Online]. Available: https://blog.bitdegree.org/did-you-know-there-are-861-blockchains-c60e1720fad5.

[363] D. H. Collins and R. L. Warr, "Failure time distributions for complex equipment," *Quality and Reliability Engineering International ,* vol. 35, pp. 146-154, 2018.

[364] E. Petritoli, F. Leccese and L. Ciani, "Reliability and Maintenance Analysis of Unmanned Aerial Vehicles," *MDPI Journals,* vol. 18, no. 9, 2018.

Glossary

ABE	Attribute Based Encryption
AI	Artificial Intelligence
ASICS	Application Specific Integrated Circuits
BADA	Blockchain-based Aid Delivery Assurance
BIDAS	Blockchain and IoT Delivery Assurance on Supply chain framework
BPMS	Business Process Management Systems
BT	Blockchain Technology
BTTF	Blockchain Technology Transformation Framework
CARs	Canadian Aviation Regulations
CAV	Connected and Automated Vehicles
CDIC	Canada Deposit Insurance Corporation
CDN	Content Delivery Networks
CPU	Central Processing Unit
CSV	Comma Separated Values
DAG	Direct Acyclic Graphs
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
HE	Homomorphic Encryption
HP3D	Hybrid peer-to-peer physical distribution
IoT	Internet of Things
IPFS	Inter Planetary File System
JSON-LD	Linked JSON Object Standard
JVM	Java Virtual Machine
LEM	Local Energy Market
MOBI	Mobility Open Blockchain Initiative
N-CART	Network-Centric Research Team
NFC	Near Field Communication
PKI	Public Key Infrastructure
POC	Proof of Capacity

PoET	Proof of Elapsed Time
POS	Proof of Stake
POW	Proof of Work
RDBS	Relational Database System
RFID	Radio Frequency Identifier
SQL	Structured Query Language
TPS	Transactions Per Second
TYS	Trust Your Supplier
UAV	Unmanned Aerial Vehicles
VIN	Vehicle Identification Number