Reputation and Trust Management in Gem Supply Chains using Blockchain

By
Chaudhry Imran Ali
2015-NUST-MS-IS-119181

Supervisor
Dr. Shahzad Saleem
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Information Security (MS IS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(August, 2019)

Approval

It is certified that the contents and form of the thesis entitled "**Reputation and Trust Management in Gem Supply Chains using Blockchain**" submitted by **Chaudhry Imran Ali** have been found satisfactory for the requirement of the degree.

Advisor: **Dr. Shahzad Saleem**
Signature: _____

Date: _____

Committee Member 1: **Dr. Adnan Khalid**

Signature: _____
Date: _____

Committee Member 2: **Dr. Naveed Ahmed**

Signature: _____
Date: _____

Committee Member 3: **Dr. Syed Taha Ali**

Signature: _____
Date: _____

Dedicated

to

My loving parents and my wife, who have been there to support and motivate me during my masters degree

Truly dedicated to my supervisor Dr. Shahzad Saleem. It would never have been possible without his efforts and encouragement

Certificate of Originality

I hereby declare that this submission titled **Reputation and Trust Management in Gem Supply Chains using Blockchain** is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or any other education institute, except where due acknowledgment, is made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic is acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: Chaudhry Imran Ali
Signature:_____

Acknowledgment

I would like to thank Allah Almighty for His blessings and giving me this opportunity, the strength and the patience to complete my MS thesis finally, after all the challenges and difficulties. I am very thankful to my parents for their love, prayers and never-ending support throughout the research work. I wish to thank all my family members, especially my wife for her support, encouragement and motivation.

I am indebted to profound gratefulness and sincere efforts of my advisor Dr. Shahzad Saleem at SEECS - NUST, Pakistan for his facilitation, outstanding supervision, continuous support, and providing me the opportunity to conduct research under his supervision.

I would also like to thank Ms. Sidra Malik at UNSW, Australia in co-advisory role, for her guidance, research support and supervision in understanding the topic and providing me with the opportunity to work with her.

I offer special thanks to my committee members, Dr. Adnan Khalid, Dr. Naveed Ahmed, and Dr. Syed Taha Ali who have always given me their precious time and guidance during my entire thesis phase. Many thanks for their valuable suggestions and comments on my research work that has helped me in successful completion of my MS thesis.

Chaudhry Imran Ali

Table of Contents

List of Figures

List of Tables

Abstract

Supply chains today generally face many complex challenges when focusing on traceability, provenance, trust and integrity. When applied to gem industry, users' requirement for originality of produce and its worth, industry players' requirement for greater transparency, and lack of effective legislation to achieve this has been of concern. This work aims to facilitate corporate responsibility for due diligence and improvement in gem supply chain management. Evolution and application of blockchain technology here addresses the inherent issues of transparency in supply chains. Blockchain provides an immutable trail of all transactions taking place in a supply chain. However, trust itself cannot be established for the associated data in totality. A trust management framework is proposed as a mechanism to address the trust challenge in blockchain enabled gem supply chains. We propose a multi-layered architecture over blockchain for managing trust in gem supply chain. Our novel approach ensures credible end product at the retailers' end in terms of proofs of location, custody and assessment. The trust management in our solution also involves the reputation management of traders. We have also automated the reputation score calculation using smart contracts. Our proposed solution can help stimulate a fair pricing mechanism as future work that can be based on the trust level associated with the end product and the reputation of the seller. Our architecture is developed using Hyperledger, and is supported by shared network model which ensures scalability and provenance with minimal overhead.

Chapter 1

Introduction

This chapter provides an account of general security issues in digitized supply chains. Gem stone supply chain was selected as a use case to conduct our research. Discussion later develops focusing on provenance, traceability, accountability, reputation systems and trust management using the blockchain implementation of a supply chain. A detailed problem statement further provides an account of the need and importance of this research. Moreover, several motivation factors regarding applicability for our proposed architecture in various business domains are briefly stated to signify the importance of our research. A layout of this document is provided in the last section.

1.1 Overview

Business is mostly about competitiveness. Supply chains are critical to ensuring that a business yields maximum profit in least possible investment of resources. Blockchain technology offers an ideal combination of data storage, security, integrated payment models, and cost reduction which makes it worthy to be explored for application in business supply chains.

1.1.1 Definitions

Before we proceed, it is important that we define some keywords which will be used through out this documents. An account of these definitions is as follows:

1.1.1.1 Traceability

Traceability is a term that, in context of our research, usually refers to establishing chain of custody of produce within a supply chain. Schwagele

describes forward and backward traceability of a product in supply chain between origin and the retailer, referring it to as Tracking and Tracing respectively [4].

1.1.1.2 Provenance

According to Price and Burton, provenance information generally establishes the place of origin, or source, for an artifact or an object of value [5]. In case of gem supply chains, we use the term provenance to refer to the place of mining or discovery of a gem.

1.1.1.3 Trust

We are opting to benchmark Whitener's definition of trust [6], which states:

"First, trust in another party reflects an expectation or belief that the other party will act benevolently. Second, one cannot control or force the other party to fulfill this expectation - that is, trust involves a willingness to be vulnerable and risk that the other party may not fulfill that expectation. Third, trust involves some level of dependency on the other party so that the outcomes of one individual are influenced by the actions of another".

1.1.2 Blockchain

Blockchain was first introduced as an underlying architecture facilitating the crypto currency of Bitcoin [7]. Blockchain is an immutable ledger of blocks where each block stores a set of information records known as transactions. These blocks are hash chained such that once a block becomes a part of chain, nothing in the past can be changed about that block. Thus, blockchain can be termed as distributed database that holds records of digital data or events in a way that makes them tamper-resistant. Every transaction is recorded on a block and then these new blocks are broadcast as ledger. This ledger is synchronised among all the nodes on peer to peer network which is why it is highly transparent. The core architecture of blockchain system is that of a distributed system.

1.1.3 Distributed System

It is essential to understand distributed systems to correctly understand blockchain. Distributed systems platforms are modeled for users to view

a single interface, behind which multiple nodes are interacting and coordinating with each other to accomplish a single common task. Global supply chains have a distributed architecture. Our research emphasizes on application of blockchain, a traditionally decentralized immutable ledger, in supply chain. Our work contributes developing reputation to facilitate trust management for the produce and the participants in gem supply chains by adding credibility to data generation and introducing rewards.

1.1.4 Transparency and Blockchain

Transparency has long been a challenge in supply chain management. Application of blockchain as a solution has transformed this area for the better. Blockchain, keeping a very secure record, provides every single detail of all the products and phases in the supply chain. From procurement of raw goods to sale and customer support, blockchain keeps track of movement of material within the supply chain. With that kind of ownership data, for which integrity is not an issue, transparency can be provided in order to either introduce rewards or penalties by managing trust. Moreover, since data is available to every authorized participant in the network, it can help to examine transactions, perform audit, discover anomalies, perform remedial actions, and much more.

1.1.5 Research Areas

There are several dimensions to this research project generally spanning over areas of distributed systems, blockchain, reputation systems, trust management and supply chain digitization. In coming chapters, we shall briefly introduce the mentioned areas and focus primarily on existing research related to application of blockchain in supply chain and evolution of reputation systems.

1.1.6 Use Case: Gem Industry Supply Chain

As a use case, we have studied applicability of blockchain in gem stone supply chain where the mined produce can be tracked right from when its extracted, traded and reaches the retailer shelf.

1.2 Problem Statement

Modern supply chains heavily rely on technology infrastructure. While there has been a lot of research on human resource, operations, technology, sustainability and risk factors related to supply chains, the areas of trust integration, layout and transparency have largely been of less focus. The evolution of block chain technology is interesting and it has many promising security features as discussed in sections 1.1.2 and 1.1.4. Blockchain facilitates integrity and privacy of data to a greater extent. However, a basic supply chain blockchain cannot guarantee and improve quality of data stored on it. In order to achieve comprehensive trust, there's a need for improved trust management for produce, traders and consumers.

Building reputation and managing trust for supply chain participants is not easy as ensuring the credibility of data does not depend on a single source. As stated in 1.1.6, we opted for a use case of gem stone supply chains. The following factors limit the development of an effective trust management system using blockchain:

1. How can trust be established along with provenance in gem stone supply chains?
2. Unlike Bitcoin blockchain, where the origin of digital currency can be verified over blockchain itself, the data associated with physical events is not verifiable over blockchain. Hence the supply chain data on blockchain cannot be trusted.
3. Supply Chain is complex with multiple sources of data and each data source must be assessed for its part in trust management.
4. Supply Chain demands a hybrid trust model which can support the reputation of produce and the traders.
5. The trust management systems involve the penalties and incentives which are difficult to monetize for blockchain based supply chain solutions.
6. Integration of trust management systems with blockchain based solutions.

1.3 Motivation

In today's business, customer and end user is of critical importance. With growing conscience and information available to gauge marketed claims by

businesses, the end users tend to drive transparency in modern business operations such as supply chains. A reputation system based on inherently secure blockchain network shall put forth non-tampered and accurate notion of accountability. Such a system shall help improve the trust levels attached with produce and traders, and provide participating nodes with rewards based incentives in supply chain.

This research may be applicable to different areas such as financial systems, technology, production, processing, data security, etc. by applying area specific customization. In Pakistan, opportunity exists of practical applications to record keeping operations, production and processing supply chains, e.g. mining industry, land records department, agriculture and dairy supply chains etc.

1.4 Our Approach

The block diagram in Figure 1.1 shows the phases in which our research work has been carried out.

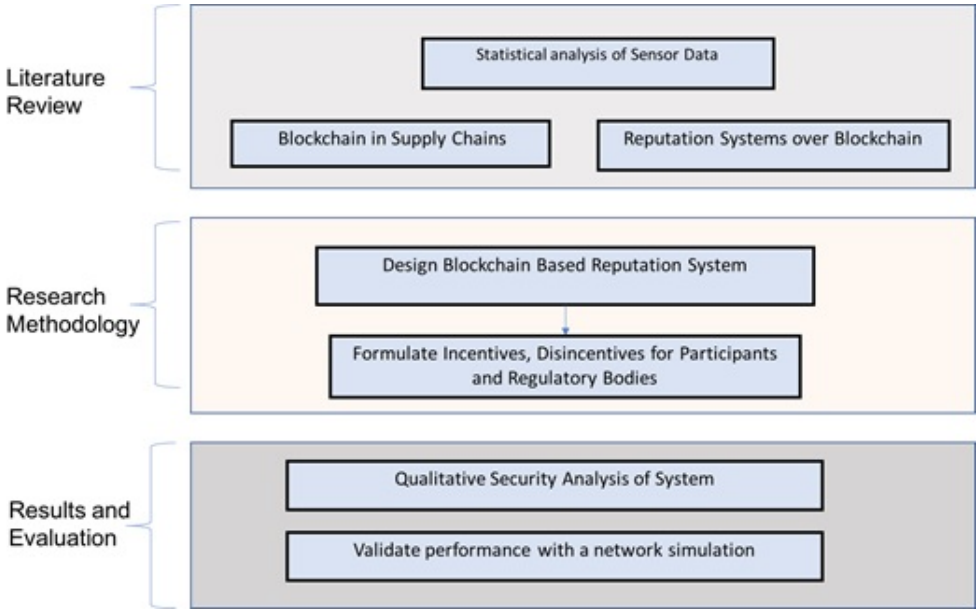

Figure 1.1: Proposed Research Methodology

The next chapter 2 provides an account of the technologies related to our research. In consequent chapters we discuss above-mentioned research phases in Figure 1.1 in detail.

1.5 Thesis Organization

This document is divided into several chapters with each chapter addressing a specific phase of the research conducted. An overview of the details of each chapter is provided below:

- **Chapter 1 (Current):** This chapter provides an account of general security issues in digitized supply chains. Gem stone supply chain was selected as a use case to conduct our research. Discussion later develops focusing on provenance, traceability, accountability, reputation systems and trust management using the blockchain implementation of a supply chain. A detailed problem statement further provides an account of the need and importance of this research. Moreover, several motivation factors regarding applicability for our proposed architecture in various business domains are briefly stated to signify the importance of our research. A layout of this document is provided in the last section.

- **Chapter 2:** This chapter provides an overview of supply chain, trust, transparency and reputation systems. Various tagging technologies that are used to track produce in supply chains are briefly explained. It further details overview of the Blockchain technology architecture and its application to modern supply chains. Furthermore, this chapter sheds some light on Hyperledger, the implementation platform used to implement our use case gem industry supply chain.

- **Chapter 3:** This chapter provides an account of existing work relating to provenance and establishing trust in digitized supply chains using blockchain. Blockchain technology has evolved greatly over recent years and its application to modern supply chains is very useful. An extensive literature survey has been done to mention various such traceability solutions in gem stone industry. Moreover, an account of state-of-the-art trust management solutions in supply chain management using blockchain has been provided. Different reputation systems that exist and their shortcomings are mentioned. We further discuss how a blockchain implementation helps provide a better solution to the shortcomings of existing work.

- **Chapter 4:** This chapter describes the methodology of our proposed blockchain based trust management solution for gem supply chain. The design is explained in terms of general architecture, proposed trust mechanisms and consumer benefits. The proposed trust framework can assign the trust score to an asset based on its provenance, custody

and quality information stored on blockchain. The framework also supports the reputation of supply chain participants in a permissioned blockchain. Supply chain specific transactions are formulated which help in finding instant and long term reputation scores for an asset and traders in the network. Lastly, we summarize how these mechanisms can benefit a end term consumer.

- **Chapter 5:** This chapter describes the implementation related details of our proposed blockchain based framework. Implementation primarily comprises of an experimental setup depicting an abstract gem supply chain. Our experimental setup is described in context of related technologies that have been used in the blockchain implementation. Discussion covers the transaction flow with respect to the proposed model and Hyperledger framework. The blockchain architecture discussion includes the basic model, participants, access control, queries and transactions on the ledger. The transaction flow lists the systematic flow of transactions from clients with respect to both query and write transactions on the network. The third section in this chapter discusses how and which technologies have been used in context of our implementation, which include Hyperledger Fabric, Hyperledger Composer, Hyperledger Caliper, and Apache bench-marking tool.

- **Chapter 6:** This chapter first provides a qualitative security analysis of our proposed framework with respect to the known security attacks in context of reputation systems. It also discusses the system assumptions with respect to security and blockchain in built security features. The second section of this chapter outlines a brief discussion of the benchmarks i.e. transaction commitment time, query time, throughput, latency and resource consumption. The results are obtained using the tools described in chapter 5 for both the blockchain hosting Trust Management System (TMS) and without a TMS. Discussion related to the results is outlined in the subsequent sections.

- **Chapter 7:** This chapter describes the synopsis of our thesis work, research findings, conclusion, and future work directions.

Chapter 2

Background

This chapter provides an overview of supply chain, trust, transparency and reputation systems. Various tagging technologies that are used to track produce in supply chains are briefly explained. It further details overview of the Blockchain technology architecture and its application to modern supply chains. Furthermore, this chapter sheds some light on Hyperledger, the implementation platform used to implement our use case gem industry supply chain.

2.1 Supply Chain

Supply chains have been described by Londe and Masters [8] as a business process in which material is passed between entities. Production businesses usually involve multiple operators that make it possible to get the product ready for the end user. These intermediary players involved in raw material production, assembly, wholesale, logistics and retail are all parts of the supply chain. Lambert et al. describe a supply chain as a collection of firms that make a product or service possible for the end user [9]. Christopher [10] categorizes these participating firms in upstream and downstream categories performing the role of suppliers and distributors respectively to make the product possible for end user. The nature of relationships among supply chains participants have evolved over time as the rules of engagement have evolved over time.

2.1.1 Adversarial Interaction

Business has always been about efficiency and profit. Traditional interaction among supply chain participants has been on aggressive and negotiation

based on confrontation or intimidation in order to cost of doing business. As described by Hacker et al., in the past business negotiations involved heavy reliance on leverage which mostly resulted in a win-lose scenario [11]. In other cases, as described by Welty and Becerra-Fernandez, aggressive competition among suppliers used to be crafted in order to improve cost. However, in this case the participants usually failed to exercise total potential [12].

2.1.2 Long-term Stable Interaction

With the rise of twenty first century emerged the concept of globalization. Zineldin and Jonsson mention that growing international and regional interaction along with more efficient and effective availability of information called for a more stable, trusting and long-term interaction between supply chain participants [13]. This gradually evolved into a world with rapid outsourcing where businesses preferred to focus on their core business. This provided a platform for long-term relationships between supply chain participants, according to Sahay [14].

2.1.3 Collaborative Interaction

Business relationships have evolved into mutually beneficial setups between manufacturers, distributors, retailers and customers. The primary focus being on exchange of value and expertise helps lower costs and risks. Sahay and Maini mention that such kind of an interaction requires established trust and commitment [15]. Provenance, trust and value are complex in real world operations and play an important role in managing these kinds of business relationships in modern supply chains.

2.2 Supply Chain and Trust

Trust in definition has a large number of influencing factors and can be explained in various ways. In addition to section 1.1.1.3, Mayer puts forth a relatively general definition that trust may be established when a party A is willfully vulnerable to party B where party A expects party B to undertake important tasks and party A has no means to confront party B [16]. Using this, Kannan and Tan emphasize the importance of trust as core part of the supply chain operations [17].

Chandra and Kumar state that the evolution regarding the role of trust in supply chain started when the cost theory of business transactions was challenged putting emphasis on trust and collaboration [18]. The argument

advocated availability of certain competitive advantage if trust is established properly. Trust also was proven to decrease the level of uncertainty. Furthermore, having established a trusted relationship, focus rightly shifted towards the need of the end user, which itself was a great benefit of trust.

2.3 Trusted Records

Reliability is measured by effectiveness of the controls and ability of the author of that control, according to Duranti and Rogers [19]. Reliability has primarily to do with trusting the source of information. Duranti and Frank further describe that a trusted record of transaction primarily means a record that is reliable and authentic [20]. An authentic record is that has trust associated to its identity. Integrity of a record also contributes to its authenticity mentions Lemieux [21]. Lemieux further states that authenticity of a record also depends on its management over time [21].

2.4 Reputation Systems

Reputation Systems are extensively used in e-commerce websites as we consider customer experience important. One of such well known reputation systems is that of ebay.com. A reputation system aims to establish a trustworthiness of sellers and minimize the risk of fraud. Other application areas include stockexchange, filesharing and peer to peer applications. In case of peer to peer decentralized networks such as blockchain, a reputation system can incentivize for more user participation and also avoid the potential misbehavior on account of losing reputation on blockchain. We first briefly discuss different approaches used for building a reputation system followed by some specific literature on their application in blockchain.

Various trust and reputation systems have been proposed or implemented in different open systems, e.g. P2P, multi-agent or e-commerce systems. In attempt to systematically compare the various approaches, reputation systems can be classified into three broad categories according to Wang and Vassileva [22]:

2.4.1 Centralized vs. Decentralized

In a centralized system, a central node is responsible for managing the reputations of all the other nodes in the network. The presence of central reputation manager is missing in peer to peer nodes. These decentralized systems need to share and build a consensus over a reputation calculation which tend to

rely on more complex and sophistication. Majority of the reputation management systems (RMS) designed for web services are centralized.

2.4.2 Agents vs. Resources

Trust and reputation systems can be classified as agent systems or resource systems. In agent based systems, the reputation of people/nodes (agents) is modelled where resource systems, the focus is modelling reputation of resources, which could be assets or services. There is no fine line between both as building the reputation of people/agents also serves for the purpose of building representation of the reputation of resources.

2.4.3 Global vs. Personalized

In global reputation systems, the reputation of an entity (i.e. a agent/asset/service) is based on the feedback from the public and visible to all the members. In personalized reputation systems on the other hand, for a particular agent, the reputation is built on the feedback from a group of members either selected by agent itself.

2.5 Blockchain Technology

Blockchain technology was presented by Satochi Nakamoto in 2008 in a whitepaper proposing Bitcoin, a digital currency platform [7]. Later research has over the years investigated blockchain's applicability to other areas of business. Blockchain can be seen in different perspectives relating to business or technology. Characteristics of blockchain are that it is a database that is crypto secure, immutable, append-only distributed ledger that can be updated only through a consensus mechanism among participants.

What this means from a business perspective is that blockchain provides a platform where participants can interact and exchange data of value without a centralized entity. This concept is an enabling revolution to facilitate trust and transparency like never before in transactions of value. A basic block in blockchain is made up of transaction data, a time stamp and a hash value or previous block as shown by Figure 2.1. In general terms, it is a logical organization of selected transactions put together. The structure can be customized in relation to the use case of blockchain being designed. A general structure of a blockchain hence is demonstrated in Figure 2.2.

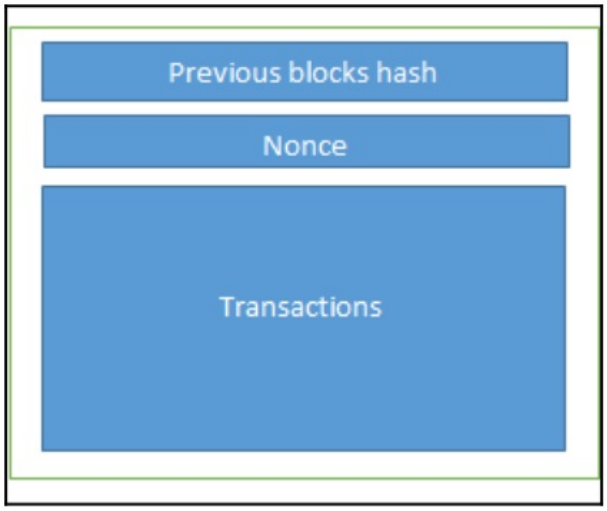

Figure 2.1: Basic view of a block [1]

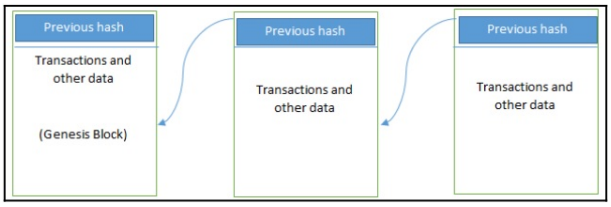

Figure 2.2: General structure of Blockchain [1]

2.5.1 Elements in a Generic Blockchain Structure

Blockchain solutions run in form of a distributed peer to peer network over traditional internet. This is conceptualized in Figure 2.3. We shall briefly discuss generic blockchain elements to develop understanding.

Address
An address of any entity over the network is unique. In case of blockchain, this every participant has an address that is usually based on participant's public key.

Transaction
In blockchain communication, participants exchange data of value among each other. This exchange is referred to as a transaction. Transaction data constitutes the core of a blockchain.

Block
A block is a collection of transactions selected to be placed on the blockchain,

alongwith some additional information such as a reference to the previous block, a time stamp, etc. This additional information depends on the use case of blockchain.

Nodes
Nodes are participants in the blockchain. The roles of these nodes are classified in light of functions performed by them. Blockchain functions include proposing and validating transactions and mining operations to help build consensus amongst peers. More use case specific roles may exist depending on the application of blockchain.

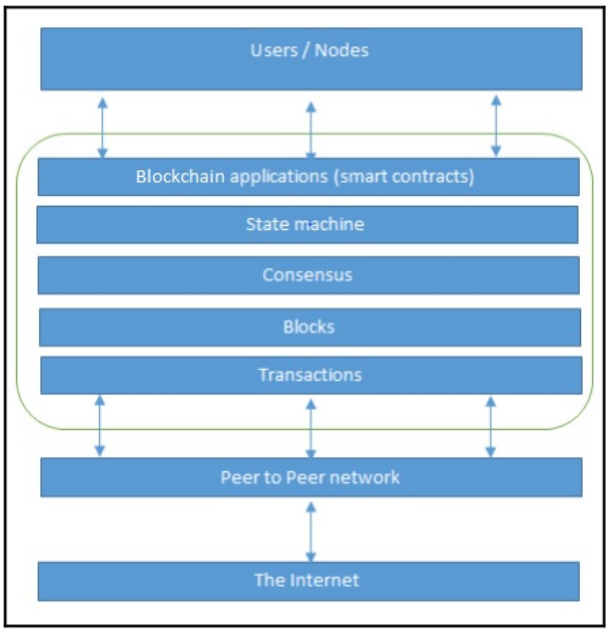

Figure 2.3: Abstract view of Blockchain over Internet [1]

State Machine
When a transaction is processed in blockchain, the whole blockchain transitions between states. This takes place as nodes initiate, execute and validate transactions.

Consensus
In order to establish a uniform state of the blockchain, an agreement must take place between nodes. This process is known as to develop consensus. In

distributed systems, it is difficult to achieve consensus on a single value or state among participating nodes. There are various algorithms that are used to achieve this task.

Smart Contracts
Smart contracts are programs to help automate logic of doing business between participants upon fulfillment of certain stated conditions. Smart contracts are quite powerful and are flexible to provide strength to blockchain operations. However, their use is relative to the blockchain application. Once the contract has been mutually agreed, it cannot be altered. Upon reaching a consensus, the miner node receives the outcome in result of a smart contract execution. The conditions in the contracts are available publicly hence are not private inherently. An application binary interface is used to access the smart contracts.

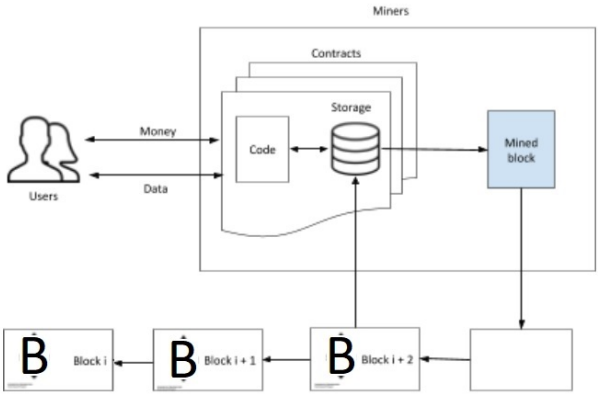

Figure 2.4: Smart contract operation

2.5.2 Accumulation of Blocks in Blockchain

Here, we describe a general mechanism in which blocks are accumulated in a blockchain. This is to develop an understanding as to how transactions are composed to form the blocks as described by Bashir [1].

1. A transaction is initiated by a node when it signs any data of value using its private key.

2. This transaction has to be validated by the participants in the blockchain, for which it is broadcast to all participants. However, usually more than a single node are part of the validation process.

3. Upon validation of the transaction, a block is created and broadcast over the network. The ledger is updated and the transaction stands finalized.

4. The new block is now a part of the ledger and any new block will refer to this block by holding the hash of this block. This acts as a second confirmation for the transactions included in the block.

5. If further confirmations are required as per the design of blockchain, a confirmation of such is made upon creation of every new block.

2.5.3 Private and Public Blockchain

Blockchains are either private or public. A predefined group of participants make up a private blockchain, whereas in a public blockchain anyone can join in at any point in time. Private blockchains suite businesses more as they provide a sense of privacy. However, an issue of trust arises as participants may collude and consensus achieved maybe on fabricated data. There are several blockchain architectures which are hybrid in nature comprising the qualities of both public and private blockchains.

2.5.4 Permissioned Blockchain

A permissioned blockchain consists of participants that are mutually trusted and known already. Since, the trust is already there, the need to build a distributed consensus is not essentially required. Hence, a light protocol for mutual agreement can be used to establish shared state and version of records on the blockchain. A permissioned ledger can be public or private, however in case of public blockchain, managing operation revolves around a regulated access control.

2.6 Hyperledger

Hyperledger is an open-source blockchain technology. This project began in 2015 when several independent companies decided to come together and contribute towards developing a much needed industry standard for blockchain technology. Under the umbrella of Linux foundation, the project has been continuously evolving.

Blockchain is not a one-size that fits all kind of a technology as every business has its own requirements and specific alternation is required in each

case. For this purpose, hyperledger design philosophy is towards a modular, secure, interoperable, standalone and complete with APIs standard. Amongst its other proposed use case scenarios, one is towards implementation of provenance solutions in supply chains which made it suitable for implementing our research.

The hyperledger family comprises of a number of frameworks and tools, listed below, which are suitable for solving different problems.

2.6.1 Hyperledger Frameworks

Hyperledger platform has the following frameworks to facilitate blockchain implementations:

- Hyperledger Burrow
- Hyperledger Fabric
- Hyperledger Indy
- Hyperledger Iroha
- Hyperledger Sawtooth

Hyperledger Fabric For our implementation we opted to use Hyperledger Fabric as it provides a flexible platform for developing blockchain solutions with a modular approach. Fabric provides a high degree of confidentiality, resiliency, flexibility and scalability. As we have discussed that our proposed solution required a permissioned blockchain model, Fabric facilitates that. Moreover, Fabric has been developed keeping in view performance issues with blockchain, like resource exhaustion and slow resolution, which was a preferred choice.

2.6.2 Hyperledger Tools

Hyperledger platform has the following tools to support blockchain implementations using forementioned hyperledger frameworks:

- **Hyperledger Caliper** is a performance assessment tool of the framework that measures functionality against a defined set of use cases.
- **Hyperledger Cello** is an integration tool that include on demand deployments of modules in a blockchain solution.

- **Hyperledger Composer** is a toolset that enables easy development of blockchain solutions and smart contracts. Hyperledger Fabric is well supported by Hyperledger Composer.
- **Hyperledger Explorer** provides a viewing mechanism to inspect details, logs and authentication information of complete data or selected blocks. It facilitates web-based viewing of blockchain implementations.
- **Hyperledger Quilt** revolves around an interoperatibility protocol, Interledger Protocol (ILP) that facilitates inter-ledger transactions and communication.

Our implementation to assess our proposed model is facilitated by Hpyerledger Fabric, Hyperledger Caliper, Hyperledger Composer and Hyperledger Explorer.

2.6.3 Hyperledger Consensus Methods

Consensus mechanism is a means by which participating nodes agree to complete a transaction and provide for validation of the transaction block. Consensus primarily requires establishing correctness of all the transactions in a block. This is achieved through smart contracts which verify the order and results of execution on which there is an agreement at a global state.

Speed, scalability and latency are common problems when dealing with blockchain networks. There are various consensus mechanisms that are used to achieve consensus depending on different network requirements. Default blockchain implementation in case of Bitcoin uses a Proof of Work algorithm to achieve consensus. Other than that, two main categories are lottery-based and voting-based algorithms.

Lottery-based algorithms are useful in scenarios where scalability support is of importance. There can be a single or multiple winner nodes amongst the miners and the winner sends the block to rest of the participants to seek validation. However, as the number of winners increase and proposals made by each node are to be resolved, finality of the transaction becomes an issue.

On the other hand, a lower latency is provided by the voting-based algorithms. In this mechanism, the block validated by majority of the participants is finalized. However, it is much slower in achieving consensus since all the participants exchange messages with each of the other participants.

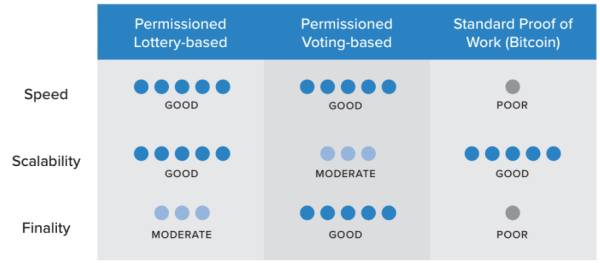

Figure 2.5: Comparison of approaches to achieve consensus

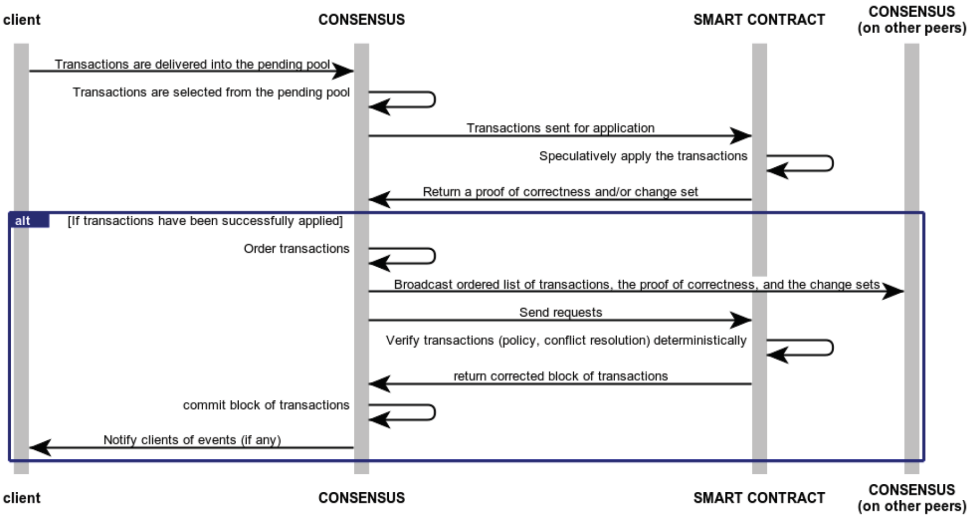

Figure 2.6: General consensus protocol in Hyperledger

2.7 Tagging Technologies

Different tagging technologies are used to track items and material in supply chains. This information over blockchain is used to establish provenance, on the basis of which trust can be managed. A few of the common tagging mechanisms are described here for better understanding of chain of custody and location of an item in the supply chain.

2.7.1 Quick Response (QR) Codes

QR codes are binary codes that work on the same concept as that of barcodes. These codes are presented in a two dimensional binary depiction, black and white, of pixels. QR codes are processed faster than usual barcodes. The common use cases are revolve around identification and product portfolio management. Micro and nano QR codes are used in modern gem stone and

mineral mining supply chains.

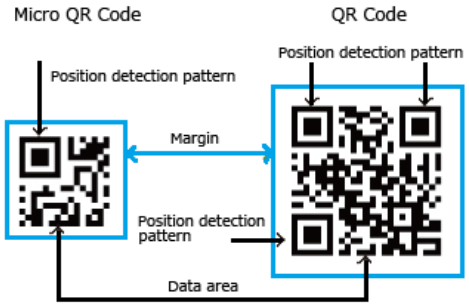

Figure 2.7: QR codes

2.7.2 Radio Frequency Identification (RFID)

RFID is implemented using specific hardware comprising a tag, a reader and an antenna. The reader is connected to a computer and is used to scan the RFID tag. A tag is scanned when within scanning range of an RFID antenna embedded in the RFID reader. The scanning operation is successful when a second antenna embedded in the tag reflects the reader antenna signal. A rectifier converts the reader's signal to power up the tag. The tag has a small memory that stores the product information. RFID technology only requires certain proximity and does not require the reader and tag to be in sight of each other.

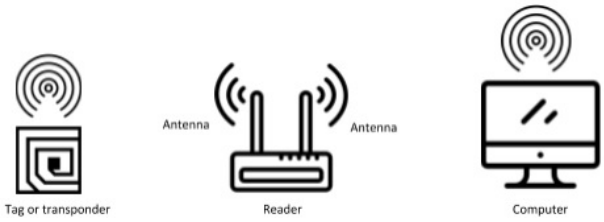

Figure 2.8: Basic RFID Scanning

2.7.3 Near Field Communication (NFC)

NFC has been advocated to be a secure short range communication technology. For a device to be able to communicate through this, it has to be NFC compatible. The two communicating devices should be in close proximity to

each other with an in between range of 4cm. NFC facilitates quick sharing of data simply by establishing physical device contact. It is considered very secure due to the very short distance between the communicating devices.

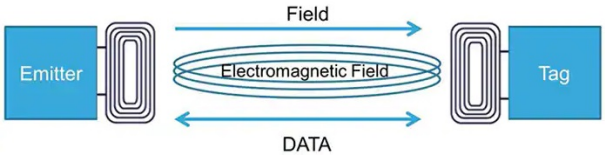

Figure 2.9: NFC Technology Basics

Chapter 3

Related Work

This chapter provides an account of existing work relating to provenance and establishing trust in digitized supply chains using blockchain. Blockchain technology has evolved greatly over recent years and its application to modern supply chains is very useful. An extensive literature survey has been done to mention various such traceability solutions in gem stone industry. Moreover, an account of state-of-the-art trust management solutions in supply chain management using blockchain has been provided. Different reputation systems that exist and their shortcomings are mentioned. We further discuss how a blockchain implementation helps provide a better solution to the shortcomings of existing work.

3.1 Track and Trace

As Schwagele had put it for supply chains, forward and backward traceability of a product between origin and the retailer is referred to as Tracking and Tracing respectively [4]. However, the definitions may change with different industrial sectors.

Traceability does not necessarily mean that the product is completely traceable such that each step in its life cycle is verifiable. In the gem industry, the use of tagging technologies is a must and micro QR codes are very common to refer to information regarding origin.

In coming sections we provide an account of existing research on traceability in blockchain based supply chains. Then, we move onto detailing state-of-the-art on traceability in gem industry supply chains using both conventional models and blockchain in seperate sections. An effective traceability and provenance solution supplements trust managed through a reputation system in supply chain management.

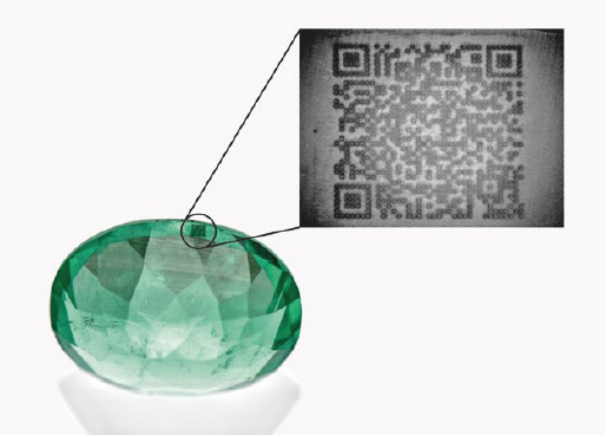

Figure 3.1: Micro QR inscribed on an emerald

3.2 Traceability using Blockchain in Supply Chains

Blockchain has gotten the supply chain businesses interested and many solutions have been proposed to enforce transparency and traceability. Many industry leaders like IBM and Walmart [23] have contributed to such solutions. Some of the examples include Hyperledger Framework [24], Block-verify [25], and Provenance [26]. The nature of these systems is proprietary with any detailed architectural information not being available generally.

There has been a lot of contribution from academia and individuals besides the aforementioned industry solutions. The published research in this domain is described below in categories of supply chain use cases.

3.2.1 Agri and Food Supply Chains

A generalized design for agricultural and food supply chains is presented by Feng [27] that is based on public blockchain and sensor data from the supply chain. The work has been improved by Feng catering the issue of scalability [28]. However, the proposed work has many unexplained aspects like organization of blockchain, access and system audit.

Originality is of extreme importance in alcohol products in determining their value. Biswas et al. in [29] provide a traceability solution for wine production. The proposed system is a private blockchain implementation using MultiChain and establishes traceability for individual bottles. It is proposed that the origin and history information is stored in the blocks that are verified by pre-selected nodes. However, the system has scalability issues.

Furthermore, the design does not address provenance for actual ingredients of the wine.

Like any other distribution network, fish supply chains start at the producer and ends with the consumer. This supply chain has many intermediary participants. A research into Tuna fish supply from Indonesia has shown that there is substantial room for improving transparency and traceability [30]. The fish is processed locally and then distributed to local and international client base. However, there is lack of information for fishing trips that hinders establishing provenance. This is also because suppliers have aggregated product from different producers. Another issue is human intervention in records management.

3.2.2 Manufacturing Supply Chains

Toyoda, et al. [31] propose a system to trace produce by storing the product and owner information on the blockchain for the period of possession. Such a system is helpful to limit counterfeiting. The produce is tagged and for every stage in trade transit, the tag information is updated. However, the solution is limited to traceability between the manufacturer and the consumer. It does not facilitate establishing provenance for the product before being in manufacturer's possession, for example, information about the origin of raw material used. Abeyratne et al. [32] propose an alike system for the card board manufacturing industry with similar design limitations.

Counterfeiting is a grave concern in medical and healthcare products. Various such false products are captured due to false origin and fake identity. A blockchain based solution proposed by Modum addresses a similar concern in medical products [33]. The solution caters for monitoring temperature data associated with such products through out the chain of custody in the supply chain. A unique identifier associated with each product is stored in the blockchain along with the related sensor data and metadata, as described by World Health Organisation [34]. However, the solution essentially does not factor in establishing provenance.

3.2.3 Art and Craft Supply Chains

Arts and crafts work is very precious for artists, production houses, heritage centres, governments and for collectors. Every player is extremely concerned about the origin of the work. The present mechanisms are incapable to ensure authenticity of the artifacts and are not thoroughly reliable. The onus of responsibility usually lies with the intermediaries, for example, the auctioneers, who fear a slippery slope. Therefore, provenance information is very much

desirable for everyone. Codex protocol title registry is implemented using blockchain by Codex, where ownership history of an artifact is represented by a token [35]. The registry also stores hash values of related transaction data. However, there are various associated challenges. The solution cannot deal with existing artifacts. The other obvious challenge is establishing fidelity between physical artifacts and associated records.

3.3 Traceability without Blockchain in Gem Industry

3.3.1 Overview

Traceability and provenance are hot topics in the gem industry supply chains. The implications are on business, customers, environment, human rights and much more. Recent research studies and reports by Walker [36], Archuleta [37], CIBJO [38] shed light on traceability in gem industry. Recent reports by Human Rights Watch [39] thoroughly explain rights abuse in mining and production of gems. Gem industry is of a very complex structure and due to this deep fragmentation, information available as to the mining, production and sale of these gems is very valuable.

The information related to provenance has become very sought after by consumers, traders and collectors of these gems as claimed by Nash et al. [40] and De Angelis et al. [41]. There is a global call by relevant organisations and platforms for increased scrutiny and responsibility for the practices in gem industry [42] [43]. This has motivated legislation at the government level both in the United States and European Union - Dodd-Frank Reform and Protection Act, Conflict Minerals Regulation respectively.

Table 3.1: Origin determination for gems by laboratories globally [3]

#	Gem	Common Origin
1	Alexandrite	Africa (Madagascar, Tanzania), Brazil, Russia, Sri Lanka
2	Cu-bearing Tourmaline	Brazil, Mozambique, Nigeria
3	Demantoid	Madagascar, Namibia, Russia
4	Emerald	Afghanistan, Brazil, Colombia, Ethiopia, Zambia
5	Ruby	Afghanistan, Madagascar, Mozambique, Myanmar, Tanzania, Thailan, Vietnam
6	Sapphire	Kashmir, Madagascar, Myanmar, Sri Lanka
7	Spinel	Madagascar, Myanmar, Sri Lanka, Tajikistan, Tanzania, Vietnam
8	Tsavorite	East Africa (Kenya, Tanzania)

Earlier 21st century, the gem industry was struck with grave concerns regarding blood diamonds and there was a lot of research published in order

to determine provenance for the diamond industry specifically. However, according to Dalpe et al. no certain mechanism can be said to ascertain the origin of the diamonds based solely on traditional scientific apparatus [44]. Mostly, the following geographic locations for determination of origin are considered by global laboratories as shown in Table 3.1.

A major challenge in gem industry is cutting of a stone into smaller pieces. There is no scientific method to ascertain the origin of a cut stone. Therefore, the industry has adopted other methods like proof of origin and proof of custody.

Similarly, research for distinguishing freshwater pearls from cultured ones shifted from origin determination to using benchmarks derived through sampling. However, Hanni and Cartier have emphasised that the focus has been back on ascertaining the origin of these pearls [45].

Norton et al. describe that there are various traceability models which are applicable in different scenarios and have a variable success rate [46]. The most common models include: 1) Identity Preservation, 2) Bulk Commodity or Segregation, 3) Mass Balance, and 4) Book and Claim. Table 3.2 presents a brief insight into utility of each method.

Table 3.2: Sustainability of existing traceability models [3]

Traceability Model	Approach	Level	Cost	General Example	Gem Example
Identity Preservation or Track-and-Trace	Certified materials and products are physically separated from non-certified materials and products at each stage along the supply chain.	Highest	Very Costly	Consumer would know exact farm from which a banana or salad was sourced.	Exact mine-of origin information is tracked through the supply chain.
Bulk Commodity or Segregation	Separates certified from non-certified materials but allows mixing of certified materials from different sources. All producers must comply with the certification standards.	High	Costly	An organic chocolate bar that contains cacao beans from various organically certified producers. Another example is Kimberley Process rough diamonds certified as 'conflict free'.	An aggregation of goods from one company that operates several mines; also useful for gem regions/countries and could be complemented by gemmological analysis.
Mass Balance	Certified and non-certified materials can be mixed. However, the exact volume of certified material entering the supply chain must be controlled. Claims of 'this product contains X% of certified ingredients' can be made.	Low	Slightly Costly	If 20% of the total cocoa purchased comes from fair trade sources, 20% of a company's chocolate bars made with that mix of cocoa can include the fair trade certified label.	Material from different mines (and certified and non-certified goods) can be mixed. Traceability information is lost.
Book and Claim	Allows all actors of a supply chain to trade in certificates for certified sustainable materials. Buying certificates allows retailers and manufacturers to claim that their business supports the production of sustainable materials. Claims of 'this product supports the sustainable sourcing and production of essential commodities' can be made.	Low	Reasonable	Companies wishing to make sustainability claims can purchase certificates (even though their goods may not be certified) that support sustainable production.	A synthetic diamond manufacturer may buy credits and contribute to sustainable mining activities.

3.3.2 Industry Initiatives

As discussed earlier, in the wake of blood diamonds issue, the industry shifted focus to proof of custody methods to facilitate traceability. The tables 3.3 and 3.4 provide an over the years account of several industry initiatives in this regard - conventional and blockchain based traceability models respectively.

Table 3.3: Industry initiatives for non-blockchain based traceability [3]

Initiative and Year	Year	Material	Chain of Custody Model	Supply Chain Segment
World Jewellery Confederation	1961	Jewellery, Metals, Diamonds, Stone, Pearls and Coral	Product Disclosure	Entire Jewellery Industry
Kimberley Process Certification Scheme	2000	Diamonds	Bulk commodity (traceability)	Country of export, only for rough
CanadaMark (Dominion Diamond Mines)	2003	Diamonds	Bulk commodity (traceability)	Diamond industry, from mine to end consumer
Extractive Industries Transparency Initiative (EITI)	2003	Oil, gas and mineral resources	EITI Standard	Mining company payments made to governments
Diamond Development Initiative	2005	Diamonds	Maendeleo Diamond Standards (MDS)	ASM diamond mines (e.g. Sierra Leone)
Responsible Jewellery Council	2005	Coloured stones, diamonds, gold, platinum and silver	Code of practices and chain of custody (gold only)	Entire jewellery supply chain (coloured stones are currently under review)
Initiative for Responsible Mining Assurance	2006	Minerals and metals	Independent third-party verified responsible mining assurance system for mining companies	Mining companies
Love Earth (Walmart)	2008	Gold and Diamonds	Identity preservation (traceability)	Select mines, refineries, manufacturers and retailers
OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High Risk Areas	2009	Minerals (including diamonds and coloured stones)	Due diligence guidelines for sourcing of minerals	Entire supply chain
Diamonds with a Story (Rio Tinto)	2013	Diamonds	Identity preservation (traceability)	From mine to end consumer
Signet Responsible Sourcing Protocol for Diamonds (D-SRSP)	2016	Diamonds	Guidelines for responsible diamond sourcing	Suppliers to Signet Jewellers
M2M Program (GIA)	2017	Diamonds	Platform for consumers to visualise a diamond's story from rough to cut	A rough diamond submitted by a diamond mining company, tracked all the way through manufacturing and retail via M2M platform

3.4 Traceability using Blockchain in Gem Industry

One of the main reasons of considering blockchain an obvious mechanism to provide provenance is Smart Contracts. Kim and Laskowski state that smart contracts not only facilitate authentication of ownership but trades are

Table 3.4: Industry initiatives for blockchain based traceability [3]

Initiative and Year	Year	Material	Chain of Custody Model	Supply Chain Segment
Tracr (De Beers)	2017	Diamonds	Blockchain traceability	From mine to end consumer via blockchain
Diamond Time-Lapse Protocol	2018	Diamonds	Permissioned private blockchain	Manufacturer and retailer interface as well as a consumer interface
Provenance Proof	2018	Coloured stones	Blockchain traceability	From mine to end consumer, via blockchain
TrustChain	2018	Gold and Diamonds	Permissioned private blockchain	From mine to end consumer, via blockchain

automatically validated as well [47]. Investigating blockchain for provenance solutions has a lot to do with smart contracts, as similarly described by Shrier et al. [48].

Petersen and Janson explain the potential of blockchain mechanism as having the ability to resolve existing trust issues in large-scale complex industries [49]. There are various industry solutions proposed for problems in gem industry. These include for diamond industry [32], gem trading [50], jewellery [51], artifacts [52], gem stones [53], minerals [54], general luxury ornaments [55]. The warranties inherently provided by the blockchain mechanism is investigated by the Kimberly Certification Scheme [56]. Everledger, a company providing technology solutions, has recently developed a protocol to track and trace complete journey of a single diamond. A consumer can keep track of all the information through a smart phone [57].

Among several industry initiatives, the recently launched De Beers' GemFair solution in collaboration with Diamond Development Initiative, adocavtes the idea of storing critical information of value [58]. Forexample, in case of a mining site, first hand evidence in form of timestamped photo images can be maintained at the blockchain. The diamond development initiative solution for diamonds traceability is planned to link to the GemFair solution [58].

As we have discussed earlier, our research problem revolves around the fact that strength of the blockchain lies in the transaction data stored on it. There is no built in mechanism for blockchain to verify the event in totality, only the data presented to it can be verified. Therefore, the supply chain would require third-party validation for the system along with independent audits. Traditionally, blockchain solves the problem of reinforcing claims since the ledger is immutable using cryptography mechanisms. Our research is focused on how we can augment the trust level associated with the data, to-be stored on the blockchain, using a reputation management system.

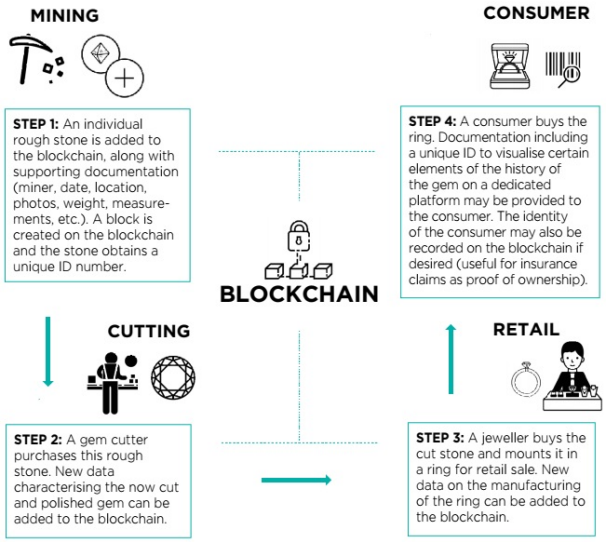

Figure 3.2: A general block diagram for gem blockchain solution [2]

3.5 Trust and Reputation using Blockchain

While blockchain may constitute adequate suitable proof for certain financial articulation statements, it may not give adequate audit or evidence depending upon the type of transactions and role of participants. For instance, in spite of the fact that the exchange of goods is recorded on the blockchain, the auditors may be unable to verify the claimed behavior of the node as a good or bad actor on the blockchain. We describe the general role of reputation systems and their importance in blockchain systems in the following sections.

Reputation systems work well for solving complex trust problems specially in case of public blockchain architecture where the participation of nodes in the network is permission-less (anyone in the network can join and generate transactions). It is also important to state here that in case of permissioned blockchain systems such as those suggested for supply chains (where known supply chain participants interact), the reputation engine could be partially centralized and decentralized. Though there are plenty of reputation systems designed for e-commerce, the area of blockchain based reputation systems is still evolving.

3.5.1 Fraud in Emission Trading

Khaqqi et al. has proposed a novel model for Emission Trading Scheme (ETS) which incorporates blockchain technology to address fraud issues in

ETS management [59]. A reputation system is built on top to improve the systems efficacy. The system is based on priority values where sellers with a higher reputation score have access to better offers. However, the reputation score does not get updated frequently since it is based on the feedback from auditors. This infrequent updating leaves room for exploiting the offers and bidding. The reputation based trading system signifies the participants towards their commitment to participate in emission reduction efforts which is an effective approach for useful participation in emission trading scheme but not applicable to supply chains.

3.5.2 Malicious node in Vehicular Networks

Another of blockchain application is the automobile industry with its increasing development using Internet of Things (IoT). Yang et al. in their work, propose a blockchain reputation system to ensure the data credibility rather than just integrity of the data [60]. The proposed reputation engine highly depends on a large number of messages associated to keep the reputation for changing vehicular environments which causes a network overhead. A temporary centre node is selected to act as a reputation engine. The centre node is selected on the basis of election. It is argued that ratings should be stored on blockchain after consensus among the participating vehicles. This consensus serves as a means of verifying possible malicious entries. The distributed consensus and fair election of these minors adds to the throughput of the network.

3.5.3 A Case of Anonymous Rating

A promising approach for trust less, privacy preserving reputation system is presented by Schaub et al. [61]. It is emphasized that a blockchain based reputation system specially designed for e-commerce applications which can preserve the anonymity of the consumers contributing to the reputation of the service provider. Every time a consumer wants to rate. Their approach highlights the benefits of anonymous rating but lacks some research questions as the number of valid tokens available which are used for rating the service providers.

3.5.4 Reputation in Wireless Sensor Networks

A node authentication mechanism is provided by Moinet et al. in context of autonomous wireless sensor networks [62]. The authors propose their work based on the human like knowledge base which evolves over the time. The

proposed approach is interesting as it is time evolving and we build our architecture on top of such a time evolving reputation system for supply chain.

3.5.5 IBM Crypto-Anchors

Crypto-anchors have been presented recently by researchers at IBM [63]. These anchors serve as digital fingerprint that are tamper-proof and are pinned to products as proof of identity. This addresses counterfeiting in production supply chains. However, its applicability in supply chains needs to be investigated for cost and other factors.

3.6 Suitability for Supply Chains

Despite the extensive use of blockchain technology and profound research over the decades for reputation systems alone, the two systems can complement each other in supply chain if they are thoroughly thought through. We observed that the existing systems mentioned in section 3.5 are unsuitable for supply chains of gem industry where provenance is the most crucial aspect due to following shortcomings:

1. Supply Chain are based on permissioned blockchain meaning that only designated nodes can take part in the recording transactions on blockchain. We may not only want to build a reputation from only a trading party but also from audit bodies, validators, consumers and competitors. Hence supply chain is a multi-role based distributed network with every agent has different stakes.

2. The credibility of supply chain information is important. The IoT sensors contributing to the additional fingerprint to the claimed data cannot be ignored. Currently none of the blockchain based reputation system relates the credibility of sensor information which is much used in the IoT domain.

3. The proposed solutions in literature either rely on pre-calculated reputation values for the data or these values are collected over a single source, i.e. one time GPS coordinates. Other methods only consider data capture using IoT as a trust enabling factor in blockchain solutions.

4. The complexity of gem supply chain demands an atomic reputation model, which must be generic enough to fit multiple supply chain

scenarios. Existing models for trust formulation over blockchain contribute lack trust and reputation formulation required for both the assets and nodes in the network.

5. It is of less discussion so far how the trust mechanisms be automated over blockchain layer or if there is a need for trust information requests to be logged on the blockchain. Not all the proposed methods are tested for their network efficiency or blockchain platform compatibility.

6. The existing approaches lack in providing end to end holistic model for trusting a valuable asset, a consumer trust over data and its integration over the blockchain layer.

In Chapter 4, 5 and 6, we discuss our proposed solution in detail. In light of this discussion, Chapter 7 provides a conclusion addressing the limitations discussed above.

3.7 Addressing the Research Gap

In this section, we mention the objectives of research and that how our research can be beneficial to gem industry supply chain management.

3.7.1 Objectives of our Research

The objectives that were set for this research work are following:

1. Development of a reputation engine which is based on multiple reputation factors, credibility of sensor data, and multiple role based agents.

2. To incorporate the stake as disincentives and incentives with respect to the agent reputation.

3. Development of a permissioned blockchain based trust management system which is evolving, adaptive and reliable over the time.

4. Detection of fake transactions and reputation frauds over permissioned blockchain networks.

3.7.2 Applicability of our Research

Our proposed solution shall help augment the following aspects of supply chain management in the gem industry:

3.7.2.1 Reputation and Trust Management

As described earlier, there are different roles of every supply chain entity on permissioned blockchain. Based on these roles there are multiple events or transactions on the blockchain. For every event, a reputation metric is calculated. Since the events happen consequently, the reputation calculation function is a time decreasing function which evolves as new reputations are built over recent data. Through calculation of this reputation, trust management is done and reflected in digital profiles of supply chain entities. These profiles are visible as ratings and reputation factors when a supply chain participant trades.

3.7.2.2 Determining Agent Incentives and Disincentives

On the blockchain system, the malicious participants stake their reputation and may have a chance to lose some amount in escrow until the transaction and reputation of the supply chain node is deemed trust worthy. On other hand, if the supply chain node maintains a reputation over a certain time in the network, it is eligible for rewards in terms of any crypto tokens. Determining how these crypto tokens can be consumable by supply chain primary producers is a separate challenge that is intended for future work. If these tokens are present in terms of fiat currency then it can cut a huge technology dependency for primary producers in order to redeem these awards.

3.7.2.3 Sensor Data Fingerprinting in Blockchain

We here present a holistic model for sensor based information accumulation which can give a statistical fingerprint based on the data in blockchain, sensor information with respect to the types of sensors and their application, and a module for building a link between analytical fingerprint of the data, transactions on the blockchain and data payload stored off chain.

3.7.2.4 Regulation and Audit Control

The use of blockchain-based technology can be beneficial for audit and regulation purposes because it is secure for storing information, while allowing reliable third-party verification. Our solution would help regulators relate the blockchain based automated reputation, and view the exact same information in the ledger, to that the supply chain participants claim. This means the reputation can be endorsed by the external third parties and can result in a control for supply chains.

Chapter 4

Proposed Design Methodology

This chapter describes the methodology of our proposed blockchain based trust management solution for gem supply chain. The design is explained in terms of general architecture, proposed trust mechanisms and consumer benefits. The proposed trust framework can assign the trust score to an asset based on its provenance, custody and quality information stored on blockchain. The framework also supports the reputation of supply chain participants in a permissioned blockchain. Supply chain specific transactions are formulated which help in finding instant and long term reputation scores for an asset and traders in the network. Lastly, we summarize how these mechanisms can benefit a end term consumer.

Before we discuss our proposed methodology for trust management in gem supply chains using blockchain, we present a top-level depiction of a gem supply chain given by Figure 4.1. This shall serve as a reference in our detailed discussion.

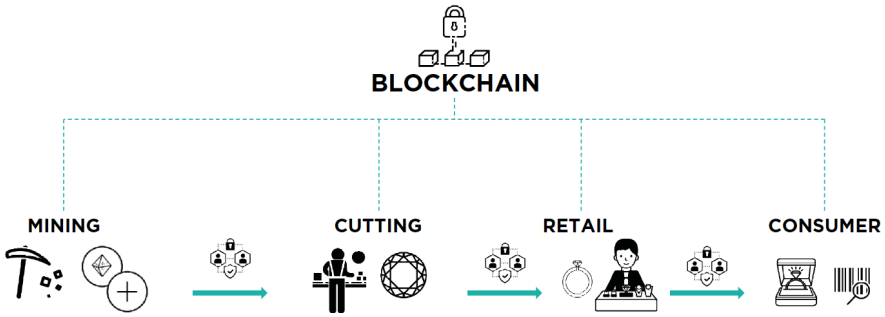

Figure 4.1: A typical gem supply chain [2]

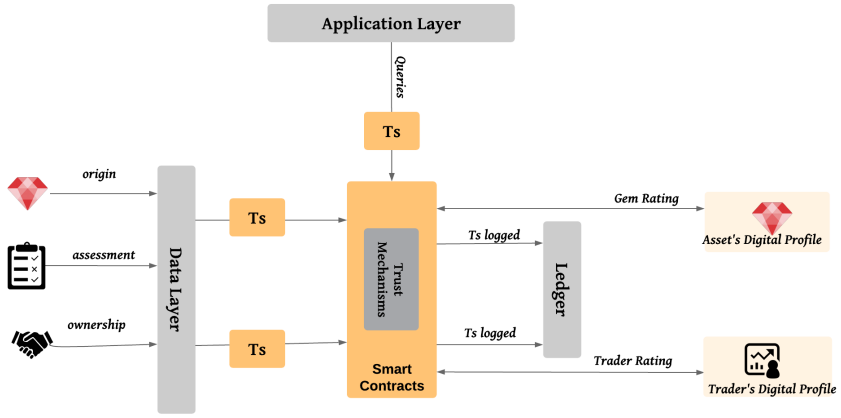

Figure 4.2: Architecture of Proposed Framework

4.1 Trust Framework over Blockchain

Blockchain proves that logged data has not been changed. This is supported by many blockchain based solutions as outlined in Chapter 3 which provide the traceability and integrity of the supply chain events. The main problem to address, common to all use cases, is proving the logged data is true. To rely on data, we need to trust the data source. In Chapter 3, we outlined the major challenges for digital supply chains with respect to trust management. In order to facilitate trust for gem supply chains, there are multiple data inputs constituting to the trust value of a gem stone at the shelf. The system's effectiveness also depends on the actors in blockchain and their stakes in honestly participating in the blockchain system. A generalized blockchain-based trust architecture is shown in Figure 4.2.

We introduce three key modules in a known architecture of blockchain solutions. A typical blockchain solution consists of three layers namely, the data, blockchain and the application layer. We describe functionality of each layer of the architecture.

- **Data Layer:** The data layer deals with the data generating interfaces in the gem supply chain, as shown in figure 4.2. The layer involves the actors and assets in the system namely the traders, Internet-of-Things (IoT) sensor devices, assets (gems) and third party assessors. All of these participants contribute to the data logged onto the blockchain layer. However, generally in gem supply chains, this data is observational rather than digital. To evaluate the data trust, we introduce two base modules, in coming sections 4.3 and 4.4, on data layer which quantify the trust of assets and traders with respect to an individual

event respectively.

- **Blockchain Layer:** Once the corresponding trust level is calculated for a particular event, it is logged on the blockchain in form of transactions, shown as Ts in figure 4.2, along with the other data related to that event. It is important to mention that the data can be stored in the databases off the chain and only the hash of data, with it's trust value can constitute a transaction. The transactions are formulated in accordance with the individual supply chain event and smart contracts automate the trust calculation and update digital profiles of either assets or the actors in supply chain system.

- **Application Layer:** Once we have immutable data on the blockchain and digital profiles, this data is provided to end users using application layer. Application layer interacts with the blockchain layer when it receives queries, in the form of transactions, from the end users. The cumulative trust level of assets and reputation of traders based on the history of transactions pertaining to them are calculated. Thus, the end user receives the information regarding the trust level of an asset based on data constituents and the long term reliability of the seller.

Before the detailed description of our trust management system, we first discuss our underlying network model in the next section.

4.1.1 Permissioned Blockchain Model

As stated in Chapter 1, permissioned blockchain model is best suited to supply chains and thus adopted by us as a design choice in this proposed work. Our architecture for blockchain network is based on work published by Malik et al. where the supply chain actors and IoT devices are pre-registered with the system since the participants are already known [64]. In permissioned blockchain model, the access policies for the network and rules are defined by the top-level consortium. This consortium manages the permissions of the blockchain network, the rewards and penalties for all the participants. Discussing the consortium in detail is out of the scope of our research. We assume that a consortium is in place that manages and reviews the network policies. A generalized diagram for better understanding of a consortium is provided in Figure 4.3.

As we can see, this consortium consists of two organisations ORG1 and ORG2 in permissioned blockchain network N. The peers P1, P2, P3 and P4, in both participating organisations, communicate through a channel C. The communication policy (CP) for this channel is devised jointly by Member

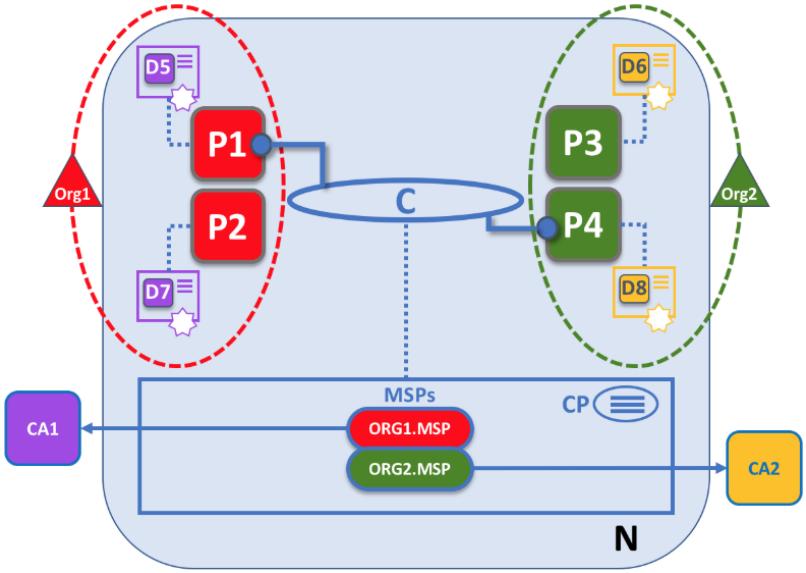

Figure 4.3: An example of a permissioned blockchain based consortium

Service Providers (MSPs) of both participating organisations. Each organisation can choose its own Certificate Authority (CA) that issues certificates to respective organisation. All the permissions and regulations in a permissioned blockchain are managed through a consensus on policy by all the participating organisation MSPs.

The coming sections describe the core network model, transaction flow and our methodology to quantify trust in the assets and traders of the gem supply chain.

4.2 Network Model

For traceability via sensor nodes, we assume an application agnostic tiered IoT network model presented by Wang et al. based on the location sensors and the gateway nodes [65]. We have opted for this model as it depicts a generic architecture for IoT devices assuming they have limited resources and are generally constrained. Based on this model, we propose a tiered network model consisting of IoT sensors, supply chain actors and blockchain validators. In Figure 4.1, we depict a typical gem supply chain from a miner to a retailer where mobility of these assets are supported by IoT devices. For our research work, Global Positioning System (GPS) sensors providing location data are used as IoT devices.

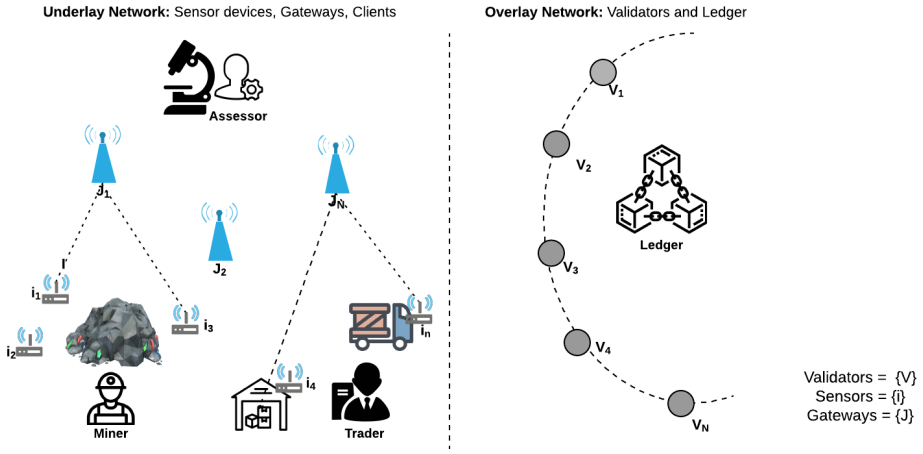

Figure 4.4: Network Model

4.2.1 Two-Tiered Design

A network model in our system consists of base nodes in a network which can contribute to the data on blockchain, as shown in Figure 4.4. These nodes include the participants of gem supply chain as well as the state-of-the-art IoT devices which supply chains today are equipped with. Our tiered model is split into two tiers - base tier and upper tier.

Base Tier: The base tier consists of sensors collecting the GPS information of the gem lots all the way through supply chain from the mining site up till retailers' shelf.

Upper Tier: The upper tier consists of gateway nodes which constitute to a node issuing sensor transactions to the blockchain layer.

The transaction issuing is limited to upper tier gateway nodes as generally the base tier sensor nodes are resource constrained to generate blockchain transactions. Also, the massive amount of information generated at the sensor level would increase the transaction send rate for the application of blockchain and raise scalability issues.

4.2.2 Network Flow

When the network is initialised, all the nodes, meant to generate transactions on the blockchain, get registered on the network using their public and private keys. The assets on the other hand are registered with a unique identifier. Both for the assets and nodes, digital profiles are created on blockchain platform which are used for storing the reputation scores discussed later in this chapter.

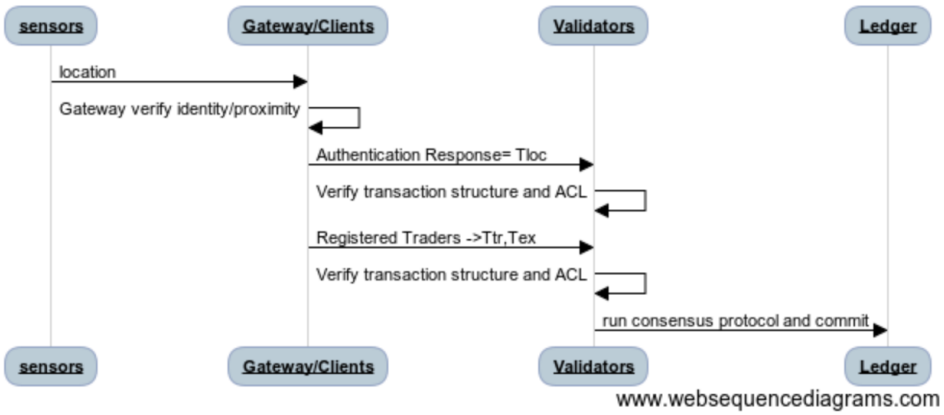

Figure 4.5: Network Flow

As the nodes get registered on the network, they can now issue transactions signed by their private keys. The sensors are recording the information through gateway nodes. The gateways verify sensor devices based on their identity and proximity. Apart from the the gateways, the supply chain actors are generating transactions by recording the asset trade on blockchain. These transactions then get validated from validators of the network according to the proposed transaction structure and access policies. The blockhain explorer nodes, interfacing with application layer, provide the information to end-users based on the queries and the access-level of end users generating the queries.

Having defined the trust architecture and the network model, the next sections focus in depth on how the trust is formulated for assets and the traders in this framework.

4.3 Trust Mechanisms for Assets

Recall from chapter 3 that where scientific methods of proving origin claims fail, methods like Proof of Origin and Proof of Custody have a great significance. We further include Proof of Assessment to establish another criteria. The three terms are described as:

Proof of Origin (PoO): Proof of origin is to establish the originating place and event of an individual gem in the supply chain. In our understanding PoO should constitute of Proof of Existence (PoE) and Proof of Location (PoL). PoE states that information regarding existence of a gem and related event must be available. PoL states that the information relating to physical trail of the gem from its origination to the retailers' shelf should be available.

Proof of Custody (PoC): Proof of Custody is to establish the chain of possession for an individual gem in the supply chain. PoC refers to the information of any change in possession of a gem between supply chain traders.

Proof of Assessment (PoA): Proof of Assessment is an important aspect to establish further trust in a gem in the supply chain. PoA refers to the information comprising assessment of a gem by an industry specific authority that is part of the blockchain network.

We are going to establish in our proposed trust model that PoP, PoC and PoA can be used to augment the trust associated with the gem stone and reputation of the participants trading in the gem industry. We build on the proposed work by Malik et al. [66] and extend it to gem supply chains.

4.3.1 Trust Model

As evident from above factors, the trust level of a gem stone constitutes from multiple observations. These observations are an instant referring to unique supply chain events as a gem is passed from one trader to another. These can be individual observations or they can be cumulative and contribute to a final trust value of gem on retailer's shelf. Cumulative trust value of a gem is derived from the factual trust worthy information that exists related to a gem stone. A gem stone which has a trust value supported by multiple factors, such as origin, its custody by traders and quality assessors; is most trust worthy for a consumer. Technically this information is constituted by the provenance of gem, its mobility from mine to different traders, and any physical quality assessments performed by a third party. A gem stone which has history of all the mentioned information stored on blockchain is considered to be the most trust worthy. Thus, trust in an asset can be modeled as:

$$Trust_{stone} = f(PoO, PoC, PoA) \tag{4.1}$$

where f is a function mapping trust in proof of asset's origin PoO, proof of asset's custody PoC, and proof of asset's assessment PoA. The function f is considered to be application specific with a value out of maximum of 1. However, for simplicity, lets assume a simple mapping of function f as the weighted sum of trust components (i.e. PoA, PoC, PoO) as:

$$Trust_{stone} = (x_1 \times PoO) + (x_2 \times PoC) + (x_3 \times PoA) \tag{4.2}$$

Where,

$$x_1 + x_2 + x_3 <= 1 \tag{4.3}$$

And,

$$PoO, PoC, PoA <= 1 \tag{4.4}$$

This mapping calculates the trust level of an asset where the weighting factors, x_1, x_2 and x_3 are decided by the consortium. For example, for a hand crafted jewellery, assessment value is of substantial significance. The PoA in this will be given the highest weight. Furthermore, in case of a fresh water pearl, origin information is most valuable. Thus, making PoO have the highest weight.

Control vs. Flexibility: There can be two approaches to evaluate trust in the stone which depend on the weight factors x1, x2 and x3. Each approach has its pros and cons. A more controlled approach is adapted as shown in equation 4.3. In this approach, the factors x1, x2 and x3 must be recommended or assigned by a single entity agreed upon by the consortium. Here, the three weight factors are explicitly dependent (change in one factor brings a must dependent change in the other two factors). A more flexible approach could have been to assign implicitly independent values for the three weight factors. Here, each factor could have a value of between 0 to 1 and each factor could be assigned by a different entity as agreed by the consortium. We opted for more control as a foul rating could be generated for a single proof our of PoO, PoC and PoA which could unnecessarily impact the true rating of the gem.

The trust levels from PoA, PoC and PoO are already stored instantaneously on asset's profile based on the supply chain events. The final trust value can be calculated on the consumer request or it can be automated with each trade. This can also be considered as a one time calculation and can be automated when a gem stone reaches the consumer shelf. In the next sections we explain in detail how the trust components PoO, PoC and PoA are computed in our model.

4.3.2 Proof of Origin

Gem supply chain process starts with the existence of a mined stone as shown in Figure 4.1. It is of critical importance as how to trust the claimed origin of gem when it is mined. Many blockchain based provenance solutions discussed in 3 depend on the transactions confirming the existence of raw material. Our solution for provenance stems from the fact that for a valuable gem, just the log of it's existence is not enough. To authenticate the origin of the gem, we rely on IoT sensors such as GPS locators to authenticate the origin and location information right from the mining point. Consequently, our proposed model depends on two things for provenance and establishing

Proof of Origin: i) Proof of Existence (PoE) ii) Proof of Location (PoL).

We have Proof of Origin as:

$$PoO = PoE + PoL \tag{4.5}$$

Where,

$$PoE, PoL = 0.5 \tag{4.6}$$

Proof of Existence (PoE): A ledger for a gem stone is instantiated with a transaction T_{ex}, submitted by a miner confirming the existence of a new asset on the blockchain. The structure of T_{ex} is given by:

$$T_{ex} = [GID|H_{gdata}|CID|Sig_m|PU_m] \tag{4.7}$$

where GID corresponds to the unique identifier assigned to a gem stone. H_{gdata} is the hash of data related to attributes of a gem stone (name, type, size, weight, location), CID is the identifier of respective smart contract (discussed in chapter 5). Sig_m and PU_m are miner's signature and the public key respectively.

Once a gem stone's existence is confirmed on blockchain through T_{ex}, we can now use this digital information to further relate to supply chain events confirming the trade of this gem as it makes it's way to the shelf.

Proof of Location (PoL): To prove the origin, trusting the location information of the gem in T_{ex} is not enough. To ensure that the geographic locations claimed in T_{ex} are factual, we introduce PoL based on GPS sensors. The data logged by the sensor devices is the location information of the gem i.e. latitude, longitude and the GPS sensor confidence value. The confidence value of the sensor device relates how much a sensor node is sure of its own observation and can be stored together with the GPS coordinates.

In order to further illustrate this, consider the Figure 4.4. We assume each mine has a set of GPS sensor nodes attached to the site and/or the vehicle transporting the assets to it's next location. These GPS sensors send location coordinates periodically pertaining to a specific asset or a lot of assets. This location information must be stored under the digital profile of an asset on the blockchain. However, the sensors reporting the location information are resource constrained and cannot directly host a blockchain client architecture for generating transactions to be stored on asset's profile. Secondly, the sensor information is generated on a massive scale in IoT, thus it is not in a best practice to log all the information on blockchain as it will increase the latency of the network.

To ensure efficiency, the sensor based transactions on the blockchain are logged by the gateway nodes instead. The intuition to use this data logging

is based on the model proposed by Brambilla et al. [67]. From Figure 4.4, every time a GPS location information is generated with respect to an asset, a request from a sensor device is generated to the gateway node. The GPS sensor nodes can communicate with the gateway nodes using any short range communication technology such as Zigbee or Bluetooth Smart. The sensors periodically send the location coordinates to the neighboring gateways in proximity. The location information is denoted by $Req_s i$, which is a request from sensor i to gateway j to generate a transaction information on blockchain. This request is given by:

$$Req_s i, j : \left\{ \begin{array}{c} GID \\ latitude, longitude \\ conf_i \\ Sig_i \\ PU_i \end{array} \right\}$$

where GID corresponds to the unique identifier assigned to the sensor. The respective location coordinates are given by $latitude, longitude$. The sensor's confidence is provided by $Conf_i$. Sig_i and PU_i are sensor's signature and the public key respectively.

Every gateway has a list of registered sensor devices within its proximity. Upon receiving a request from a sensor device, a gateway node which receives the request performs a validation before a transaction is logged on the blockchain. The validation is based on the following:

1. The request is generated from one of the registered sensor devices $i_0.....i_n$) in the underlay network.
2. It contains the valid signatures of the requesting device.
3. The request is generated for a valid asset, i.e. for this to be verified, T_{ex} must exist on the ledger for the corresponding GID.
4. An admissible geographic location with the gateway node is present, i.e. this is based on calculating the distance between the gateway and the sensor node, if in range the location information is considered to be valid.

After the verification, a response from gateway is generated as a transaction, T_{loc}, which is given by:

$$T_{loc} = [GID|H(Req_{i,j})|latitude, longitude|L_v|Sig_j|PU_j] \tag{4.8}$$

where GID is the gem stone's unique identifier, $H(Req_{i,j})$ is the hash of original request from the sensor, the respective location coordinates $latitude, longitude$,

the signature and public key of respective gateway node j and the location validity parameter L_v.

As we have discussed that confidence value attached to GPS sensor determines if the data generated by it is reliable. It is a fact that a GPS module may erroneously report the location information. The governing principle in calculation of L_v is based on the sensor's confidence $Conf_i$ and validity of its location data. The gateway node validates the location information with respect to the confidence level of the reported location. In our proposed solution, sensor's confidence $Conf_i$ is considered to be 1, if it exceeds a certain minimum acceptability threshold and 0 otherwise. The confidence thresholds are again dependent on sensor modalities and hence application specific.

In our proposed model, for every change in gem's location, location is valid and L_v is true (equals to 1) only when the sensor has admissible reported location with a high confidence level. The possible values of these are given below:

$$L_v = \begin{cases} \text{trusted}, & \text{high}Conf_i \text{ with location within proximity} \\ \text{not trusted}, & \text{low}Conf_i \text{ with location within proximity} \\ \text{not trusted}, & \text{high}Conf_i \text{ with location out of proximity} \\ \text{not trusted}, & \text{low}Conf_i \text{ with location out of proximity} \end{cases}$$

It is important to mention that the sensor information is often generated at a higher rate. This massive data from sensor devices can effect the blockchain's scalability if all the data is logged on the blockchain. This increases the transaction send rate and high latency. To keep the latency low, one of the design choices is to only log the information when the sensor information deviates from expected value. We already have L_v as the decision parameter for trusting sensor information. The gateway node sends T_{loc} ony when the information deviates from the previous stored value of L_v or after a specific period of time. In this way, we can increase the system scalability by limiting location transactions being massively stored on blockchain. The L_v parameter can also be used to determine if the sensors reporting the location deviated from the proximity range.

A PoO for a gem exists if it has corresponding T_{ex} and T_{loc} log. However, for a valid T_{loc} to have existed, L_v vector for that gem must contain all values as true, i.e. equal to 1.

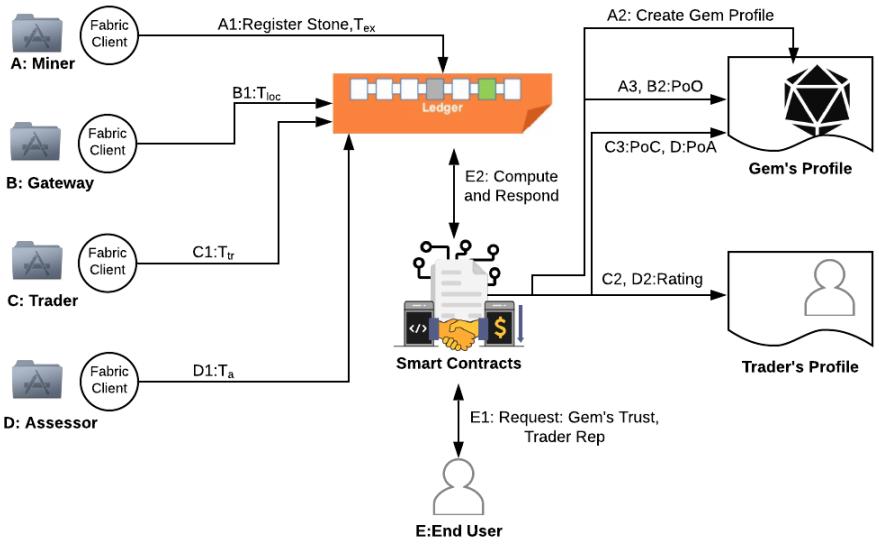

Figure 4.6: Transaction Data Flow

4.3.3 Proof of Custody

While *PoO* is sufficient to support provenance information, ownership history is another parameter for buyers and auditors in gem industry to be interested in. It is important as in conflict scenarios, an asset may be reported at the given location but in different ownership. Sometimes, an asset is of a greater value if it's reported to have remained in custody of fewer owners. Thus, this ownership history is referred to as Proof of Custody. This information is updated whenever the gem is traded. A transaction T_{tr}, confirming trade and change of ownership is given by:

$$T_{tr} = [GID|H_{gdata}|Sig_s|PU_s|Sig_b|PU_b] \tag{4.9}$$

where GID and H_{gdata} are same as in T_{ex}, and in place of miner who supposedly logs the data regarding mined gem, we have seller and buyer with their signatures and public keys as Sig_s, PU_s, Sig_b, and PU_b respectively.

A miner can also take a role of a trader and issue a T_{tr} confirming the trade of original gem stone. A PoC exists to be true (equals to 1), if a gem's digital profile contains T_{tr} and a corresponding rating is added to the profile.

4.3.4 Proof of Assessment

In gem and jewellery markets, physical assessment of stones is a known practice using isotopic, spectroscopic and geochemical methods [3]. These physical assessments are often to assess origin. For this, country of origin reports

are generated to support the claimed provenance. Other than geographic origin determination, research is also done in distinguishing the type of stone based on it's quality using various sampling methods. For example, in case of pearls, lab assessments are conducted to distinguish natural pearls from cultured pearls. Similar is the case for pearls from freshwater or saltwater. These reports however, hold a significance for the trader, consumer or even an investor.

The physical assessments of gems by a third party thus cannot be deprecated and is incorporated in the proposed blockchain solution. We propose that the assessment by the third-party is done for both, the gem in trade and the seller of the gem by evaluating his claim. Seller's assessment is discussed in the coming section 4.4. A new transaction T_a is generated which refers to the hash of data corresponding to assessment of the gem, i.e. a report signed by the lab. This transaction can be issued by a registered third party, such as laboratory. T_a is given by:

$$T_a = [GID|H_{data}|Sign_{auth}|PU_{auth}] \tag{4.10}$$

where GID is the identifier for gem, H_{data} is the hash for the laboratory assessment which could be a certificate or a report. $Sign_{auth}$ and Pk_{auth} are signatures and public key for the issuing authority.

A PoA exists to be true (equals to 1), if a gem's digital profile contains T_a and a corresponding rating is added to the gem's profile.

4.4 Trust Mechanisms for Traders

4.4.1 Motivation

As stated previously in 1, besides asset's own trust level, traders in the system must also be evaluated to encourage honest trade practices. As incentives for encouragement of fair trade, rewards and penalties are introduced by increasing or decreasing the reputation of a trader.

The trust of trader in supply chain stems from number of factors such as seller's reputation, buyer's willingness to continue business relationship, the satisfaction level of a buyer, the assessment of trading asset by a third party and much more. Reputation and trust are relative, and in our work we refer to the trader's reputation as a measure of trust. Generally, supply chain vendors supposedly would want to make long term investments with a trader of higher reputation to gain maximum profits. In gem industry specifically, it becomes of sheer importance. However, one may argue that in reality most of the factors contributing to trader's reputation are subjective with respect to

a buyer and thus hard to quantify in digital systems. We formulate trader's reputation to thwart this subjectivity from a buyer by introducing multiple factors for reputation formulation described in next sections.

4.4.2 Trade Event based Reputation

When a trader registers himself on the permissioned blockchain network, it is assigned an initial reputation score, R_0. The governing principle to update this score is based on the ratings given to a trader, at the point of sale trade T_{tr}, by the assessor $r_{a\to s}$ and the buyer $r_{b\to s}$. These ratings are instantiated with respect to T_{tr} and stored in trader's digital profile on the blockchain. The overall rating of a trader based on his sales is given by:

$$R_s = R_0 + \delta R \tag{4.11}$$

where R_0 is the base reputation score and δR is the reputation update factor which is given by:

$$\delta R = \frac{r_{a\to s} \cdot \lambda + r_{b\to s} \cdot C_b}{2} \tag{4.12}$$

where $r_{a\to s}$ is assessor's rating for the seller, λ is the weighted factor determining if seller's claim is proven, $r_{b\to s}$ is the buyer's rating for the seller, and C_b is referred as conflict measure. The reputation update factor δR is normalised between a range of 0 to 1.

We propose that while trading, the buyer rates the seller as the seller is the asset holder. The seller on the other hand raises a conflict if the trading experience was dis-satisfactory. C_b is the ratio of number of good sales of a buyer to the number of sales made by him. Good sales are where a conflict is not raised by the seller. Thus, we propose weighted rating of $r_{b\to s}$, which is directly proportional to buyers conflict measure, C_b i.e. if a buyer is known for conflicted sales, his rating for other sellers must be of lower weight while purchasing a new asset.

The second parameter in the seller's rating is the assessor's rating $r_{a\to s}$. The intuition to add this parameter stems from the real world practise in supply chain where a buyer often purchases an item based on it's assessment from a third party. The assessing third party approves or disapproves of seller for its claims based on the assessment. Even though, if a seller is dishonest of his claims (for which he must get a negative rating), the asset will be rated on the basis of it's quality. Thus, assessor generates ratings for (i) the asset, based on the quality as described in T_a (see Section 4.3.4), (ii) the seller, if

the assessment is supportive of the seller's claim about the asset. For the latter case, $r_{a \to s}$ is weighted by λ. If the assessment by the assessor supports the claim of the seller, λ is 1 and it is -1 otherwise.

4.4.3 Long Term Reputation

R_s is the seller's reputation at the time of one trade and added to his profile. However with the passage of time as the number of trades increase, an overall reputation score R is generated which reflects the seller's rating over his past sales. For calculating R, aggregation, median or other reputation mechanisms mentioned in Chapter 3 can be used. We calculate the overall score R of a seller at time t_k as:

$$R(t_k) = \sum_{t_i=t_0}^{t_k} R_s(t_i) \times e^{\frac{-(t_k - t_i)}{t_k}} \tag{4.13}$$

where t_0 to t_k represent the initial and the recent time of trades in history. R_s is weighted by a time decay function such as $e^{\frac{-(t_k - t_i)}{t_k}}$ to give more importance to the recent events in time.

Time Decay Function: Time decay function, also referred to as exponential decay function, depicts the decrease in value of an entity at a percentage rate consistent over time. The general representation of a decay function is given by e^{-wx}. It is a function which is opposite of exponential growth. The behaviour of time decay function with different decay constants is shown in Figure 4.7. It is evident that rate of decay increases when the function is applied with large decay constants, shown by the blue line.

A general decay function is represented as:

$$e^{-wx} \tag{4.14}$$

We have customized it with w = 1 and x as follows:

$$x = \frac{-(t_k - t_i)}{t_k} \tag{4.15}$$

The overall rating R is calculated on demand or after a specific interval to ensure that common trade transaction T_{tr} is less computationally expensive. The on-demand R is to be issued in a separate transaction and calculated by a dedicated smart contract on the blockchain.

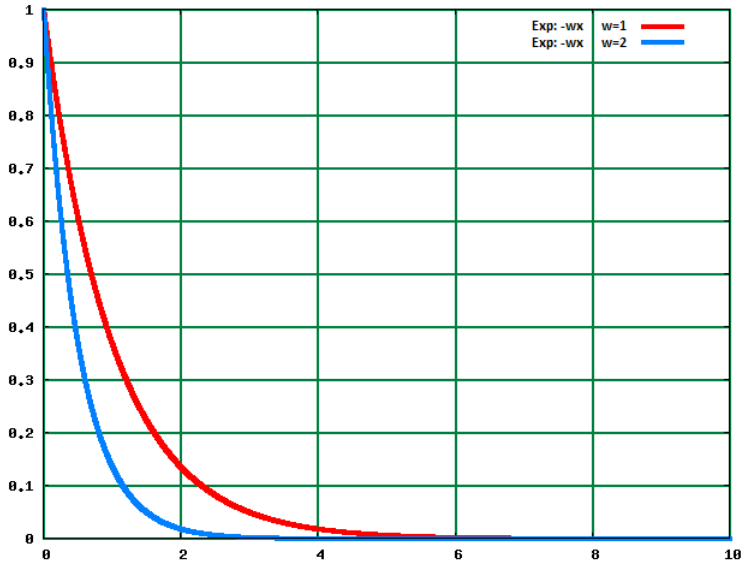

Figure 4.7: Time decay function with varying decay rates

Chapter 5

System Implementation

This chapter describes the implementation related details of our proposed Blockchain based framework. Implementation primarily comprises of an experimental setup depicting an abstract gem supply chain. Our experimental setup is described in context of related technologies that have been used in the blockchain implementation. Discussion covers the transaction flow with respect to the proposed model and Hyperledger framework. The blockchain architecture discussion includes the basic model, participants, access control, queries and transactions on the ledger. The transaction flow lists the systematic flow of transactions from clients with respect to both query and write transactions on the network. The third section in this chapter discusses how and which technologies have been used in context of our implementation, which include Hyperledger Fabric, Hyperledger Composer, Hyperledger Caliper, and Apache bench-marking tool.

5.1 Architecture of Blockchain Design

The architecture of our model relies on Hyperledger framework. The framweork provides Composer - a tool set that models and builds blockchain business network design, and integrate it to the network with other existing business systems. A model definition in Hyperledger Composer is based on:

- Model File (.cto): contains the data structure for user defined types, assets, transactions and participants of the system.
- Script File (.js): contains the functions of transactions which are later combined and hosted as contracts.
- Access Control List (.acl): contains the role based acccess of participants to write or query transactions from the ledger.

- Query File (.qry): contains the queries which the system will recognise.

5.1.1 Assets

The asset we have used in this implementation is of one type, i.e. gem. The asset properties contain the data related to it, its location information which is also in form of transactions, its trust score and the assessment and custody details. The custody, assessment and location parameters are dynamic and keep on updating in a Gem's profile as a result of corresponding transactions. A .cto model of gem is shown in Figure 5.1.

```
asset Gem identified by tradingSymbol {
  o String tradingSymbol
  o String description
  o String ProductType
  o Double quantity
  o location[] locations optional
  o DateTime receivedDateTime optional
  o ARating[] PoA optional
  o String[] PoC optional
  o Double [] Trust optional
  --> Trader owner
  --> Contract contract
}
```

Figure 5.1: Gem in .cto file

5.1.2 Participants

The participants in our model include trader, assessor and gateway. These participants are chosen as they are transaction contributors in our supply chain network model (see Figure 4.4). Every participant role has a unique identifier. The trader participant can take a role of miner, trader or both. The gateway has list of device Ids to identify the registered GPS sensor devices. A .cto model of a trader is shown in Figure 5.2.

```
participant Trader identified by tradeId {
  o String tradeId
  o String firstName
  o String lastName
  o Boolean revoke default = false
  o Integer[] reputation optional
  o Double min_trust optional
  o Integer[] rep_by_regulator optional
```

Figure 5.2: Trader in .cto file

5.1.3 Transactions

The transactions in our model include the three basic transactions namely, exist, trade and location. These transactions cover the seventy percent functionality of our model. The rest of the transactions are categorized under query transactions. The query transactions are also important as they control the readability access of the system and must be specified for accessibility specified in ACL. Figure 5.3 shows how T_{loc}s are embedded into a gem's profile upon commitment to the ledger. An example of transaction log on Hyperledger Historian is shown in Figure 5.4 which represents the transactions' type along with the date,time and issuer(not shown here) of the transactions.


```
{
  "$class": "org.example.trading.Gem",
  "tradingSymbol": "WGRP_R01",
  "description": " any description",
  "ProductType": " Diamonds",
  "quantity": 40,
  "locations": [
    {
      "$class": "org.example.trading.location",
      "latitude": 88.408,
      "longitude": 64.566,
      "Lv": true,
      "Req": "Officia.",
      "commodity": "resource:org.example.trading.Gem#WGRP_R01",
      "transactionId": "56de3503-9ffc-4f0f-972f-79e916555d0e",
      "timestamp": "2019-08-08T06:12:11.612Z"
    },
    {
      "$class": "org.example.trading.location",
      "latitude": 107.645,
      "longitude": 6.64,
      "Lv": true,
      "Req": "Consectetur.",
      "commodity": "resource:org.example.trading.Gem#WGRP_R01",
      "transactionId": "3cfde743-6075-4bb7-8620-47e1dce08fbc",
      "timestamp": "2019-08-08T06:13:04.919Z"
    },
    {
      "$class": "org.example.trading.location",
```


Figure 5.3: Location Transactions for a Gem

5.1.4 Access Control List

- Participants can read all the data in their records, which include their profile data and the transactions made.
- Participants are allowed to read their own history of transactions and restricted from viewing others' transactions on the network, see Figure 5.5.

Date, Time	Entry Type
2019-08-06, 15:03:11	location
2019-08-06, 11:01:09	Gexists
2019-08-05, 09:42:33	Trade

Figure 5.4: Transactions updating in Ledger (Hyperledger Composer)

- The assessors have a readability request to trader's transactions.
- Participants can submit only the transactions which they are allowed to: for example the T_{ex} transaction can only be submitted by a trader with a role of a miner.
- Participants are restricted from updating their own profile data.
- If a participant is revoked from participation, he is restricted from resetting/ or joining the network again.
- Participants with the miner role can edit/update certain information of the asset before it is traded.

```
rule R3_TradersSeeOwnHistoryOnly {
  description: "Traders should be able to see the history of their own transactions only"
  participant(t): "org.example.trading.Trader"
  operation: READ
  resource(v): "org.hyperledger.composer.system.HistorianRecord"
  condition: (v.participantInvoking.getIdentifier() != t.getIdentifier())
  action: DENY
}
rule R2_EnableTradeTxn {
    description: "Enable Traders to submit transactions"
    participant: "org.example.trading.Trader"
    operation: ALL
    resource: "org.example.trading.Trade"
    action: ALLOW
```

Figure 5.5: ACL Example from .acl

5.2 Transaction Flow

This section explains at what stage the transactions are verified and logged onto ledger and reputations/trust scores are updated. The supply chain

participants such as miners and traders enroll with the business organizations certification authority, which is a body hosting the blockchain solution. Note, as mentioned in Chapter 4, it is assumed that the participants are registered from a physical CA before being issued a digital identity or participation rights in permissioned blockchain network. Business model hosting our proposed trust management framework with a set of transactions, smart contracts and ACL are installed on endorsing peers. These endorsing peers validate the transactions and maintain the current state of the ledger.

The transaction flow of our model is shown in Figure 5.6. A client application is hosted on a device with a trader, mining site or vehicle. When a client node submits a transaction to the validators (see figure 4.4), the validators of the system endorse the transactions if:

- signatures of client are valid
- transaction is not submitted in past
- transaction follows the transaction architecture as described in the model .cto
- transaction does not voilate the ACL rules.

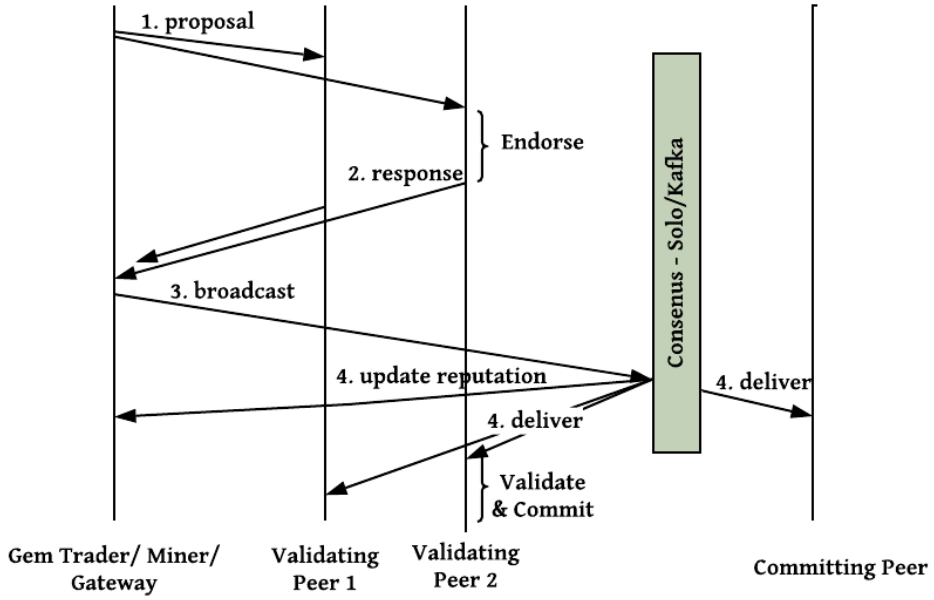

Figure 5.6: Transaction Flow

The validation response, either true or false is communicated back to the traders application (step 2 in figure 5.6. At this stage, the response is also

verified by the application for the validity of validators' signatures. These responses are then compared to reach on a consensus of a valid response. Note that the initial request could be either to write a supply chain event log at the ledger or it could be an application querying the ledger for some information. The response from the validators for the queries are considered complete here as they do not require something to be written in the ledger. For the write transactions; the (request, response) are then broadcast to the ordering service which manages the consensus mechanisms. The consensus here is drawn on ordering the verified transactions before they are committed to the ledger. Once the order is agreed, the transactions get delivered to the committing peer (another validator with this role) which records them on the ledger. The reputation and trust scores are also updated at this stage.

5.3 Experimental Setup and Related Technologies

5.3.1 Blockchain Model - Hyperledger Fabric and Hyperledger Composer

Our blockchain model was built using Hyperledger Fabric - an open source permissioned blockchain framework implementation. It was intended to developing applications over blockchain which could support a modular architecture. Also it allows users to choose the consensus mechanisms for permissioned blockchain to be simply pluggable. Smart contracts, which contain the logic of the blockchain application, are known as chaincode and deployed using container technology.

Fabric can work standalone using a command line in Linux. However, it is also supported by Hyperledger Composer as a pluggable run time which is created using docker containers that can host: peers of the system, the orderers and CAs.

The default state database we used for our system is goleveldb which is used for storing the ledger. Network configuration, i.e. such as number of peers and organisations, the type of consensus algorithm and etc was set to be 2 peer, 1 organization network. However, the consensus algorithm was varied between Solo or Kafka and the network model can be extended according to Figure 4.3.

5.3.2 Blockchain Server Hosting - AWS

AWS Elastic Cloud (EC2) service provides convenient use of cloud. This service has been used to host the blockchain provenance model on different servers. The servers replicated different regions storing information in parallel on blockchain to increase scalability.

5.3.3 Blockchain Application Testing - Apache Benchmark

The application level queries on Hyperledger fabric are usually run through explorer, using POST and GET requests. To automate and stress test the application level queries, we used Apache Benchmark Tool which is used for benchmarking and stress testing HTTP, Hypertext Transfer Protocol. Since the servers can receive the requests through REST APIs (GET and post requests), this tool was used to automate the query requests sent to the ledger.

5.3.4 Hyperledger Network Testing - Caliper

Hyperledger Caliper allows users to measure the performance of a specific blockchain implementation with a set of predefined use cases. The performance of our use case was tested using Hyperledger Caliper. It is a project of Hyperledger, and used as a benchmark tool for stress testing the network. When configured with the Hyperledger use case implementation, it can test the performance features based on the application or user's requirement. The tests can be conducted with the following benchmarks:

- TPS (Transactions Per Second)
- Transaction Latency
- Transaction Throughput
- Resource utilisation

We used the above benchmarks to test the performance of reputation based transactions. The performance was further compared with the baseline application model, i.e. a model without trust management.

Chapter 6

Security Evaluation and Results

This chapter first provides a qualitative security analysis of our proposed framework with respect to the known security attacks in context of reputation systems. It also discusses the system assumptions with respect to security and blockchain in built security features. The second section of this chapter outlines a brief discussion of the benchmarks i.e. transaction commitment time, query time, throughput, latency and resource consumption. The results are obtained using the tools described in chapter 5 for both the blockchain hosting Trust Management System (TMS) and without a TMS. Discussion related to the results is outlined in the subsequent sections.

6.1 Reputation based Attacks and Defence Mechanisms

Reputation systems ensure that the reputation metrics are a true reflection of system's participants and they are far from manipulation. This purpose of a reputation system is hard to achieve if the participants are able to improve their own reputation or lower the reputation of other participants, thus dishonest participants can benefit unwarrantedly and honest participants are disadvantaged. Malicious participants of the system mostly target the personal benefit or availability and accuracy of the system. In this section we discuss several security related attacks with respect to reputation systems and evaluate how resilient is our model to those attacks. With the reputation and trust management on blockchain, the choice of defence mechanisms is dependent on the design decisions. Apart from this, permissioned or public blockchain networks in built security measures can mitigate some of the

traditional reputation based attacks. For the rest of the other attacks, additional measures in design strategy are formulated to prevent those attacks i.e. by devising defensive or access control mechanisms.

We limit our scope of malicious participants to supply chain actors only and discuss the remaining section considering the following assumptions:

- The third party assessors and permissioned blockchain network (administrator and peers) are considered to be honest.
- Every physical node in supply chain is validated by CA before it is assigned a digital identity in permissioned blockchain.
- We assume the network is secured with state of art IDPS. The IoT sensors are protected from manipulation and permissioned blockchain nodes (administrator and peers) are considered to be honest, hence insider attacks are only limited to the supply chain traders and outsider attacks are excluded from the scope of discussion in this section.

6.1.1 Sybil Attack

A trader tries to increase his reputation by creating multiple identities, where each identity would be used to trade and relate the reputation score back to one trader.

Defence: Unlike public blockchains where participants can create multiple anonymous identities, permissioned blockchain only allow registered identities to take part in the network. Also, unlike Bitcoin blockchain where all communication is digital, the identities in our system are physically connected to supply chain events and are verified by a certification authority. Thus, it is impossible for a supply chain trader to keep creating aliases.

6.1.2 Whitewashing

The attacker tries to repair his reputation by exploiting some system vulnerability.

Application: if the reputation of a trader becomes low, he may reset the reputation to R_{min} by joining the network again.

Defence: As discussed for *Sybil Attacks*, a trader's registration is controlled via certification authority and blockchain network administrator. Thus, it is beyond the control of a trader to join or re-join the network(after revocation) without being approved by a third party.

6.1.3 Bad-mouthing

This is a very well known attack in context of reputation systems which aims to lower the reputation of another participant by giving a false rating.

Application: In our model, traders may individually or colluding with others want to lower a trader's reputation.

Defence: Reputation score of a trader is computed in a way that a trader gets a rating from assessing authority and a buyer. In case buyer's rating is dishonest, the seller has honest rating from assessing authority. Secondly buyer's stake of getting a positive conflict score maximizes, which prevents him from dishonestly rating the seller. Colluded bad-mouthing attacks however can be monitored on validators' end.

6.1.4 Ballot Stuffing

In this attack, a maliciously behaving trader creates fake trade transactions in order to increase the reputation of one's self.

Application: For this to be successful, a trader must be permitted to have done electronic trades with himself.

Defence: A trader is restricted to initiate a digital trade with himself, thus any transactions where the buyer is same as seller will be rejected at the validator's end.

6.1.5 Orchestrated Attacks

The afore-mentioned attacks deploy one strategy, however in orchestrated attacks, the attackers collude to launch a multifaced colluded attack. The attackers may change attack vectors, change identities in coalition, or simply keep varying their honest behavior over the time. These type of attacks normally target the system's formulation.

Application: One example of such attack could be where colluding attackers divide them into teams which oscillate between their behaviors i.e. honest and dishonest. This type of attack is known as oscillation attack as categorized by Hoffman et al. [68]. The honest team would try to launch attacks to increase his reputation by getting fake reputations from dishonest teams. Dishonest teams may falsely repute their colluded partners or slander the honest competitors.

Defence: For orchestrated attacks, the dishonest party continues to act dishonestly because it has no monetary stake except for losing a reputation score. First, it is important for CA or validation authority to issue identities based on the valid supply chain activity. Secondly, a base payment as a

stake can be stored against each registration which will be held by a smart contract and only be confiscated when a reputation score becomes lower than R_min. In this way, the above mentioned example of oscillation attack can be discouraged.

6.2 Results

6.2.1 Transaction Commitment Time

Transaction commitment time refers to the time taken by a transaction to be logged onto the ledger after it is first received from the client. In this section, we compare the transaction commitment time for the most common transactions of our system, i.e. T_{ex}, T_{loc} and T_{tr} with respect to the choice of different ordering mechanisms available in Hyperledger Fabric i.e. Solo and Kafka.

Figure 6.1: Transaction Commitment Time

6.2.1.1 Solo and Kafka Comparison

The ordering service impacts the transaction commitment time significantly. With Hyperledger Fabric, we have a choice of Solo and Kafka ordering service. Kafka is a fault tolerant orderer for a suggested usage in production, while Solo is a single node orderer with no fault tolerance recommended to be used for testing and development.

From figure 6.1, note that the transaction commitment time for all the transactions is higher than expected which is more than two seconds. This is due to the configuration *.yaml* file which has a default wait time of 2000 milli seconds before the transactions are actually committed. Overall, for

the comparison of orderers there is no significant different between the two except for Solo being more efficient in case of T_{tr}.

6.2.2 Query Time

Query time refers to the time taken for the blockchain to return the transaction IDs related to the query for a "trusted asset". Since there are three parameters constituting in the trust PoA, PoO and PoC; for the evaluation of our proposed system, these query benchmarks are classified into three types: (i) finding the chain of custody for these gems (ii) and finding the origin information, i.e. T_{ex} with respect to each recourse and (iii) finding if T_a i.e. PoA exists for an asset. Since finding the origin information is most expensive query, we monitor the query times for single and multi sourced gems.

6.2.2.1 Single-Sourced Gems

By single source we mean the Gems which do not go through a process of mixing or sorting thus there is a single T_{ex} corresponding to each asset.

To evaluate this, we stress the network with queries ranging from 1 to 150 and compare the query times with respect to two orderers in Hyperledger, Solo and Kafka. The results in Figure 6.2 show the comparative query times in milliseconds for both Solo and Kafka across different transactions. It is noted that on average, PoC takes longer than PoO and PoA. This is primarily due to more number of transactions in the ownership information whereas for PoO and PoA, we specifically have lesser or in some cases only one transaction.

6.2.2.2 Multi-Sourced Gems

In Chapter 4, we discussed a case of multi sourced gems where a gem may be mixed with other similar gems sourced not necessarily from the same origin. Since, the transactions confirming the original batch, T_{ex}, would be multiple and there would be a single transaction corresponding to mixing/sorting feature. This will in turn cause multiple nested queries when origin information is required and hence it is important how quick our system is able to generate PoO. Figure 6.3 shows the overall query time with respect to number of sources. It is evident that, with seven multi-resourced gems, the time to find the sources is only 1.5 secs, which is in acceptable ranges in real world.

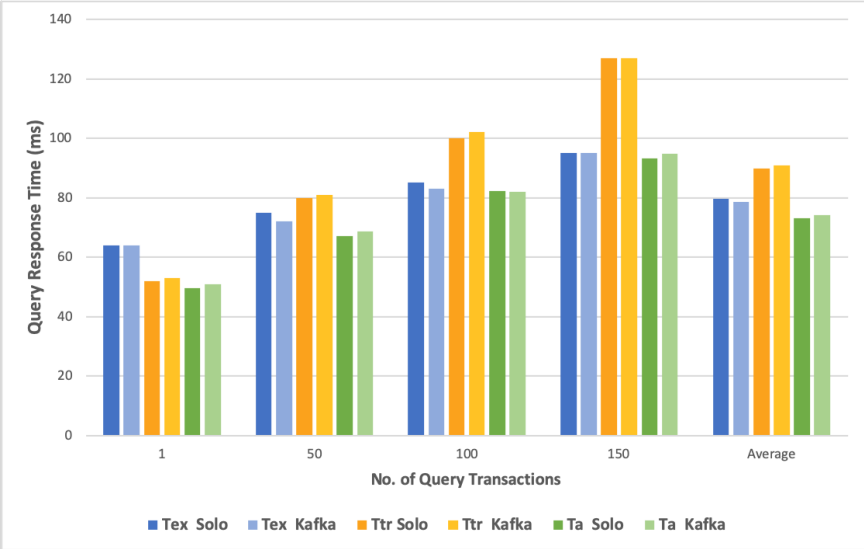

Figure 6.2: Query Times for Single-sourced Gems

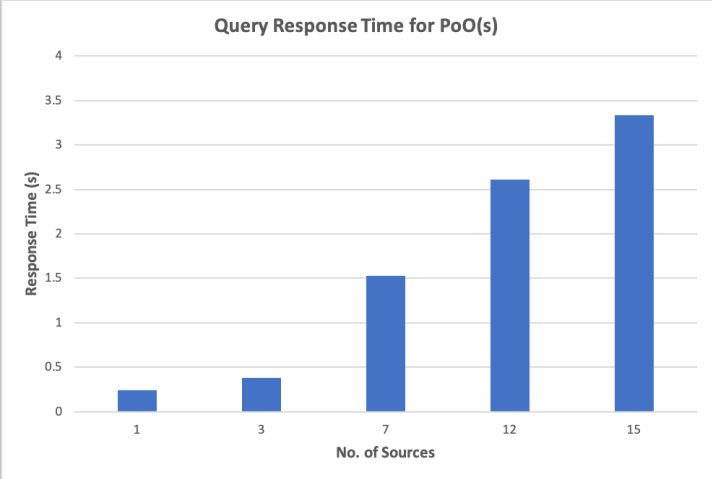

Figure 6.3: PoO Query Times for Multi-sourced Gems

6.2.3 Throughput and Latency

From the results pertaining to the transaction commitment time, we observe the T_{tr}, takes longer to commit due to TMS calculations being coupled with the trades in the system. Thus this transaction is further tested with throughput and latency of the system.

Latency is equivalent to network latency, i.e. the time it takes for a transaction to be written on ledger. The throughput on the other hand is the performance of the system with the rate at which the transactions are

received. These both parameters are interlinked; if the throughput of the system becomes low, the latency is higher. We compare the performance of T_{tr} with our Trust Management System(TMS) and compare it with baseline system without TMS.

6.2.3.1 Transactions with TMS

Table 6.1: Latency and Throughput with TMS

Test	Name	Succ	Fail	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	rep-network	1000	0	10.0 tps	0.94 s	0.14 s	0.34 s	10 tps
2	rep-network	1000	0	20.0 tps	4.16 s	0.12 s	0.85 s	20 tps
3	rep-network	1000	0	29.7 tps	7.17 s	0.23 s	3.70 s	27 tps
4	rep-network	1000	0	34.9 tps	3.60 s	0.43 s	2.20 s	33 tps
5	rep-network	1000	0	40.0 tps	5.41 s	0.24 s	2.80 s	36 tps
6	rep-network	1000	0	45.6 tps	15.68 s	0.56 s	8.49 s	36 tps
7	rep-network	1000	0	83.0 tps	24.14 s	1.38 s	19.05 s	36 tps
8	rep-network	1000	0	112.5 tps	24.76 s	2.01 s	18.28 s	35 tps
9	rep-network	1000	0	143.4 tps	28.04 s	3.98 s	21.47 s	34 tps
10	rep-network	1000	0	147.1 tps	27.29 s	3.35 s	20.99 s	35 tps
11	rep-network	1000	0	300.2 tps	30.98 s	3.33 s	26.20 s	32 tps
12	rep-network	1000	0	399.5 tps	31.11 s	14.50 s	27.28 s	31 tps
13	rep-network	1000	0	492.1 tps	32.52 s	13.02 s	28.45 s	30 tps

Table 6.1 shows the latency and throughput of the system with a trust management system. Note only trades are tested as here. It is noted that system depicted a very low average latency at start but later as the transaction send rate was increased from 10 tps to 500 tps, the latency was increased rapidly as an order of approximately 25 seconds for 10-500 transactions. The throughput on the other hand showed a stable behavior after the transaction send rate of 30.

6.2.3.2 Transactions without TMS

From table 6.2, the results are drawn for a system which is not maintaining reputation and trust scores for gems and participants. The trend for the increase in latency is quite similar to that of the system with trust manage-

ment. However, it can be noted that the increase in latency is after 50 tps whereas for the system with TPS, the latency is higher right after 30 tps.

Table 6.2: Latency and Throughput without TMS

Test	Name	Succ	Fail	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	rep-network	1000	0	10.0 tps	0.96 s	0.12 s	0.35 s	10 tps
2	rep-network	1000	0	20.0 tps	0.79 s	0.10 s	0.32 s	20 tps
3	rep-network	1000	0	30.0 tps	0.48 s	0.12 s	0.29 s	30 tps
4	rep-network	1000	0	35.0 tps	0.95 s	0.14 s	0.38 s	34 tps
5	rep-network	1000	0	40.0 tps	2.03 s	0.25 s	1.10 s	38 tps
6	rep-network	1000	0	45.0 tps	11.40 s	0.47 s	5.54 s	38 tps
7	rep-network	1000	0	72.7 tps	20.70 s	1.09 s	14.53 s	39 tps
8	rep-network	1000	0	143.2 tps	23.91 s	1.32 s	15.67 s	37 tps
9	rep-network	1000	0	181.6 tps	25.61 s	2.10 s	19.60 s	37 tps
10	rep-network	1000	0	150.4 tps	25.10 s	6.65 s	19.10 s	37 tps
11	rep-network	1000	0	292.3 tps	30.21 s	14.56 s	25.51 s	33 tps
12	rep-network	1000	0	386.7 tps	29.39 s	2.61 s	24.92 s	34 tps
13	rep-network	1000	0	475.7 tps	32.52 s	14.49 s	27.97 s	31 tps

6.2.4 Resource Consumption

Resource consumption in the system refers to the memory, CPU usage and the process memory consumption i.e. either a write or read operation on the ledger. The resource consumption details which resources in the system can get overloaded given the increase in transaction rate and the proposed model which hosts a TMS. Similar to throughput and latency calculations, we draw results based on a system model without TMS and with TMS.

Table 6.3 shows the resource consumption of the proposed model and Table 6.4. As it was a single peer, and two organization network that was tested for caliper, we can observe that the maximum resource consumption is on the validators end , i.e. peers of organisation 1 and 2. The second resource constrained device is Docker which is hosting the fabric container itself. The expected comparison noted is the disk-write i.e. transactions committed to the ledger taking the space of 19.5 MB in case of peers of TMS and 18MB in case of a system without trust management. However it will be interesting to note the distribution of resource consumption among peers when the configuration hosts more than one peer.

Table 6.3: Resource Consumption with TMS

TYPE	NAME	Memory(max)	Memory(avg)	CPU(max)	CPU(avg)	Traffic In	Traffic Out	Disc Read	Disc Write
Process	node local-client.js(avg)	132.6MB	127.9MB	53.06%	32.86%	-	-	-	-
Docker	dev-peer0.org2.example.co...oy.58	119.3MB	112.1MB	97.56%	33.03%	21.5MB	19.0MB	0B	0B
Docker	dev-peer0.org1.example.co...oy.58	119.9MB	113.5MB	95.03%	32.69%	21.5MB	19.0MB	0B	0B
Docker	peer0.org2.example.com	285.6MB	277.8MB	38.51%	26.07%	30.6MB	72.4MB	0B	19.4MB
Docker	peer0.org1.example.com	272.5MB	265.2MB	38.46%	26.08%	30.5MB	72.3MB	0B	19.4MB
Docker	orderer.example.com	36.7MB	31.3MB	6.02%	3.86%	9.5MB	18.9MB	0B	11.3MB
Docker	ca.org1.example.com	6.5MB	6.5MB	0.14%	0.00%	2.9KB	0B	0B	0B
Docker	ca.org2.example.com	6.4MB	6.4MB	0.00%	0.00%	2.9KB	0B	0B	0B

Table 6.4: Resource Consumption without TMS

TYPE	NAME	Memory(max)	Memory(avg)	CPU(max)	CPU(avg)	Traffic In	Traffic Out	Disc Read	Disc Write
Process	node local-client.js(avg)	138.8MB	132.8MB	46.53%	34.37%	-	-	-	-
Docker	dev-peer0.org2.example.co...oy.58	110.4MB	108.8MB	92.49%	29.63%	17.0MB	15.3MB	0B	0B
Docker	dev-peer0.org1.example.co...oy.58	113.5MB	111.2MB	88.09%	29.40%	17.0MB	15.3MB	0B	0B
Docker	peer0.org1.example.com	297.6MB	290.1MB	34.15%	26.89%	25.8MB	63.8MB	0B	18.1MB
Docker	peer0.org2.example.com	302.9MB	294.9MB	35.40%	26.77%	25.8MB	64.1MB	0B	18.1MB
Docker	ca.org2.example.com	6.5MB	6.5MB	0.00%	0.00%	3.5KB	0B	0B	0B
Docker	ca.org1.example.com	6.4MB	6.4MB	0.00%	0.00%	3.6KB	42B	0B	0B
Docker	orderer.example.com	30.3MB	25.6MB	6.60%	4.48%	8.8MB	17.4MB	0B	10.5MB

Chapter 7

Conclusion and Future Work

This chapter describes the synopsis of our thesis work, research findings, conclusion, and future work directions.

In this work, we have proposed a trust framework for providing end to end trust in gem supply chains. Our solution can be adopted for other various supply chain use cases such as food, manufacturing, pharma supply chain. We formulate asset's and traders' credibility based on whether the data contributed by them is trust worthy.

The trust of an asset stems from proof of location, proof of custody and proof of assessment, a multi source data model. We also evaluate the credibility of sensor information while determining the proof of location. Moreover, the assessments from a physical third party, a factor on which various supply chain applications depend upon is also reflected in our system while calculating the reputation of traders and trust for a gem stone. The overall trust model for gem stone is the weighted sum of the proofs where the weights can adjusted according to the requirements of the end user. The reputation model for traders on the other hand, is event based as well as long term; where reputation is obtained via time evolving function.

The proposed model was implemented using Hyperledger Fabric, a permissioned blockchain framework. The performance analysis was benchmarked against latency, throughput, resource consumption and query times. The system was stress tested with various transaction rates to monitor the latency and and throughput. The overhead caused for trust framework was quite less when compared to the baseline system to an order of few transactions per second. However, it will be interesting to note the effect of increasing organisations and peers on these parameters with varying orderer services.

The query time was also monitored for finding origin for single and multi

sourced gems. The results showed that the query time for finding multiple sourced gems was in acceptable range(for 7 sources, 1.5 seconds).

7.1 Future Work

Our proposed framework could be further extended in three domains:

- The trusted assets i.e. having a high data credibility will should be of higher price in worth. A questionable gem on the other hand should be of lower price if does not provide a high trust element. Thus a fair pricing model can be built along with TMS.
- Monetising the traders' incentives and penalties can bring a great weight to TMS. Also monetary stakes can prevent the traders from behaving maliciously.
- The regulation and audit with TMS is yet to be explored, and holds a potential for further insight. In this regard, traders can also be monitored for their expected behavior using machine learning given their transactions and trust score in past.

Bibliography

[1] I. Bashir, *Mastering blockchain.* Packt Publishing Ltd, 2017.

[2] (2019) Facette magazine. [Online]. Available: https://www.ssef.ch/wp-content/uploads/2019/02/facette-2019.pdf

[3] L. E. Cartier, S. H. Ali, and M. S. Krzemnicki, "Blockchain, chain of custody and trace elements: An overview of tracking and traceability opportunities in the gem industry." *Journal of Gemmology*, vol. 36, no. 3, 2018.

[4] F. Schwägele, "Traceability from a european perspective," *Meat science*, vol. 71, no. 1, pp. 164–173, 2005.

[5] T. D. Price and J. H. Burton, "Provenience and provenance," in *An Introduction to Archaeological Chemistry.* Springer, 2011, pp. 213–242.

[6] E. M. Whitener, S. E. Brodt, M. A. Korsgaard, and J. M. Werner, "Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior," *Academy of management review*, vol. 23, no. 3, pp. 513–530, 1998.

[7] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] B. J. La Londe and J. M. Masters, "Emerging logistics strategies: blueprints for the next century," *International journal of physical distribution & logistics management*, vol. 24, no. 7, pp. 35–47, 1994.

[9] D. M. Lambert, M. C. Cooper, and J. D. Pagh, "Supply chain management: implementation issues and research opportunities," *The international journal of logistics management*, vol. 9, no. 2, pp. 1–20, 1998.

[10] M. Christopher, *Logistics and supply chain management.* Irwin Professional Publishing, 1992.

[11] S. K. Hacker, J. T. Israel, and L. Couturier, "Building trust in key customer-supplier relationships," *The performance center and satisfaction strategies*, 1999.

[12] B. Welty and I. Becerra-Fernandez, "Managing trust and commitment in collaborative supply chain relationships," *Communications of the ACM*, vol. 44, no. 6, pp. 67–73, 2001.

[13] M. Zineldin and P. Jonsson, "An examination of the main factors affecting trust/commitment in supplier-dealer relationships: an empirical study of the swedish wood industry," *The TQM magazine*, vol. 12, no. 4, pp. 245–266, 2000.

[14] B. S. Sahay, "Understanding trust in supply chain relationships," *Industrial Management & Data Systems*, vol. 103, no. 8, pp. 553–563, 2003.

[15] B. Sahay and A. Maini, "Supply chain: a shift from transactional to collaborative partnership," *Decision*, vol. 29, no. 2, pp. 67–88, 2002.

[16] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review*, vol. 20, no. 3, pp. 709–734, 1995.

[17] V. R. Kannan and K. Choon Tan, "Buyer-supplier relationships: The impact of supplier selection and buyer-supplier engagement on relationship and firm performance," *International Journal of Physical Distribution & Logistics Management*, vol. 36, no. 10, pp. 755–775, 2006.

[18] C. Chandra and S. Kumar, "Enterprise architectural framework for supply-chain integration," *Industrial Management & Data Systems*, vol. 101, no. 6, pp. 290–304, 2001.

[19] L. Duranti and C. Rogers, "Trust in digital records: An increasingly cloudy legal area," *Computer Law & Security Review*, vol. 28, no. 5, pp. 522–531, 2012.

[20] L. Duranti and P. C. Franks, *Encyclopedia of archival science*. Rowman & Littlefield, 2015.

[21] V. L. Lemieux, "Trusting records: is blockchain technology the answer?" *Records Management Journal*, vol. 26, no. 2, pp. 110–139, 2016.

[22] Y. Wang and J. Vassileva, "A review on trust and reputation for web service selection," in *27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)*. IEEE, 2007, pp. 25–25.

[23] M. del Castillo, "Walmart, kroger & nestle team with ibm blockchain to fight food poisoning," *Online verfügbar unter https://www.coindesk.com/walmart-kroger-nestleteam-with-ibm-blockchain-tofight-food-poisoning*, 2017.

[24] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, 2016, p. 4.

[25] (2015) Block verify, [online]. [Online]. Available: http://www.blockverify.io/

[26] (2017) Provenance:every product has a story. [Online]. Available: https://www.provenance.org/

[27] F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology," in *2016 13th international conference on service systems and service management (ICSSSM)*. IEEE, 2016, pp. 1–6.

[28] ——, "A supply chain traceability system for food safety based on haccp, blockchain & internet of things," in *2017 International Conference on Service Systems and Service Management*. IEEE, 2017, pp. 1–6.

[29] K. Biswas, V. Muthukkumarasamy, and W. L. Tan, "Blockchain based wine supply chain traceability system," in *Future technologies conference*, 2017, pp. 1–7.

[30] (2015) Future of fish. making sense of wild seafood supply chains. a report created for the nature conservancy. [Online]. Available: http://futureoffish.org/sites/default/files/docs/resources/TNC.SeafoodSupplyChainReport.V10.Web_.pdf

[31] 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*, vol. 5, pp. 17 465–17 477, 2017.

[32] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," 2016.

[33] (2018) A blockchain enabled track and trace technology solution for medical product supply chains. [Online]. Available: https://modum.io/system/

[34] (2007) World health organization. anti-counterfeit technologies for the protection of medicines. [Online]. Available: http://www.fip.org/impactglobalforum/pdf/backgroundinfo/IMPACT%20-%20AC%20Technologies%20v2.pdf

[35] (2018) Tcodex protocol. a decentralized title registry and cryptocurrency for the arts & collectibles market, whitepaper. [Online]. Available: https://www.codexprotocol.com/

[36] S. Walker, "Diamond miners respond," *Engineering and Mining Journal*, vol. 218, no. 9, pp. 58–66, 2017.

[37] J.-L. Archuleta, "The color of responsibility: Ethical issues and solutions in colored gemstones." *Gems & Gemology*, vol. 52, no. 2, 2016.

[38] (2018) Cibjo sets up industry-wide working committee to formulate responsible sourcing guidance for gem and jewellery sectors. cibjothe world jewellery confederation, milan, italy, 8 may. [Online]. Available: www.cibjo.org/cibjo-sets-up-industry-wide-workingcommittee-to-formulate-responsible-sourcing-guidancefor-gem-and-jewellery-sectors

[39] (2018) The hidden cost of jewelry:human rights in supply chains and the responsibility of jewelry companies. human rights watch, new york, new york, usa, 99 pp. [Online]. Available: www.hrw.org/sites/default/files/report_pdf/jewellery0218_web_0.pdf.

[40] J. Nash, C. Ginger, and L. Cartier, "The sustainable luxury contradiction: Evidence from a consumer study of marine-cultured pearl jewellery," *Journal of Corporate Citizenship*, no. 63, pp. 73–95, 2016.

[41] M. De Angelis, F. Adıgüzel, and C. Amatulli, "The role of design similarity in consumers evaluation of new green products: An investigation of luxury fashion brands," *Journal of cleaner production*, vol. 141, pp. 1515–1527, 2017.

[42] (2018) Jade: Myanmars big state secret. global witness, london. [Online]. Available: www.globalwitness.org/en/campaigns/oil-gas-and-mining/myanmarjade

[43] (2018) Challenges to advancing environmental and social responsibility in the coloured gems industry. [Online]. Available: ResponsibleEcosystemsSourcingPlatform,Geneva,Switzerland,44pp

[44] C. Dalpé, P. Hudon, D. J. Ballantyne, D. Williams, and D. Marcotte, "Trace element analysis of rough diamond by la-icp-ms: a case of source discrimination?" *Journal of forensic sciences*, vol. 55, no. 6, pp. 1443–1456, 2010.

[45] H. A. Hänni and L. E. Cartier, "Tracing cultured pearls from farm to consumer: A review of potential methods and solutions," *Journal of Gemmology*, vol. 33, no. 7, pp. 239–245, 2013.

[46] T. Norton, J. Beier, L. Shields, A. Househam, E. Bombis, and D. Liew, "A guide to traceability: A practical approach to advance sustainability in global supply chains," *United Nations Global Compact Office: New York, NY, USA*, 2014.

[47] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.

[48] D. Shrier, W. Wu, and A. Pentland, "Blockchain & infrastructure (identity, data security)," *Massachusetts Institute of Technology-Connection Science*, vol. 1, no. 3, pp. 1–19, 2016.

[49] O. Petersen and F. Jansson, "Blockchain technology in supply chain traceability systems," 2017.

[50] (2017) Singapore diamond investment exchange (sdix) partners with kynetix and everledger to trial first-ever blockchain verification and record-keeping service for diamond trading. [Online]. Available: www.sdix.sg/singapore-diamondinvestment-exchange-sdix-partners-kynetix-everledgertrial-first-ever-blockchain-verification-record-keepingservice-diamond-trading,accessed

[51] (2018) Jewelry companies team up with ibm on blockchain platform. [Online]. Available: www.reuters.com/article/us-blockchain-diamonds/jewelry-companies-team-up-with-ibm-on-blockchainplatform-idUSKBN1HX1BD

[52] (2018) Why the art world is looking to blockchain for tracking and provenance. medium, 11 may. [Online]. Available: https://medium.com/ethereum-art-collective/why-the-art-world-is-looking-to-blockchain-for-trackingand-provenance-f7329618f6f7

[53] (2018) Gbelin working to create blockchain for colored stones. [Online]. Available: www.nationaljeweler.com/diamonds-gems/social-issues/6197-guebelin-working-to-create-blockchain-for-coloredstones

[54] R. Global *et al.*, "Blockchain for traceability in minerals and metals supply chains: Opportunities and challenges," 2017.

[55] L. Meraviglia, "Technology and counterfeiting in the fashion industry: Friends or foes?" *Business Horizons*, vol. 61, no. 3, pp. 467–475, 2018.

[56] (2016) Kimberley process: Mid-term report. [Online]. Available: www.kimberleyprocess.com/en/system/files/documents/kimberley_process_mid-term_report.pdf

[57] (2018) Everledger announces the industry diamond time-lapse protocol. [Online]. Available: www.idexonline.com/FullArticle?Id=43757

[58] (2018) De beers to pilot digital programme in sierra leone to sell ethically sourced diamonds. [Online]. Available: https://www.ft.com/content/8ff2414c-43d6-11e8-93cf-67ac3a6482fd

[59] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft, "Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application," *Applied Energy*, vol. 209, pp. 8–19, 2018.

[60] Z. Yang, K. Zheng, K. Yang, and V. C. 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)*. IEEE, 2017, pp. 1–5.

[61] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2016, pp. 398–411.

[62] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," *arXiv preprint arXiv:1706.01730*, 2017.

[63] (2018) Ibm crypto anchors. [Online]. Available: https://www.research.ibm.com/5-in-5/crypto-anchors-and-blockchain/

[64] S. Malik, S. S. Kanhere, and R. Jurdak, "Productchain: Scalable blockchain framework to support provenance in supply chains," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*. IEEE, 2018, pp. 1–10.

[65] W. Wang, K. Lee, D. Murray, and J. Guo, "Discovering objects and services in context-aware iot environments," *International Journal of Services Technology and Management*, vol. 25, no. 3-4, pp. 326–347, 2019.

[66] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and iot supported supply chains," *arXiv preprint arXiv:1906.01831*, 2019.

[67] G. Brambilla, M. Amoretti, and F. Zanichelli, "Using blockchain for peer-to-peer proof-of-location," *arXiv preprint arXiv:1607.00174*, 2016.

[68] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys (CSUR)*, vol. 42, no. 1, p. 1, 2009.