

Håkon Pelsholen Busterud  
Sigurd Eilerås

# What makes Users Trust Security and Privacy of a Blockchain-Based Supply Chain System?

Master's thesis in Computer Science, Databases and Search

Supervisor: Jingyue Li

Co-supervisor: Jakob Notland

January 2022



Håkon Pelsholen Busterud  
Sigurd Eilerås

# **What makes Users Trust Security and Privacy of a Blockchain-Based Supply Chain System?**

Master's thesis in Computer Science, Databases and Search  
Supervisor: Jingyue Li  
Co-supervisor: Jakob Notland  
January 2022

Norwegian University of Science and Technology  
Faculty of Information Technology and Electrical Engineering  
Department of Computer Science



# Abstract

Blockchain systems have gained increased interest over the past few years, and several new fields of use, such as supply chain systems, are being researched. Since blockchain is still a new technology with clear limitations, various papers have explored how it can be altered and improved upon in order to support use cases outside of the limited scope of digital currencies. Supply chain systems not only require a solid technological framework, but also perceived trust amongst users. Using established technologies and interviews, this study aimed to produce a blockchain system for the purposes of ensuring trust and privacy amongst consumers and producers in supply chain systems. This study covers the aspects that determine whether the user believes their best interests are maintained and their data is protected in blockchain systems.

The system model and implementation draw heavily on existing cryptographic methods and literature of privacy and security in blockchain systems. Storing raw data on the blockchain itself in supply chains can be a potential privacy issue, so this solution uses an off-chain database for data storage, only storing its corresponding hash value on the blockchain to assure data integrity. Additionally, the system uses zkSNARKs in order to create unlinkable tokens for signing transactions. This is in attempt to further ensure privacy of the data producers sharing their data in supply chain systems, by effectively making the data input anonymous. The implemented modules and components can be applied to a variety of blockchain systems, however this would require modification to the underlying blockchain components. That said the implementation has potential to be more generalized.

Users in technical systems are not only concerned with the technical aspects of privacy, but also the perceived security and privacy of systems. This study has, based on a set of user interviews, built upon existing theory and formulated theory as to what makes a user trust the data presented to them in a system and trust that their privacy is maintained. The research process concludes that users want access to as much information and data regarding a system as can be provided. However, they also prefer data which is presented in a simpler, more conceptual manner, compared to technical details. Users notably also seem to respond more positively to explanations which stress the properties of a system, rather than the more technical aspects. The results also show trust increases with increasing transparency into the system as long as the information is presented in a way that is approachable to the users.

# Sammendrag

Blokkjedesystemer har sett økt interesse de siste årene, og flere nye bruksområder, som forsyningskjedesystemer, forskes på. Siden blokkjeder fortsatt er en ny teknologi med klare begrensninger, har ulike artikler utforsket hvordan de kan modifiseres og forbedres for å støtte brukstilfeller utenfor det begrensede omfanget av digitale valutaer. Forsyningskjedesystemer krever ikke bare et solid teknologisk rammeverk, men også opplevd tillit blant brukerne. Ved bruk av etablerte teknologier og intervjuer hadde denne studien som mål å produsere et blokkjedesystem med det formål å sikre tillit og personvern blant forbrukere og produsenter i forsyningskjedesystemer. Denne studien dekker aspektene som avgjør om brukeren opplever at deres interesser ivaretas og deres data er beskyttet i blokkjedesystemer.

Systemmodellen og implementeringen bygger i stor grad på eksisterende kryptografiske metoder og litteratur om personvern og sikkerhet i blokkjedesystemer. Lagring av rådata på selve blokkjeden i forsyningskjeder kan være et potensielt personvernproblem, så denne løsningen lagrer dataene i en ekstern database i stedet for blokkjeden, og lagrer bare dens tilsvarende hash-verdi på blokkjeden for å sikre dataintegritet. I tillegg bruker systemet zkSNARK-er for å lage ulinkbare transaksjoner. Dette gjøres for å ytterligere sikre personvernet til dataprodusentene som deler dataene sine i forsyningskjedesystemer, ved å effektivt anonymisere dataene. De implementerte modulene og komponentene kan brukes sammen med en rekke blokkjedesystemer, men dette vil kreve modifikasjon av de underliggende blokkjedekomponentene. Når det er sagt, har implementeringen potensial til å bli mer generalisert.

Brukere i tekniske systemer er ikke bare opptatt av de tekniske aspektene ved personvern, men også den opplevde sikkerheten og personvernet til systemene. Denne studien har, basert på et sett med brukerintervjuer, bygget på eksisterende teori og formulert teori om hva som gjør at en bruker stoler på dataene som presenteres for dem i et slikt system og at deres personvern blir ivaretatt. Forskningsprosessen konkluderer med at brukere ønsker tilgang til så mye informasjon og data om et system som kan gis. Imidlertid foretrekker de også data som presenteres på en enklere, mer konseptuell måte sammenlignet med en forklaring med fokus på tekniske detaljer. Brukere ser også ut til å respondere mer positivt på forklaringer som understreker egenskapene til et system, snarere enn de mer tekniske aspektene. Resultatene viser også at tilliten øker med økende åpenhet inn i systemet, gitt at informasjonen presenteres på en måte som er tilgjengelig for brukerne.

# Preface

We would like to thank our supervisor, Jingyue Li, for his considerable help in designing this research and crystallizing the novelty of this thesis. We would also like to thank Jakob Notland who co-supervised this thesis, we received great advice related to blockchain from him. All the participants in the interviews also have our gratitude, without their contribution we would not have been able to conduct this study.

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Research Motivation . . . . .	1
1.2	Research Goals . . . . .	2
1.3	Research Questions . . . . .	3
1.4	Contribution . . . . .	4
1.5	Outline . . . . .	4
<b>2</b>	<b>Background</b>	<b>5</b>
2.1	Sociological Trust to Digital Trust . . . . .	5
2.1.1	Conceptual model of Trust . . . . .	6
2.2	Data Security and Privacy . . . . .	7
2.3	Cryptographic hash functions . . . . .	8
2.3.1	Secure Hash Algorithm . . . . .	9
2.4	Elliptic Curve Cryptography . . . . .	10
2.4.1	EdDSA . . . . .	10
2.5	Blockchain . . . . .	11
2.5.1	Blockchain Building Blocks . . . . .	12
2.5.2	Types of Blockchain Networks . . . . .	13
2.5.3	Consensus Modules . . . . .	14
2.6	Zero-Knowledge Proofs . . . . .	17
2.6.1	Proofs and Arguments . . . . .	18
2.6.2	zkSNARKs . . . . .	18
2.6.3	RSA in zkSNARKs . . . . .	20
2.6.4	NP and Complexity-Theoretic Reductions for zkSNARKs . . . . .	20
2.6.5	Quadratic Span Programs for solving zkSNARKs . . . . .	21
<b>3</b>	<b>Related Work</b>	<b>22</b>
3.1	Increase Trust in Supply Chains using Blockchain . . . . .	22
3.1.1	Potential Risks for Consumers in Supply Chains and how Blockchain can Mitigate those Risks . . . . .	22



3.1.2	How Transparency, Tractability, and Perceived Trust Affects Blockchain Adoption in Supply Chain . . . . .	25
3.2	Digital Trust in the Web-Based Applications . . . . .	26
3.2.1	Characteristics of a Perceived Trustworthy Web Application . . . . .	26
3.2.2	Perception of Adequate Security and Privacy, and how it Increases Trust . . . . .	28
3.2.3	Algorithm Transparency and how it Affects Trust . . . . .	30
3.2.4	Privacy and Security as Drivers for a Users Perceived Trust in Blockchain . . . . .	33
3.3	Providing Privacy and Security in Blockchain Systems . . . . .	36
3.3.1	Off-Chain Data Storage . . . . .	36
3.3.2	Zero-Knowledge Proofs in Blockchain . . . . .	40
<b>4</b>	<b>Research Method</b>	<b>43</b>
4.1	Explorative Study to find Drivers of Trust . . . . .	43
4.1.1	Research Motivation . . . . .	44
4.1.2	Use case: Fairtrade . . . . .	45
4.1.3	Development of Clickable Prototypes . . . . .	48
4.1.4	Interviews and User Testing . . . . .	63
4.2	Re-interview and User Test of Improved Prototypes . . . . .	64
4.2.1	Expanding the Graphical Explanation . . . . .	65
4.2.2	Presentation of Blockchain Data . . . . .	65
4.2.3	Improved Prototypes . . . . .	66
4.3	Technical Implementation to Address RQ3 . . . . .	69
4.3.1	Research Motivation . . . . .	70
4.3.2	System Design . . . . .	70
<b>5</b>	<b>Results</b>	<b>71</b>
5.1	Explorative Study to find Drivers of Trust . . . . .	71
5.1.1	Rating of the Prototypes . . . . .	71
5.1.2	RQ1: Elements that Enhance Perceived Trust from Step 1 . . . . .	76
5.1.3	RQ2: Technical Details and Explanations to Enhance Trust . . . . .	77
5.2	Re-interview and User Test of Improved Prototypes . . . . .	79
5.2.1	Results for Prototype 1.5 . . . . .	79
5.2.2	Results for Prototype 2.7 . . . . .	79
5.3	Technical Implementation to Address RQ3 . . . . .	80
5.3.1	System Model . . . . .	80
<b>6</b>	<b>Discussion</b>	<b>88</b>
6.1	Perceived Trust in a Technical System . . . . .	88

---

6.1.1	RQ1: Elements that Enhance Perceived Trust . . . . .	88
6.1.2	RQ2: Technical Details and Explanations to Enhance Trust . . . . .	91
6.1.3	RQ3: Unlikable Transactions and High Level of Privacy with Blockchain . . . . .	93
6.2	Limitations and Assumptions . . . . .	94
6.2.1	Interviews and User Tests . . . . .	94
6.2.2	Use Case: Fairtrade - Blockchain . . . . .	95
6.2.3	System Implementation . . . . .	96
<b>7</b>	<b>Conclusion and Future Work</b>	<b>97</b>
	<b>Bibliography</b>	<b>99</b>
<b>A</b>	<b>Link to Clickable Prototypes</b>	<b>103</b>
A.1	Data provider . . . . .	103
A.2	Data consumer . . . . .	104
<b>B</b>	<b>Interview Guide</b>	<b>105</b>
B.1	Explorative Study to find Drivers of Trust . . . . .	105
B.1.1	Data Provider . . . . .	106
B.1.2	Data Consumer . . . . .	106
B.2	Re-interview and User Test of Improved Prototypes . . . . .	108
<b>C</b>	<b>Link to Code Repository</b>	<b>109</b>

# Chapter 1

## Introduction

This chapter provides an introduction to the topic of blockchain and its usage in supply chain systems. The research goal of the thesis is stated, along with three research questions. The research questions provide the foundation of the research throughout the thesis and its structure.

### 1.1 Research Motivation

Use of blockchain has risen to achieve widespread adoption in recent years, in large part due to the widespread coverage and use of Bitcoin, Ethereum and other digital currencies [Nakamoto, 2009, Buterin, 2013]. One of the most important reasons for this increase in use is the fact that blockchain networks do not require a centralized trusted party to operate. Another essential aspect of blockchain networks is data immutability, meaning data stored on the blockchain is practically infeasible to alter. These properties, along with the concept of block validation, make blockchain systems suitable for use in such digital currency schemes. This technology, however, has a variety of use cases beyond just the somewhat limited scope of digital currencies. In recent years researchers have looked at the possibility of using blockchain technology in supply chains and other systems, such as medical patient journals. This research looks at the characteristics of blockchain networks and attempts to find other suitable use cases, and whether there exists new interesting fields of research which have not been studied yet.

As detailed in Yeh et al. [2019], food traceability and transparency is an issue which could potentially be linked to and utilize the concept of decentralized blockchain networks. Currently consumers either have little to no information at all regarding the origin of the food they consume, or they have to trust in a third party system or organization, such as the Fairtrade. This is potentially a field in which a decentralized network could

link consumers more closely with producers and workers producing groceries. This decentralization, along with the data immutability aspects of blockchain networks, seem particularly useful for this specific case. However, along with these desired properties, several challenges arise. These challenges relate, in large parts, to how to ensure privacy and how to maintain security, while still making sure the data can be verified and that it has not been tampered with. Additionally, questions arise as to whether consumers and producers trust these systems and their willingness to use and utilize them to their full potential.

While blockchain is a fascinating new field of technology with potential application in this field, there are still several drawbacks to these networks, and several open unanswered questions. As mentioned, a lot of these questions relate to privacy and security aspects, as well as efficiency. Some of these issues can be amended in order to most effectively and securely utilizing blockchain in supply chain systems for food and groceries. By using a variety of cryptographic methods one can still retain, and potentially increase, the level privacy, while still retaining several of the unique and useful aspects of blockchain in and of itself. This opens several new fields of study, however, by incorporating other forms of technology one is faced with a new set of challenges.

Complicated technology, such as blockchain and various cryptographic methods, being introduced to the public at large also creates new research possibilities regarding perceived trust. Thus several questions arise regarding how to bridge the gap between humans and technology. It is essential that users trust in systems, in order for them to feel confident that the technology works in their best interest. Blockchain networks are relatively new and the public is mostly familiar with them as digital currencies. How does this translate to other systems and applications, such as supply chains?

Technical aspects of privacy and security in blockchain supply chain systems will also be investigated in this study. The goal is to develop features for a blockchain system where the users are able to upload unlinkable transactions to the blockchain to stay anonymous to the other users in the system. A possible way of integrating an off-chain database with the blockchain supply chain system to provide data integrity for the users, while maintaining a lower overhead than what would be possible with all data stored on-chain is also studied.

## 1.2 Research Goals

The research in this thesis focuses on the goal of creating a framework for privacy-preserving blockchain systems, in which users can have a high level of trust. This goal has two main aspects – the concept of a users perceived trust and the underlying

technical requirements for such a system. In this context perceived trust refers to the users' experience of trust using the site. For instance, this could be that a user trusts the information on a site, or trusts that the site does not sell their personal data. In this study, we will investigate what affects this perception of trust for a user and how this can help increase trust in blockchain systems. Thus, based on the research goal, two research questions related to perceived trust and one related to the technical implementation are defined and explained in 1.3.

## 1.3 Research Questions

**RQ1: What is important to a non-technical user when evaluating if a technical system is trustworthy in terms of security and privacy?** Trust is a subjective way for an individual to determine if their needs are likely to be met by a provider. This decision is made by the individual based on the information they possess and the way they perceive a given situation. These factors can for instance be branding, visual elements, and understandable system overviews. In this study, one of the goals is to identify which factors are important to users when determining if a system is trustworthy or not, and based on these factors discuss what can be done to enhance trust. Trust is, in this study, limited to a user's trust in a system to provide security and privacy in accordance with their expectations.

**RQ2: What is the best way to explain a technical system to a user, to convince them that their security and privacy are preserved when using the system?** A hypothesis is that one of the important factors from RQ1 is that the user's understanding of the system influences trust. Based on this hypothesis the way a technical system is explained to a user will affect the perceived trust of the system. For non-technical users using a technical system the trust, or distrust, they experience towards the system can be built on wrong assumptions about the workings of the system. This study will also investigate what the best way to explain a technical system built on blockchain and zero-knowledge proof is, to a user that is not familiar with these technologies, in order to enhance trust. In this case trust is also limited to privacy and security as is the same with RQ1.

**RQ3: How could a privacy-preserving blockchain system be designed, providing unlinkable transactions and a high level of privacy for users?** Blockchain networks store data on a shared ledger, meaning every peer in the network has access to all data and all transactions stored on the ledger. While this is an efficient way to ensure data immutability, it does not bode well for systems in which sensitive data is stored. Thus, in order to create a privacy-preserving system using blockchain, one has to find and utilize relevant cryptographic methods to support the studies of RQ1 and RQ2.

## 1.4 Contribution

This thesis thus provides the following contributions to each of the research questions detailed in 1.3:

**RQ1:** Identifying several elements in a system which affect perceived trust of security and privacy for a user and how these elements can be improved to increase the perceived trust for the users. Overall trust is increased by visual components, usability and trusted third parties. Information about the features and understandable technical explanations are particularly useful to security oriented systems, and this was investigated further in RQ2.

**RQ2:** Uncovering the preferred way for a user to be presented an explanation of how the blockchain and zero-knowledge proof system works and why the technologies used is beneficial.

**RQ3:** A framework model for a privacy-preserving blockchain system. The system stores raw data off-chain in order to limit direct access. Additionally, it uses a zkSNARK scheme in order to create unlinkable transactions and preserve anonymity in the network.

## 1.5 Outline

The following content of this thesis is structured in a set of chapters as defined below:

**Background** is the first chapter following this and details the current state of research and theory in relevant scientific fields.

**Related Work** describes the work in a detailed.

**Research Design** describes the approach to research and method design. Additionally, this chapter describes the implementation and system design for the technical implementation.

**Results** provides the results from the study and is structured in a similar manner as Research Design.

**Discussion** discusses the results in comparison to related work. This chapter also contains discussion on academic, as well as industrial, impact.

**Conclusion** is the final chapter and provides final thoughts and potential future work.

# Chapter 2

## Background

This chapter details the underlying theory for the study conducted in this thesis. The theory covers a wide range of relevant topics, most notably digital trust, data security and privacy, blockchain, and zero-knowledge proofs. These are covered in detail with a focus on particularly relevant fields of research.

### 2.1 Sociological Trust to Digital Trust

To be able to evaluate perceived trust in digital spaces one must first understand what trust is, what components of trust exist, and the similarities and differences between digital trust and sociological trust. Both Mahmood [2006] and Yan and Holtmanns [2008] present definitions of trust, and discusses, based on research, how one can map sociological trust to digital trust. This section will present definitions of trust, discuss the important elements of trust, and how trust is experienced in online or digital spaces. Lastly, a conceptual model for trust, which can be used when building trust online is presented.

One of the formal definitions of trust from Yan and Holtmanns [2008] is:

**Definition 1** (Trust - Definition 1). *Trust is a state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk.*

This definition addresses three core elements of trust. The first one is that trust always involves two, or more, entities. These can be individuals, companies, or systems, just to name a few. Uncertainty and risk is the second element of trust. When trust is involved there will always be a risk the trustee will fail to live up to the trustor's expectation. In this case, the trustor is an entity that trusts the other entity, the trustee, to act on

behalf of the trustor. The third, and final, element in this definition is that the trustor believes that the trustee is honest and to their best ability lives up to the expectations set by the trustor. An alternative, and more comprehensive, definition of trust is:

**Definition 2** (Trust - Definition 2). *Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of their capacity of ever to be able to monitor it) and in a context in which it affects [our] own action.*

This definition identifies the last important trade of trust, trust is subjective to the trustor. This means that in the same situation two different individuals with the same knowledge could experience different amounts of trust towards the trustee. In addition, the term trust is also dependent on the context it is used. When psychologists use trust they use it to refer to a personal trait, in economics it is often used when talking about risk management, and in sociology, it relates to social structures.

In addition to echoing this definition of trust, Mahmood [2006] also draws a distinction between internal trust and external trust. Internal trust is the kind of trust, as defined above, where an entity trusts that a different entity will provide a service. External trust is the trust a trustor must have in the external factors, all the factors that are not under the control of the trustor or trustee. External trust typically plays bigger role in digital and online spaces than what it does in other trust relationships. This might be due to experiences of system failures, bad internet connection, a lack of understanding which leads to higher perceived risk, or other factors the service provider can not control.

### 2.1.1 Conceptual model of Trust

Mahmood [2006] presents, based on empirical and theoretical studies and market trends and definitions of trust, a conceptual model to understand trust and how to enhance trust in online environments. This model is based on 4 aspects:

- **Professionalism:** This is a trait that often is described as an entity with good standing in an industry. This is often evaluated by consumers by visual cues. In a digital environment this will often be how their web page looks, the use of graphics and pictures, the web sites usability, or the branding and marketing efforts of the company.
- **Credibility:** Credibility is how believable an entity is when presenting a statement, or how believable they are as a source of information. In the physical world, this is often evaluated by the users based on context, geography, or previous experiences. In digital mediums or online, this credibility is often provided by trusted third parties or endorsements from individuals or entities the user trusts.



- **Honesty:** This is the quality of handling and communicating in a truthful way. One prominent concern for users regarding honesty, is what the service provider does with personal data. Trusted third-party verification of correct handling of personal data is a potential solution to this. An alternative which can also increase trust is giving users control over their own data, or an easy-to-read privacy policy.
- **Capability and performance:** Word of mouth is the most effective way to increase trust with regards to capability and performance in the physical world. In a digital space, trusted referrals and online reputations are the most important factors to increase perceived trust.

These 4 elements in this model help understand perceived trust can affect trust in different ways. In some scenarios, performance might be one of the most important factors to enhance the total trust in a product or service, while other times the credibility is by far the most important factor [Mahmood, 2006].

## 2.2 Data Security and Privacy

The field of data security is concerned with the measures of detecting, preventing, and correcting violations of security when transmitting the information. For instance this can be a case where user A is transmitting a file to a different user B, where the file contains sensitive information which should be protected against a third user trying to access it. A different example is a case where user C receives a message from user D, that user C can trust that this message is from user D.

A definition of computer security from Guttman and Roback [1995] goes as follows:

**Definition 3** (Computer Security). *The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).*

Stallings [2017] derives 3 objectives that are key in computer security.

- **Confidentiality:** The term confidentiality covers two concepts in computer security. The first one is data confidentiality that is focused on assuring that private and confident information is not made available to individuals or institutions that should not have access to that information. The second part is privacy that assures that the individuals that provide private information are in control of information that may be collected and stored, and by whom that information can be shared.
- **Integrity:** Under integrity, there are also two important concepts. The first is data integrity, meaning that data, either stored or transmitted, is not changed in

an unauthorized way. System integrity on the other hand is a term used to describe an aspect of computer security that focuses on the system working as intended and performing its operations in the way it is expected.

- **Availability:** The term availability, defines the assurance that data is available when it needs to be available.

Together these 3 traits are referred to as the CIA trades and are considered the most important factors to provide adequate computer security. Additionally, there are many more categories in computer security. Two of the most important according to Stallings [2017] are:

- **Authenticity:** The property of trusting that the message or transmission originated from the person or entity that claimed to have sent it. This means that a receiver can trust that the information provided came from the source that they think it came from.
- **Accountability:** Is the property of being able to trace an action uniquely back to the entity that performed that action. This is important since completely secure systems are not possible yet, so tracking security breaches is important to hold the entity that violated the security accountable.

According to Stallings [2017] it's not tangible to provide all these five security properties in the same system because they often require different attributes from the system that is hard, or impossible, to combine. Therefore, what one provides of security and privacy to a system depends on the needs of that system. Some systems require a extremely high availability, and to achieve this it can neglect some of the other properties, while other systems require perfect data integrity without the need for high availability.

## 2.3 Cryptographic hash functions

As described in Stallings [2017], *hash functions* are functions which accept a variable-length block of data as input, and then produces a fixed-size bit array, called a *hash value*. These functions should ideally produce evenly distributed and seemingly random outputs, meaning a principal object of the hash function is data integrity. Thus a change in any input bits should, with a high probability, produce a change in the resulting output hash value.

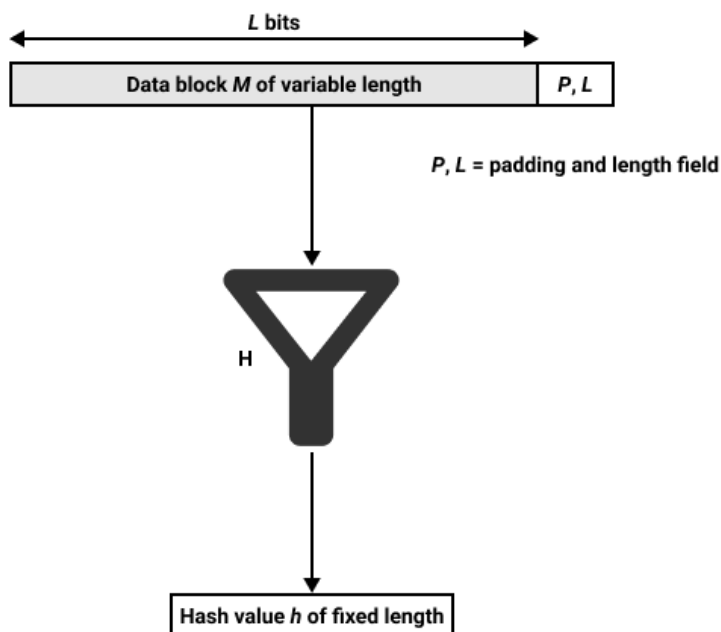


Figure 2.1: Cryptographic hash function. The hash value  $h = H(M)$ , where  $H$  is the function and  $M$  is the message block.

For more security applications, Stallings [2017] says a special type of hash function is required, namely a *cryptographic hash function*. Like with normal hash functions, cryptographic hash functions take a variable-length input block and generates a fixed-size hash value. Cryptographic hash functions, however, also require another property. This property is that it should be computationally infeasible to find a data object which maps to a pre-specified hash value, or two data objects which map to the same hash result. Thus, one can use cryptographic hash functions to determine whether data has been changed.

### 2.3.1 Secure Hash Algorithm

The most widely used hash function in recent years is the *Secure Hash Algorithm (SHA)* [Stallings, 2017]. This is mainly due to the fact that almost every other widely used hash function has been found to have substantial weaknesses. The SHA family was introduced with *SHA-0*, which was then found to have weaknesses and revised, resulting in *SHA-1*. Table 2.1 shows an overview and comparison of the various algorithms in the SHA family.

Algorithm	Message Size	Block Size	Word Size	Message Digest Size
SHA-1	$< 2^{64}$	512	32	160
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512
SHA-512/224	$< 2^{128}$	1024	64	224
SHA-512/256	$< 2^{128}$	1024	64	256

Table 2.1: A comparison of the different algorithms in the SHA family and their parameters.

## 2.4 Elliptic Curve Cryptography

While RSA is currently the most commonly used public-key cryptography for encryption and digital signatures, a competing system has arisen, namely *elliptic curve cryptography (ECC)* as described in Stallings [2017]. The use of ECC is motivated by a few important factors, one of them being key size. As key length for secure use of RSA has increased in recent years, processing load on applications using RSA has also increased. ECC uses a far smaller key size compared to RSA, offering equal security. This in turn reduces processing overhead.

### 2.4.1 EdDSA

The *Edwards-curve Digital Signature Algorithm (EdDSA)* is an ECC Josefsson and Liusvaara [2017]. It is a variant of Schorr's signature system based on twisted Edwards curves. The design is intended to be faster than existing digital signature schemes, without affecting the level of security in a system. EdDSA was introduced in Bernstein et al. [2011] for *Ed25519* and *Ed448*, and has several advantages to other digital signature schemes. These advantages include high performance on various systems; no need for a random number for each signature; resilience to side-channel attacks; small public keys (32 or 57 bytes) and signatures (64 or 114 bytes) for Ed25519 and Ed448, respectively; "complete" formulas, meaning they are valid for all points on the curve; and lastly collision resilience. A generalized version of the EdDSA was described in Bernstein et al. [2015].

**Ed25519** The version of EdDSA signature scheme over SHA-512 and Curve25519 is called Ed25519. Curve25519 is an elliptic curve which offers 128 bits of security, using a 256 bit key-size [Josefsson and Liusvaara, 2017].

## 2.5 Blockchain

A blockchain is a cryptographically linked, growing list of records, called blocks. The technology was implemented for use as a distributed ledger, to be maintained and managed in a peer-to-peer network, thus in a decentralized fashion. Blockchain technology intentionally makes it hard to alter data retroactively. The reason for this is that its structure makes it so the alteration of data in a single block, requires alteration of data in all subsequent blocks. This way one could easily check and verify whether data has been altered after being added to the blockchain.

Blockchain was first introduced as the core technology used in the digital currency Bitcoin by Nakamoto [2009]. While originally only used in digital currencies, like Bitcoin, the field has expanded and blockchain is now being used in a variety of other services, such as other financial services, risk management, gaming, government, and internet of things. Blockchains viability in other services are due to several intrinsic properties, which makes it desirable for the aforementioned use cases. These intrinsic properties are decentralization, persistence, anonymity, and audibility. As a technology blockchain builds on multiple existing fields of research, most notably cryptographic hashing, game theory, and consensus mechanisms, as well as several other modern computer science concepts. While blockchain as a technology shows great promise, it is facing some considerable challenges, as described by the scalability trilemma formulated by Vitalik Buterin, which states that you can only have two out of the three properties decentralization, scalability, and security [Zhang and Jacobsen, 2018]. The following sections of this paper will discuss the general blockchain architecture, as it is presented in Zheng et al. [2018].

As described, blockchain is in essence a growing list of records, this list often being described as a chain of blocks, thus the name. Network transactions are submitted by peers, these transactions are then wrapped in a block, which is subsequently proposed to be added to the blockchain. Each block in the blockchain points to the previous block with a hash value, which is obtained by hashing the content of the previous block. The previous block in the chain is referred to as the parent block relative to the block one is looking at. The very first block in the blockchain is called the genesis block, and it is unique in that it has no parent block. Every block in the chain can be viewed as a page in a distributed ledger. Seeing as the hashes used to link the blocks together are created using cryptographic hash functions on the data stored on the block, an imposter would have to recalculate every single block, if they wanted to tamper with a transaction in a block. This becomes an infeasible task very quickly, when the blockchain reaches a certain length. This is the main reason why blockchain is considered to be tamper-resistant.

A copy of the entirety of the blockchain is stored on every single node in the network, which means that there are a lot of duplications of the chain and its data. This is another reason why it is hard to tamper with, as one single change would have to be propagated throughout the entire network. Paraphrased, if one were to alter a recorded transaction, one would have to alter that transaction on many replicas stored on many different nodes in different geographical areas. This is another one of the strengths in blockchain systems, especially compared to a centralized alternative.

### 2.5.1 Blockchain Building Blocks

**Blocks** The most essential structure in blockchain are the blocks. Blocks contain batches of transactions that have been validated, hashed and are then stored in a Merkle tree. Each block contains a set of several different fields, which may vary depending on how the blockchain has been implemented. Commonly found fields in the block, are for instance: a field that indicates what validation rules to follow; a parent block hash, which is a cryptographic hash value that is pointing to the parent block of that block; a Merkle tree root hash, which is a cryptographic hash value consisting of all the transactions in that block; and lastly a timestamp, indicating when the block was originally added to the chain. One will also find fields related to the consensus algorithm used in many existing blockchains – for example in Bitcoin, the Proof-of-Work consensus algorithm is used, so a nonce field is required in the block.

**Digital signatures** Every participant in the blockchain network generate a pair of keys, one public key and one private key. Every transaction has to be signed if it is to be validated, which is done using the private key of the participant creating the transaction. Subsequently, signed transactions are added to a block. The block is committed to the blockchain, so it can be distributed across all the nodes in the blockchain network. To verify a transaction, a different participant can use the public key of the signer, and can then confirm that the transaction is valid and signed by a participant in the network.

**Blockchain characteristics** One of the main incentives behind blockchain, and thus one of its key features is the concept of decentralization. This is in strong contrast to how centralized services, such as commercial banks and government systems, work. In centralized systems, there has to be a central authority, which verifies information, and is thus verifying each transaction that is made, before they can be executed. Blockchain network transactions are handled in a decentralized fashion, meaning that transactions have to be verified by nodes in the network, handled in a peer-to-peer system, instead of having to go through a central authority. In addition to this, blockchain networks

also maintain a high level of persistence. This level of persistence arises from the fact that when transactions are confirmed and then distributed across the entire network, it is almost impossible to tamper with and alter this, without other participants in the network noticing something is wrong. The reason why the blocks, and their included transactions, have to be verified by nodes in the network, is to ensure none of the rules of the network are breached before they are accepted to the blockchain. Pseudonymity is another valuable characteristic of blockchain networks. Pseudonymity is achieved by having a user be identified by a generated address, this is to ensure that they do not have to give up any kind of personal information, sensitive or not, like a social security number or a name. Due to its structure, blockchain is transparent and traceable, as all the transactions are available and readable to the all participants in the network, and they can thus be verified by anyone. Rules for transaction and block validation are defined in the consensus modules, which are an essential aspect of blockchain networks. The consensus module decides which node will be allowed to propose the next block of transactions, and it is then appended to the blockchain and distributed to all the peers in the network. Finally, a valuable characteristic of blockchain networks is the concept of immutability. Immutability means that when data is added to the blockchain, it can no longer be altered or tampered with afterwards. This makes blockchain more secure than regular databases, as you know the data is valid, and it is not subject to change in the future.

## 2.5.2 Types of Blockchain Networks

There are multiple ways to configure blockchain networks, with different settings, depending on who should have access to it, who should be able to grant access to it and what permissions any given participant has. Generally speaking, blockchain can be grouped into four distinct types – public, private, permissioned and permissionless blockchain. However, these overlap to some extent. The following sections will explain what defines each of these four and in which ways they are similar and different.

**Public Blockchain** The first blockchain network introduced in Nakamoto [2009], famously known as Bitcoin, is the first and most well known example of a shared public ledger. Public blockchain networks can be audited by anyone.

**Private Blockchain** The difference between a public and private blockchain network, as the name implies, is that in a private blockchain network only selected and verified participants can gain access [Ethereum, 2021]. Joining such a private blockchain network requires an authentic invitation. Following the invitation, the participant has to be accepted into the blockchain network, either by the network operator or a protocol

defined by the network administrators. This means the operator has the ability to override, edit and delete entries in the blockchain. A private blockchain network operates less as a decentralized platform, and more as a distributed, private ledger. It is a solution aimed at private companies and similar organizations.

**Permissionless Blockchain** Permissionless blockchains are networks in which anyone can become a validator.

**Permissioned Blockchain** Permissioned blockchain networks can be configured and customized in a variety of ways. A set of permissions can be given to a participant upon joining a permissioned blockchain, which decides whether the participant can perform actions such as making and validating transactions. Permissioned blockchain is designed so that every participant is granted a set of permissions, which is a solution aimed at businesses and organizations intending to keep control over which participants can perform what actions, without having a truly private, invite-only blockchain network. While the terms public, private, permissioned, and permissionless blockchain denote rules regarding which users have access to and permissions on a blockchain network, and how this is configured, consortium blockchain denotes a slightly different type of configuration. A consortium blockchain network is the most common type of permissioned blockchain. It is a blockchain network, which does not belong to a single company or organization, but rather a consortium of organizations. This can for example be a set of companies working within a single industry. This distinction is useful when discussing the application of different types of blockchain. Zhong et al. [2020] is an example of an implementation of a consortium blockchain network using Hyperledger. Permissioned blockchain networks belonging to a single company is a special case.

### 2.5.3 Consensus Modules

As discussed in section 2.5, each transaction is added and then committed to the chain. This raises the question about who will be allowed to propose the next block that is added to the blockchain, the answer to this is decided by the consensus module. The consensus module decides which participant in a blockchain network gets to create the block, and also how to prevent a malicious node in the network from submitting a block containing illegitimate transactions. The consensus module contains a specific type of algorithm to which decides, through majority dominance, which node in the network will get to propose a new block [Du et al., 2017].

In Nguyen and Kim [2018] two main groups of consensus modules are presented and discussed. The first one is proof-based consensus, for example Proof-of-Work and Proof-of-Stake. These types of consensus modules are characterized by the fact that nodes



need to prove that they are more qualified to submit a block to the chain, than the other nodes in the network. The other group of consensus modules presented are voting-based consensus modules. These two groups will be described in detail in the following paragraphs

### **Proof-Based Consensus Modules**

Proof-based consensus modules are consensus modules which do consensus by having nodes joining the verifying network in order to show that they are more qualified than the other nodes to append to the ledger [Giang-Truong and Kyungbaek, 2018]. Even though proof-based consensus can be used in private and permissioned, these algorithms are most commonly found in public blockchains.

**Proof-of-Work** Proof-of-Work, based on Finney [2004], was the first type of proposed consensus module for blockchain networks. Its first implementation in blockchain networks was in Nakamoto [2009], with the release of Bitcoin. The concept builds on the idea that each node is faced with a task that requires a lot of computational power to solve, but once solved, it is easy to verify whether the answer is correct. The first node to find the correct answer to the task gets to propose a block to the blockchain. It is common for the nodes participating to receive some sort of compensation, usually in the form of cryptocurrency, for the work they put into solving this task and posting the block. This is good protection because nodes in a blockchain network trust the longest chain, so for a malicious actor who wants to tamper with any data in a block on the chain, they would need to control more than 50% of the computational power to be sure to have the longest chain. The compensation for doing honest work will outweigh the gains from tampering with the blocks on the chain, which makes for a strong incentive to be doing honest work. In the case of Bitcoin, HashCash is used as the mathematical task that has to be solved for the Proof-of-Work consensus module. Du et al. [2017] describes the HashCash algorithm in the following way:

1. **Retrive difficulty:** When 2016 blocks are mined, the Bitcoin algorithm will adjust the difficulty for the entire network. The miners have to retrieve the current difficulty before they can start mining.
2. **Transactions:** In the second step the miner has to collect a given amount of transactions, then find the Merkle Root of these transactions. The miner also needs to get the block version number, the 256-bit hash for the previous block, the current target hash value, and the nonce.
3. **Mining:** The most time-consuming part is the mining, wherein a worker traverses the Nonce from 0 to  $2^{32}$  and calculates the SHA-256. If the calculated hash value

is equal to, or less than, the target value, then that means the miner won. The miner gets to broadcast its block for verification.

4. **Restarting:** If the node uses too much time of step 3, then it restarts from step 2. If any other miner mines a block, then all other miners start from step 1.

This is not the only way to implement a Proof-of-Work consensus module, however, it is the one used by Bitcoin and some other public blockchain networks. For instance, the calculation tasks performed in a Proof-of-Work consensus module can differ.

**Proof-of-Stake.** A different proof-based algorithm is Proof-of-Stake. The algorithm in this module does not rely on miners doing energy-demanding work to validate new blocks. It is also easier to join, which can make the blockchain network more decentralized, as one does not need huge mining pools to be able to participate [Saleh, 2020]. The concept is that to be able to be selected to propose a new block to the blockchain, the node needs to put up a stake. These stakes are often in the form of the cryptocurrency associated with the blockchain. The selection process should be random and uniform, but the bigger the stake the node puts up, the more likely it is to be selected. To make sure that not only the nodes with the biggest stakes are selected, different methods are employed and implemented, to make sure that this does not happen. One example of this is that a node will be given a time out for a given time after it has been selected to make sure that the same group of nodes not always gets to mine the next block.

The owners of the cryptocurrencies need some sort of incentive to put up their cryptocurrencies as a stake. The incentive in Proof-of-Stake is that the owners that put up stakes receive a payment, which is in the form of transaction fees from the transactions in the block that they add to the chain. To avoid fraud, the block from the selected node is verified by the rest of the nodes in the network, and if they detect any errors or attempts of fraud, an amount of cryptocurrency is taken from that node's stake as a fee. For this to be efficient, the fee for proposing a fraudulent block has to be set higher than what can be gained, in the case that a node get to propose a block with invalid transactions. This means that to be able to cheat the system an actor in the network needs to own over 50% of the cryptocurrency, and given the size of blockchain networks and thus, the value of most of these cryptocurrencies, this is not feasible. The participants in a network can at any time request to withdraw their stakes and potential earnings. However, before the funds are released, the majority of the nodes need to make sure that the participant does not have any block, which has not yet been validated.

### Voting-Based Consensus Modules

Another type of consensus modules is voting-based consensus, where a node needs to reach a threshold  $T$  of the votes from the other nodes in the network, to be allowed to submit a new block Nguyen and Kim [2018]. This threshold often represents 50% of the nodes in the network. Voting-based consensus modules are most common in private and consortium blockchain, but they can also be used in public blockchains as well. This type of consensus module is intended to be democratic, however pure vote-based consensus modules do not exist, as having all nodes vote on every decision would be inefficient.

**Practical Byzantine Fault Tolerance.** Practical Byzantine Fault Tolerance (PBFT) was first introduced in Castro and Liskov [1999], and its aim was to design an algorithm that would be Byzantine fault tolerant, also in asynchronous systems like the internet. Byzantine fault, in this case, describes a distributed network, where a component may fail and the data on whether it has failed is imperfect. A system being Byzantine fault tolerant thus, means a system where, if there is uncertainty on whether a component has failed, the system is still able to function. Du et al. [2017] illustrates in four steps how PBFT is implemented in blockchain networks. The steps are as follows:

1. A client sends a request to the leader to invoke a service operation.
2. The leader then multicast the request to all the backup nodes.
3. The nodes receiving the request execute it and, sends a reply to the client that the request is executed.
4. The client waits for  $f + 1$  replies from different nodes containing the same results.  $f$  is here the maximum number of nodes that may be faulty. When the  $f + 1$  replies are received, the task is completed, and the consensus is reached.

PBFT is more commonly seen in private or permissioned blockchains like Hyperledger from IBM.

## 2.6 Zero-Knowledge Proofs

*Zero-knowledge proof* is a cryptographic method, in which one party can prove to another party that they know a value  $x$ . They do not however have to convey any other information apart from the fact that they know the value, and they do not have to share said value. In essence it is trivial to prove that one possesses knowledge of certain information by revealing it, and so the challenge lies in proving such possession without revealing anything about the information or any additional information. In recent years

zero-knowledge proofs have been utilized in blockchain networks in order to increase levels of privacy and security [Ben-Sasson et al., 2013, Ben Sasson et al., 2014].

In Goldreich and Oren [1994], there has been formulated formal definitions for zero-knowledge proofs. They are based on interactive proof systems for a language  $L$ , which is a protocol for two probabilistic time machines called the *prover*  $P$  and the *verifier*  $V$ . This paper provides the following definition:

**Definition 4** (Zero-knowledge proof). *An interactive proof system for a language  $L$  is zero-knowledge if, for every probabilistic polynomial-time machine  $V^*$ , there exists a probabilistic polynomial-time algorithm  $M_{v^*}$ , such that on input  $x$ , it produces a probability distribution  $M_{v^*}(x)$  where  $\{M_{v^*}(x)\}_{x \in L}$  and  $\langle P(x), V^*(x) \rangle_{x,y \in D_1}$  are polynomially indistinguishable.*

## 2.6.1 Proofs and Arguments

In the field of zero knowledge, one tends to differentiate between interactive proof systems and arguments. The distinction is quite technical, but worth noting. As explained in Goldreich et al. [1991], the difference between an interactive proof system and an arguments, is that in an argument the soundness condition is restricted to probabilistic polynomial-time machines. This means that in zero knowledge arguments it is infeasible, however not impossible, to fool the verifier into accepting an input that is not in the language. This means that a prover with enough computational power can create arguments with wrong statements. It is however worth noting that this is true for any public key encryption systems.

## 2.6.2 zkSNARKs

The paper Reitwiessner [2016] describes zkSNARKs and how they function in a detailed, but concise manner. zkSNARK is an acronym that stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge”, and is a type of zero knowledge proofs. More specifically zkSNARKs are a proof construction, in which a person can prove possession of certain information, such as a secret key, without having to reveal said information. This is also done without any interaction occurring between the prover and the verifier.

“Zero-Knowledge”, as described in earlier sections, implies a system in which one party can prove to another party, that a given statement is true, and this is done without revealing any information except for the validity of the statement itself. A fitting allegory for this concept could be having to show a bouncer at a bar your ID, which will reveal certain personal information such as name, date of birth and more. Using Zero-knowledge proofs you would transform your ID to another form, which would still prove that you

are of legal age, without having to reveal any such personal information. “Proof of Knowledge” in zero-knowledge proof terms, means that the prover is able to show the verifier that they know a number exists, but also that they know what this number is. This can be done without having to reveal said number or any information about it. However zkSNARKs use arguments, instead of proofs. The distinction is technical and both yield a similar result, but a more specific description based on Goldreich et al. [1991] is provided in section 2.6.1.

“Succinct” indicates that a zero knowledge proof can be solved within a few milliseconds, with a short proof length, usually within a few hundred bytes, even for very large programs. “Non-Interactive” has to do with the interaction between the prover and the verifier. The first ever zero knowledge proofs required multiple rounds of back and forth communication between these parts. Non-Interactive proofs are much more efficient, and if they are short enough they can be published to a blockchain.

As Reitwiessner [2016] puts it, zkSNARKs consist of 4 main parts:

1. Encoding as a polynomial problem.

The program to be checked first has to be compiled into a quadratic equation of polynomials, as such:  $t(x)h(x) = w(x)v(x)$ . The equality in this case only holds if the program is computed correctly. The idea is that the prover wants to convince the verifier that this does indeed hold.

2. Succinctness by random sampling

An evaluation point,  $s$ , is chosen by the verifier to reduce the problem from multiplying polynomials and verifying function equality, to simple multiplication and equality check instead. Thus we have  $t(s)h(s) = w(s)v(s)$ . This part is essential, as it efficiently reduces the proof size and verification time.

3. Homomorphic encoding/encryption

A function,  $E$ , is used for encoding/encryption. The function has homomorphic properties, but it is not fully homomorphic. This function lets the prover compute  $E(t(s))$ ,  $E(h(s))$ ,  $E(w(s))$ , and  $E(v(s))$ , without having to know  $s$ , but only  $E(s)$  as well as some encrypted values.

4. Zero Knowledge

The final piece of the puzzle, is that the prover obfuscates the values  $E(t(s))$ ,  $E(h(s))$ ,  $E(w(s))$ , and  $E(v(s))$ , by multiplying with a number. This means the verifier can still check the equations, without the prover having to show any of the encoded values.

### 2.6.3 RSA in zkSNARKs

The RSA algorithm is utilized in constructing zero knowledge proofs [Reitwiessner, 2016]. RSA is structured as follows. The prover comes up with a set of numbers:

- $p, q$ : two randomly selected, secret prime numbers
- $n := pq$
- $d$ : a randomly selected number  $1 < d < n - 1$
- $e$ : a number which satisfies  $de \equiv 1 \pmod{(p-1)(q-1)}$

Thus the prover has defined a public key  $(e, n)$  and a private key  $d$ . The randomly generated primes  $p$  and  $q$  has served their purpose and can be discarded, but it is essential that they are not revealed to anyone. Thus, due to the fact that we have the following properties, namely that  $c^d \equiv (m^e \% n)^d \equiv m^{ed} \pmod{n}$  and that multiplication in the exponent of  $m$  behaves like multiplication in the group modulo,  $(p-1)(q-1)$ , we have  $m^{ed} \equiv m \pmod{n}$ . This means a message  $m$  can be encrypted as follows:

$$E(m) := m^e \% n$$

Then the encrypted message  $c = E(m)$  can be decrypted as follows:

$$D(c) := c^d \% n$$

### 2.6.4 NP and Complexity-Theoretic Reductions for zkSNARKs

There are two main classes of problems in complexity theory, namely P and NP. P is defined as the class of problems L, which have polynomial-time programs. NP is the class of problems L, which have a polynomial-time program V, that can be used to verify a fact, given a polynomially-sized witness for that fact. There exists zkSNARKs for all problems which fall under the class of NP. Seeing as all computational problems in NP can be reduced to each other, the fact that all of them can be written as zkSNARKs is trivial.

Problems can be reduced and "flattened" in order to create zkSNARKs. This procedure consists of rewriting the problems on the form  $x = y$  and  $x = y(\text{op})z$ , where (op) can be either +, -, \* or /.

### 2.6.5 Quadratic Span Programs for solving zkSNARKs

As explained in section 2.6.4, all problems in NP can be reduced to another problem in NP. Thus, a generic zkSNARK can be found for all problems, which they can be reduced to in polynomial time. Then the task becomes to find a suitable NP problem. One type of problems which seem particularly useful for zkSNARKs are Quadratic Span Programs (QSP). QSPs consist of a set of polynomials, and the task of these programs is to find a linear combination of these polynomials which are a multiple of another polynomial. The strong definition of QSPs are as follows:

A given QSP over a field  $F$  for inputs of length  $n$  consists of

- polynomials  $v_0, \dots, v_m, w_0, \dots, w_m$  over the field  $F$
- polynomial  $t$  over  $F$
- injective function  $f : \{(i, j) | 1 \leq i \leq n, j \in \{0, 1\}\} \rightarrow \{1, \dots, m\}$

Here  $t$  is the target polynomial. The task consists of multiplying the polynomials by some factors and adding them, such that the linear combination is a multiple of  $t$ . Given a binary input string  $u$ , the function  $f$  restricts what polynomials can be used and their factors in the linear combinations.

An input  $u$  is verified by the QSP if, and only if, there are tuples  $a = (a_1, \dots, a_m)$ ,  $b = (b_1, \dots, b_m)$  in the field  $F$  such that

- $a_k, b_k = 1$  if  $k = f(i, u[i])$  for some  $i$ , ( $u[i]$  is the  $i$ th bit of  $u$ )
- $a_k, b_k = 0$  if  $k = f(i, 1 - u[i])$  for some  $i$
- $t$  divides  $v_a w_b$  where  $v_a = v_0 + a_1 v_1 + \dots + a_m v_m$  and  $w_b = w_0 + b_1 w_1 + \dots + b_m w_m$

As long as  $2n$  is smaller than  $m$  there is some freedom in choosing the tuples  $a$  and  $b$ . QSP thus only makes sense for inputs up to a given size, but this problem is removed by using non-uniform complexity.

# Chapter 3

## Related Work

This chapter will cover a section of relevant related work within the fields of blockchain; privacy and security; and perceived trust. The papers are grouped into three sections and covered in detail.

### 3.1 Increase Trust in Supply Chains using Blockchain

In this section, relevant work studying how blockchain can be used in supply chain applications is presented. Discussing both system details and implementations, but also providing analysis into benefits as to why blockchain is useful in the supply chain, makes them relevant for this current study.

#### 3.1.1 Potential Risks for Consumers in Supply Chains and how Blockchain can Mitigate those Risks

The work of Montecchi et al. [2019] focuses on how to develop consumer trust in supply chains. There are many ways a company can enhance consumer trust in a supply chain, for example by engaging trusted third-party actors to verify the companies' claims, or public relations and marketing to develop a brand that consumers find trustworthy. The authors argue that this trust consumers have in the company or supply chain is fragile and can therefore easily disappear when scandals like falsehoods printed on the labels are uncovered. This breach of trust results in a higher skepticism from the consumers of the supply chain, product origin, production method, and so on. The proposed way companies can cope with this skepticism is to increase transparency. This transparency will assure consumers of the provenance of a product, this will again increase the consumers' trust in the product, and that in turn will result in a competitive advantage for



the companies providing more transparency than their competitors. In this work provenance is defined as “information about the creation, chain of custody, modifications or influences pertaining to an artifact”.

As Montecchi et al. [2019] describes, one of the reasons why consumers perceive risk when acquiring a product is because different companies disclose different information, and that leads to an increased risk perception when acquiring the product from the company that discloses the least amount of information. Another causal factor creating a feeling of perceived risk is the fact that there is information asymmetry between a consumer and the company that provides the goods. The authors of this paper split perceived risk for consumers into four different types, as detailed below:

- **Financial risk:** This is the perceived risk a consumer feels towards the monetary value of acquiring and owning a product. Examples include the need for repairing or replacing the product after it is acquired.
- **Psychological risk:** This is the risk of a product damaging or changing the self-image of a consumer. An example of this could be for an individual to acquire a fossil car when a lot of their identity is centered around being environmentally friendly.
- **Social risk:** This risk involves whether a purchase can factor into your social standing. An example of this can be acquiring a piece of clothing with a brand which a consumer is not sure will be socially acceptable in their circle.
- **Performance risk:** This risk involves the uncertainty of the functionality of the product. An example of this can be an individual purchasing a digital device in order to be able to work remotely, but the battery life of this new device is shorter than expected, and this issue leading to the device not helping the individual solving this problem.

After identifying these four types of risks a user or consumer can experience, Montecchi et al. [2019] present a possible solution in order to address these issues effectively. The proposed solution is to have a blockchain containing all the information about a product and the supply chain of that product, in a manner which lets every individual that buys that product access it. This proposal is only conceptual and does not have a full implementation, but the authors identify four main strengths blockchain can provide to address these perceived risks:

- **Origin assurance:** This is the assurance that the claimed origin of the product is correct, whether it is the country or the region where the product originated.
- **Authenticity assurance:** This is the assurance that the product is actually produced and distributed by the brand that is displayed on the label.

- **Custody assurance:** This assurance involves traceability, in order to see who controlled of the product at every stage of the supply chain. This type of assurance is increasingly important as the complexity of supply chains increase with more steps in the supply chain.
- **Integrity assurance:** This is the assurance that the product lives up to the quality and reliability which has been promised by the company selling it. An example of this could be to assure that a type of food labeled nut-free contains no traces of peanuts.

Using blockchain to create assurance in this way is useful when provenance is lacking, and a company wishes to increase the consumers' perceived trust in their products. It can be especially useful in scenarios where trust is important, like for example pharmaceuticals or luxury items. The authors do not go into much detail regarding the implementation of this proposed solution, but make a few notes on important factors to consider when implementing the blockchain. Firstly, all actors in the supply chain need to agree on a blockchain and implement it together. Secondly, investments need to be made to lower the manual work required in the supply chain to record all the information. This would include sensors, surveillance, quick response codes, and so on. Third and final point, consumers need to understand and be able to access the information from the blockchain.

There might be risks involved for the companies to apply transparency through blockchain in this way. Firstly, this transparency can expose trade secrets, intellectual property, and supply chain details to competitors that might lead to a disadvantage. Secondly, transparency in this way can also lead to a public scandal if one is not completely sure that everything in the supply chain is done by the book. Information overload for the consumers might also be a challenge, so work done to discover what ways to display this information in a meaningful way also needs to be conducted.

Montecchi et al. [2019] is relevant to the current study because it identifies important factors that are the source of risk and uncertainty in supply chains for a consumer. The authors also present features in a blockchain-based supply chain that can address these sources of risk. This helps in understanding the current stage of blockchain-based supply chain solutions and what features that are considered important in systems like this. This is important information when working on developing similar solutions that are to provide the same assurances. In addition, this paper also provides a list of risks the consumers face in a supply chain. This helps understand what factors drive uncertainty for consumers when buying a product, this uncertainty is closely linked with trust. Therefore our work investigating trust in blockchain-based supply chain solutions builds on some of the elements related to risk and uncertainty from the study

by Montecchi et al. [2019].

### 3.1.2 How Transparency, Tractability, and Perceived Trust Affects Blockchain Adoption in Supply Chain

Yeh et al. [2019] is a paper covering the same field of research as the work presented in section section 3.1.1. The focus is on trying to develop a system of supply chain management, built using blockchain technology. The motivating factor behind the research is, also as in section 3.1.1, to use blockchain to give consumers information regarding the products they buy. This information can give insight into the origin, custody, authenticity, or other production details. This can be presented in order to help prevent agricultural fraud and increase food safety.

The authors of Yeh et al. [2019] investigate, through an empirical study, which of the benefits blockchain provides that can lead to an increase in purchasing intent from the consumers. Through the empirical study, a theoretical model prediction of the purchasing intent of a consumer is developed. This model is based on Unified Theory of Acceptance and Use of Technology 2 (UTAUT2), which is a framework for evaluating the acceptance of new technology [Tamilmani et al., 2021]. UTAUT2 is a modified version of an existing framework called UTAUT, which includes a new dimension of perceived trust. This perceived trust dimension, in addition to information transparency, is the most relevant to the work covered in this thesis. Two hypotheses centering on perceived trust and information transparency are presented in the paper:

- **H8:** Perceived trust related to the use of blockchain technology to trace food has a positive influence on purchase intention.
- **H9:** Information transparency has a positive influence on perceived trust related to the use of blockchain technology to trace food.

Yeh et al. [2019] collected through an online survey, it was 264 participants. Based on the findings in total 12 out of the 16 hypotheses were supported, the reminding 4 were not supported by the data. Both H8 and H9 were supported. It was also shown that there is a correlation between information transparency and perceived trust, and that in general information transparency leads to higher perceived trust.

The paper concludes by identifying 2 key aspects to succeed with blockchain technology in the supply chain. These 2 aspects are to get users to trust the system and technology, and for both consumers and companies to find value in using blockchain. The limitations of this work are that most of the patients did not have any experience with blockchain and hence there might be some participants that did not fully understand the underlying blockchain structure proposed in the new supply chain. Another limitation is that this

research was conducted in Taiwan, therefore it should be conducted further work to investigate if similar trends can be found in other countries and cultures.

Yeh et al. [2019] is relevant to the current study because it shows how perceived privacy, security and trust increase the intention for a user to adopt blockchain. It also shows how tractability and transparency increase the perceived trust in blockchain technology. This provides a basis for our investigation into drivers of trust in blockchain, but it is done as a qualitative study instead of a quantitative study. In addition, the conclusion of the paper where the authors present 2 factors to succeed with blockchain is an important motivator for this current study. Especially to get consumers to trust the system and technology is an important motivator for this study where the goal is to improve users' trust in blockchain, but also make them understand the benefits of the technology is also important.

## 3.2 Digital Trust in the Web-Based Applications

This section will present work related to RQ1 and RQ2. Studies that investigate what drives trust in web applications, how graphical factors affect trust, how trust relates to loyalty, and algorithm transparency will provide a basis for both the research design for this study, but also be used when discussing the findings of the current study.

### 3.2.1 Characteristics of a Perceived Trustworthy Web Application

The authors of Seckler et al. [2015] conducted an empirical study to better understand how website characteristics affect trust and distrust in users. The novelty of this work is that it measures what affects a user's trust and distrust in a website through a questionnaire. In this context, the website characteristics are graphics, structure on the site, pop-ups, or issues on the site, but can also be social factors like recommendations from a trusted peer.

The data in Seckler et al. [2015] was collected using an online survey with 27 questions about trust and distrust while using a website. In total there were  $n = 221$  participants, where  $n = 103$  participants answered questions based on a website they felt were trustworthy.  $n = 118$  answered the same questions, but describing an incident where they did not trust a website they were using. The technique used was the critical incidents method, where the questions started with the key items and had open-ended questions.

The website characteristics measured were graphic design, structure design, content

design, social-cue design, and personal and social proofs. Graphic design in this context elements like colors, fonts, or quality of the pictures on the site. Graphic design affected both trust and distrust but was more impotent for the users that experienced distrust. Examples of what lowered distrust were clashing colors and low-quality pictures. The dimension of structure design refers to the ease of browsing the website. This dimension had only an impact on trust in the sense that a well-designed and well-structured website felt more trustworthy to a user. Content design is a broad dimension ranging from information about what web protocol a site uses if two-factor validation was required, or logos of trusted third parties. This dimension was present in the answer of the users experiencing trust and distrust. Trust signals like logos of third parties were the most important factor to enhance trust, while data collection and secondary usage of the users' data was the most important for a user to lose trust in a website. Social cues were not an important factor for a significant number of participants. Finally, personal and social proofs like recommendations, ratings, and reviews were found to have no effect on the distrust users felt but did have an effect on users' trust in a webpage.

The implication of these findings is that if an entity wants to enhance the user trust on their web page, they should focus on improving the structure and the graphics of their site. They should also work on the content that strengthens the users' trust, like assurances that privacy is preserved or trust signals. Good usability and recommendations from other users also enhance a user's trust. To reduce the distrust in a website the number one is to make the graphical profile of the website look pleasant and professional. Not letting a second party use the users' data is also a major factor to limit distrust in a website. Trust, or distrust, in the brand itself is also important but requires a public strategy to change the public perception of the brand. This is not part of the scope of this work.

Seckler et al. [2015] concludes that this work helps expand the understanding of what elements and characteristics help enhance trust on a website, and what factors that reduce the trust a user has while visiting a website. This study shows that distrust is mostly affected by complex layouts, pop-ups, and design issues on the site. Trust on the other hand is more affected by social factors like recommendations or reviews. Content of the website can both reduce trust and enhance it. For example, did privacy issues lead to distrust, while security signs strengthen the users' trust in the system. The results of this work also show that distrustful experiences often occur with a lack of honesty and missing benevolence from the website owners, while trustful experiences are characterized by honesty and competency. Further work can be done to investigate in more detail what concrete content, graphical elements, trust signals, pop-ups, and so on had a positive impact on user trust. It would also be beneficial to analyze different types of websites individually, since there are different levels of privacy and security expected

to form different types.

This paper is relevant when studying and answering RQ1 because it identifies many of the elements that impact perceived trust for a consumer using a web application. The findings of this paper helped inform some of the design decisions for the prototype for the user tests. In addition, were the findings useful as a comparison to our own findings from the interviews. This was also a quantitative study, so our study can potentially add to the findings by conducting in-depth interviews and user tests.

### 3.2.2 Perception of Adequate Security and Privacy, and how it Increases Trust

In Flavián and Guinalú [2006] a study is conducted to analyze how perceived security and privacy affects a user's trust in a website. How this trust affects the loyalty to the website is also examined. The authors first define loyalty, trust, privacy, and security before discussing the relationships between them. The main part of the paper is to test the proposed hypothesis and discuss the results of the quantitative study that was conducted online by Spanish-speaking test subjects. A model that shows how privacy, security, and trust can lead to higher loyalty from the users of the website is derived from this work.

In this work, privacy is defined as an individual's ability to control the terms by which his personal information is acquired and used. Security in this paper refers to the technical aspects of providing integrity, confidentiality, authentication, and non-recognition of transactions. Even though there is overlap between privacy and security, the authors distinguish between them. In this paper, privacy is associated with what a company legally can do with a user's data, while security is associated with what technical implementations are being used to keep that user safe on that website. The authors specify that the users of a website often do not care about this distinction as long as their data is handled in a responsible way, either legal or technical. It is also worth pointing out that both the public and corporations tend to see privacy and security as one in the same.

The three working hypotheses of this study are:

- **H1:** The greater consumers' perception of security with regard to the handling of their personal data, the greater their trust in a website.
- **H2:** The greater the consumer's trust in a website, the greater the loyalty towards it.
- **H3:** Increased consumers' perception of security with regard to the handling of

their personal data will result in an increase in the loyalty shown to the website.

The results of the online survey conducted in Flavián and Guinalú [2006] clearly show that trust affects loyalty to a website. This has especially strong implementations for e-commerce companies that want a consumer to come back for more online shopping. The study also shows a clear link between the perceived privacy and security a user experiences on a website with how much trust they experience for the website and the brand. This means that the study validates all three of their hypotheses in that perceived security increases trust, trust increases loyalty, and that perceived security and handling of personal data increases loyalty.

From this conclusion, there are clear implications for businesses to increase the trust and locality of their customers by increasing perceived privacy and security. This increase in perceived privacy and security can be achieved through either legislation or through the adoption of technical systems that either preserve privacy or enhance security.

The authors point to several different directions for further research in this area. First, splitting the websites – especially the e-commerce sites – into categories to see if the requirements for trust to achieve loyalty from a consumer differs based on the type of site. For example, will the requirement for trust be greater for a financial transaction than for booking a train ticket online. Second, analyzing how perceived security affects the relationship a user has to a website. Meaning to analyze the broader relationship to understand for example how satisfaction relates to perceived privacy, security, and trust. Third, this paper is from 2006 meaning that this paper can be a bit dated since the development of the internet, wireless equipment, Wi-Fi, and so on has come a long way since then. Conduction a similar study to see if the findings still hold would be interesting, or to see what has changed now that users are much more technologically savvy. Finally, this study does not go into details regarding what specific elements enhance a user's perceived privacy and security. Studies revealing what elements lead to this prescription are also an interesting research direction. Is it for example brand recognition, trust signals, recommendations, privacy policies, or so on that leads to a website being experienced as trustworthy.

The work by Flavián and Guinalú [2006] shows that perception of good security and privacy increases trust. This is something that is investigated in this current study as well in the explanation of blockchain and zero-knowledge proof, and how these technologies increase security and privacy. Our study investigates in more detail how one can get a user to increase their perceived security and privacy when answering RQ2, something that is not fully studied in the paper. In addition, our study is qualitative meaning it is easier to get more detailed answers to what improves trust. Our study also addresses the limitation with this work mainly collecting data from e-commerce sites, this is done

by designing a user story not centered around an e-commerce site.

### 3.2.3 Algorithm Transparency and how it Affects Trust

Kizilcec [2016] conducts work to identify how transparency into how an algorithm produces its output affects the trust a user feels towards the output. The author points to the increasing rise in algorithms presence in every aspect of society, from recommendations in news feeds to machine learning in healthcare as motivation for why one should investigate what can enhance users trust in output from algorithms. The issues regarding the limited research and understanding of trust in algorithms are also pointed out. The related work has in particular been focused on the questions of why and how transparency changes trust, and the trade-off between competency, benevolence, and integrity. Some of the related work concludes that transparency increases trust, while others find no such correlation. The related work was also not tested in high-stakes environments, nor was it tested on different levels of transparency. Based on this motivation and the identified shortcomings of other work the author formulated 3 hypotheses:

- **H1:** Trust is lower if expectations are violated.
- **H2:** Changes in interface transparency affect trust depending on whether expectations are violated.
- **H3:** If expectations are violated, procedural transparency increases trust, but additional information about outcomes erodes this trust.

To measure how trust changed based on transparency and information about the algorithm, an experiment based on peer assessment in online courses was designed [Kizilcec, 2016]. How peer assessment works is that every student grades a number of  $n$  assignments, papers, or exams. This means each paper is graded by  $n$  other students. The simplest form of peer assessment is to take the median or mean of the grades and that will result in the final grade. Each student will also grade their own work. Using mean or median is a good approximation, but a tuned model proved to be more than 30% more accurate than mean or median. The algorithm behind this tuning is not as intuitive as median or mean, and the details are considered overwhelming to the majority of the users. Therefore most users still assume that the final grade is calculated using median or mean. The author argues that it is common that users makes wrong assumptions when presented with overwhelming information or lack of explanation, these assumptions are often the simplest way that system could work.

To be able to measure a massive open online course that used peer assessment as a grading method was used. In this class, each user graded  $n$  in addition to their own paper, and the final grade was calculated based on the tuned model. The class was



then split into 3 parts where they were presented with 3 different levels of transparency into the details of the algorithm. One group got a low transparency level, one group a medium and one group got a high transparency level:

- **Low:** This group was shown the text: “Your computed grade is  $X$ , which is the grade you received from your peers.” Where  $X$  is the final grade.
- **Medium:** This group got a more comprehensive explanation: “Your computed grade is  $X$  which is based on the grades you received from your peers and adjusted for their bias and accuracy in grading. The accuracy and bias are estimated using a statistical procedure that employs an expectation-maximization algorithm with a prior for class grades. This adjusts your grade for easy/harsh graders and grader proficiency.” Where  $X$  is the final grade
- **High:** Was presented the same as the medium transparency group, in addition to the raw data and how the calculations were done to reach the final score of  $X$ .

The users in Kizilcec [2016] were then asked to answer questions to understand how much trust they felt in the system, method, and output of the algorithm. The answers were recorded based on the transparency groups of the users, but also if the expectations were violated or not. If expectations were violated or not was decided by comparing the final grade with the grade the student gave them selfs. If the student had given themselves a better grade than the final grade expectations were considered violated, and otherwise expectations were not considered violated.

There were in total 120 participants. Out of this 120, 17 individuals did not complete the course of the grading so the data collected was from the reminding 103. There was 33% women and the average age was 37.15 years, based on self-reported information. 39 was placed in low transparency, 34 in medium transparency, and 30 in high transparency.

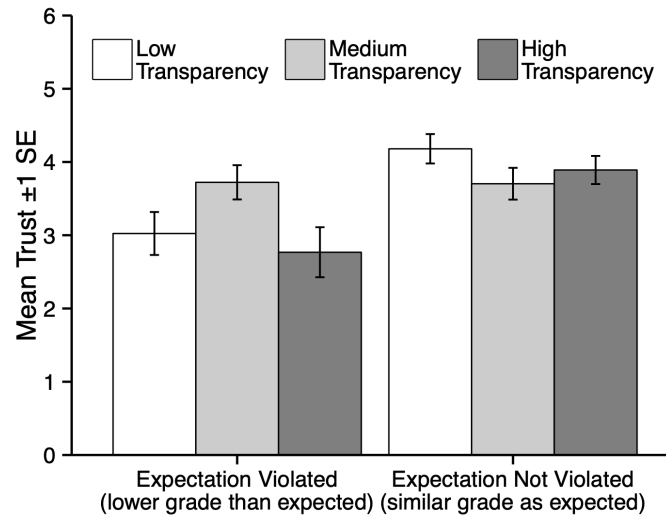


Figure 3.1: This figure shows trust in the 3 different levels of transparency for individuals that had their expectations violated, and and users that got the expected score, or better. This figure was retrieved form Kizilcec [2016].

Figure 3.1 presents the core findings of this study. One can clearly see that the overall trust of the individuals that had their expectations violated, was lower than the students that got their expected grades. The data also shows that the group with medium transparency had equal amounts of trust whether their expectations were violated or not. Both low and high transparency had lower trust than medium transparency if their expectations were violated. This was the opposite for the individuals that did not have their expectations violated. For that group, both low and high transparency had higher trust than medium transparency.

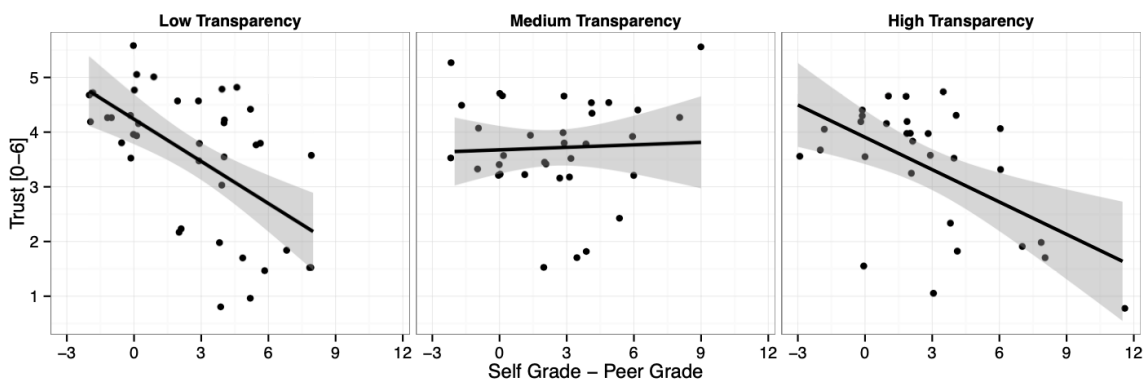


Figure 3.2: Shows how trust varies across the three categories dependent on how much the students expectation was violated. This figure was retrieved form Kizilcec [2016].

This trend is also clear when seeing that trust decreases as the difference between the

self-grade and the final grade increases for both the low and high transparency, while trust is more or less unchanged if compared to the same number, as shown in Figure 3.2.

Based on the findings there is support for H1, because the overall trust decreased when expectations were violated [Kizilcec, 2016]. It is also clear that trust varied based on transparency and interfaces when expectations were violated. Lastly, trust is again lowered for the high transparency group with expectation violation, which supports H3. The reason why the group that did not have their expectations violated had the same trends for trust for the 3 transparency levels, might be that if expectations were met their trust in the grading came from their own self-grading. A possible explanation for why the high does worse than the medium transparency when expectations are violated can be that the users have negative associations and feelings towards the low scores from their peers and therefore rate this lower. A system that does not show their raw data, but instead, a numerical example with dummy data can be used to test if this is the case.

This work has implications for interface transparency and algorithm understanding. The results clearly support the role transparency has on trust in algorithm decision-making. This shows engineers and designers that giving understandable details of how a system or algorithm produced an output may lower confusion and hence increase trust. Limitations of this work include a small number of participants, and the lack of interviews to get a better understanding of user experiences. Similar work should also be conducted in different contexts and different use cases to see if the hypotheses hold in other scenarios.

This paper is very relevant to RQ2 because it studies the same concept: how transparency into an algorithm or technology affects perceived trust. This study by Kizilcec [2016] served as motivation for the different levels of transparency into blockchain and zero-knowledge proof that is used in the design of the prototypes. The findings by Kizilcec [2016] are also used to discuss our findings when studying RQ2. Our angle is also a bit different since no expectations were violated in our user tests, and hence the hypotheses they use are a bit different from our research questions. Our study also expands on the findings by having a qualitative study instead of a quantitative one.

### **3.2.4 Privacy and Security as Drivers for a Users Perceived Trust in Blockchain**

Blockchain promises to revolutionize many online processes from finance to risk management through secure peer-to-peer transactions, distributed storage, and its immutability. Shin [2019] presents a heuristic approach to fill the gap in the literature regarding how security and privacy affect trust in blockchain systems, and again how this affects the user's intent to adopt this new technology. The motivation for this work is to better

understand what drives the adoption of the disruptive technology of blockchain and how an individual's perceived security, privacy, and trust influence this adoption.

Shin [2019] uses the Theory of Reasoned Action as a frame for the development of the hypotheses. This is a theory that addresses how behavioral intent is created based on subjective norms and human attitudes. It is especially useful when the goal is to describe user behaviors through belief and evaluation based on cognitive processes.

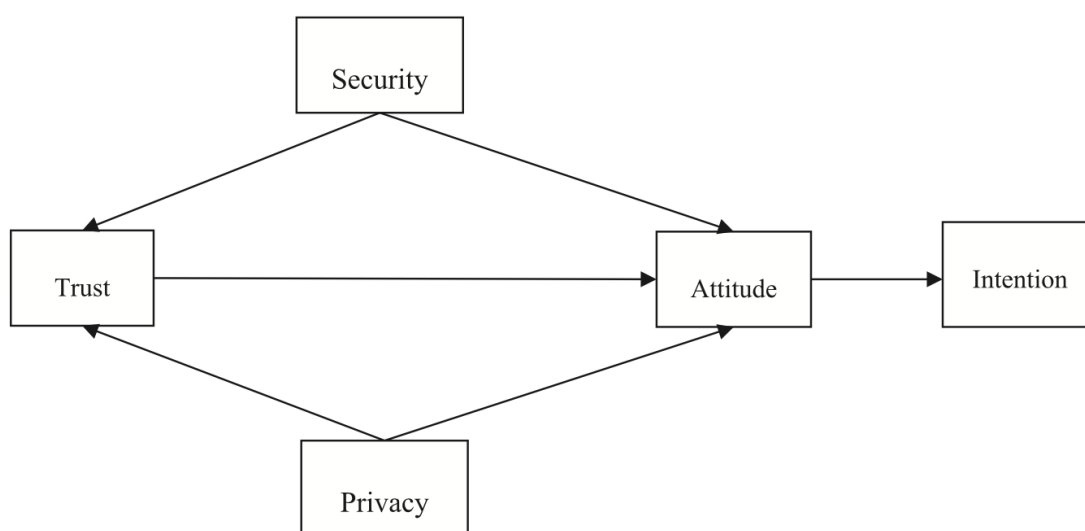


Figure 3.3: A model showing how security, privacy, trust, and attitude effects intention to adopt a new technology. This figure was retrieved from Shin [2019].

Figure 3.3 shows how intention is dependent on attitude, attitude is dependent on trust, security, and privacy, and trust is dependent on privacy and security. This is the model the author developed using the Theory of Reasoned Action, in order to evaluate what factors drive the adoption of blockchain. In this work security and privacy refers to perceived security and perceived privacy. This is a subjective value based on the individual's perceived security and privacy when using the given system and is different from the definitions of security and privacy from section 2.2. Shin [2019] developed 6 hypotheses:

- **H1:** Attitude toward blockchain has a positive influence on the intention to adopt blockchain.
- **H2:** Perceived security positively influences users' trust in blockchain.
- **H3:** Perceived security positively influences users' attitudes toward blockchain.
- **H4:** Perceived privacy positively influences users' trust in blockchain.
- **H5:** Perceived privacy positively influences users' attitudes toward blockchain.

- **H6:** Trust positively influences users' attitudes toward blockchain.

The data was collected using an online survey. In total there were 363 quality responses, and all were blockchain users. 94 users were under 20 years old, 170 between 20-35 years old, and 29 were between 36-45 years old. 52.2% identified as female and 47.8% identified as male. The survey consisted of 15 items measuring the 5 factors from Figure 3.3.

The data collected gave support for the 6 hypotheses, and thereby also gave support from the model presented in Figure 3.3. Security had a higher effect on trust than privacy. Trust's effect on attitude is strong, this shows that trust has a mediating effect on the relationship between privacy/security and attitude.

Due to the lack of research into the mass adoption of blockchain from users, this study provides useful and novel information [Shin, 2019]. The effect security and privacy have on trust, and how trust affects attitude and intention to use, was shown, giving a foundation of what drives users to trust and use blockchain. Implications of this work from a theoretical standpoint are that it helps better the understanding of how privacy and security effects trust. This will also have implications for the industry since the increase in trust and attitude also increases the user's intention of using the technology. Meaning that by increasing perceived security or privacy they can get more users for their blockchain solutions.

There are a few limitations of this work. Firstly, the population used to collect this data is already blockchain users and the vast majority are under 35 years old. This might be unrepresentative of the wider population, and different trends might be true for individuals that are unfamiliar with blockchain. Secondly, there might be paths that are crucial that are not included in Figure 3.3. An example of this could be that privacy and security affect each other, something that is likely, due to these two concepts being closely related. Thirdly, this work excludes possible external factors like platform or brand association. The impact of external factors like this should be investigated in further work along with addressing the other limitations mentioned above.

This study is interesting because there is limited research into perceived trust in blockchain and what factors influence this trust, and Shin [2019] attempts to fill this gap. The model presented in Figure 3.3, which can be viewed as a summary of the hypotheses that were confirmed, served as support when developing the interview guide. The findings from Shin [2019] were also useful when discussing our findings. Especially H6 was interesting because this confirmation indicates that trust influences a user's attitude towards blockchain, meaning that if one wants to develop a good attitude and adoption of blockchain, trust is an important factor. How this trust is developed for blockchain is both shown by Shin [2019] and in our study. Our study adds upon this work by includ-

ing many external factors in our interviews and user tests, our study is also qualitative giving a more in-depth understanding of the drivers of trust through semi-structured interviews.

### 3.3 Providing Privacy and Security in Blockchain Systems

Various papers and related work look into issues of handling blockchain data in order to preserve user privacy and maintaining various security aspects. This section is focused on two main ways of preserving privacy in blockchain networks, from two different angles.

#### 3.3.1 Off-Chain Data Storage

One of the more prevalent methods of preserving privacy in blockchain networks, which can be found in various literature, is storing the raw data in an off-chain database. The paper Kumar et al. [2020] describes a distributed model for electronically maintaining medical data, which includes patients' data, such as sensitive personal information, diagnostic reports, and doctor prescriptions. Seeing as the centralized storage model that is currently used, has a disadvantage of preserving user privacy, the paper proposes a distributed alternative. Threats related to patient privacy in a centralized model include unauthorized access of sensitive information and misuse of patients' data and medical reports. The proposed distributed alternative incorporates off-chain storage of medical data using IPFS (Interplanetary File System) and blockchain technology. The framework preserves patient privacy and facilitates easy access of medical data by authorized entities, such as healthcare providers. It also achieves consistency integrity and availability.

The underlying storage model for the framework is immutable and content-addressable. The goal is to be able to provide privacy for patient reports. The way this is achieved, is by dividing the framework into three modules, namely *data upload*, *mining process*, and *data storage*. Details about each patient is uploaded by the healthcare provider using a Web User Interface, and following that, the mining process is performed, which validates transactions and provides consistency in the network. Hash based data storage is then used to provide privacy of the patient diagnostic report.

The model, as presented in Kumar et al. [2020], consists of 5 steps, which are as follows:

1. The healthcare provider has to register in the consortium blockchain network, so

they can get the Proof-of-Identity.

2. Using a web interface, the healthcare provider uploads patient diagnostic reports.
3. The transaction, which consists of the uploaded report, is validated by miners using Proof-of-Work.
4. The transaction is then disseminated throughout the network by the miner, in order to verify the transaction.
5. The verified transaction is then stored in the IPFS distributed file storage system. In addition to this, the content-addressed hash value generated by the IPFS is stored on the blockchain in the network.

The transactions are only accessible by peers who have registered and gotten the Proof-of-Identity. Hospitals and doctors can only become part of the blockchain network after the peer registration process.

**Peer verification process.** Kumar et al. [2020] proposes an algorithm for handling the verification process by peers in the consortium network. The idea is to have the algorithm prevent malicious peers from accessing the shared documents. Proof-of-Identity is used to ensure security in the model. Peers registered in the network are provided a uniquely identifying Proof-of-Identity, which gets verified in authentication by peers.

**Data storage in the network.** The paper also presents an algorithm for storing the data in the network. A healthcare provider initiates the upload action, which adds the diagnostics report to the IPFS. Simultaneously the cryptographic hash value of the diagnostics report is added to the consortium blockchain. In order to identify the healthcare provider, mapping is performed.

There are two reasons why only the hashes and not the entire diagnostics report is stored on the consortium blockchain. The first reason is that storing the entirety of diagnostics reports would rapidly increase the size of the blockchain and cause a lot of storage issues. The second reason is that whenever peers arrive to the blockchain, they would have to copy the entirety of the chain and all the reports stored on it. This is not a scalable approach.

IPFS is used to handle the off-chain storage [Kumar et al., 2020]. IPFS is a distributed peer-to-peer hypermedia distribution protocol. The IPFS is used to generate a unique fingerprint of a file; The fingerprint is created by computing a cryptographic hash based on the content of the file. The unique hashes remove redundancy and are used for diagnostic report retrieval. The hashes also maintain privacy, by not storing the raw data directly on the blockchain.

The implementation model of the system can be divided into four main modules. Those are as follows: *healthcare provider*, *mining process*, *on-chain storage*, and *off-chain storage*. The implementation in the paper was done in *Python flask*, and it was implemented by using *core python module* by the *anaconda* open source distribution. The four modules used in the implementation can be described as follows:

1. **Healthcare provider:** This is the module which handles the collecting of patients' diagnostic reports. The diagnostic information details are collected by a healthcare provider, and is then uploaded to the network. The paper provides data based on the upload and download speed for various sized diagnostic reports and show that big files increase the computational intensity for uploads, to a much higher degree than downloads.
2. **Mining process:** The mining process module constitutes the consensus module in the implementation. This is when the block is created, which contains transaction details for each patient. The time taken for block mining and creation is detailed, and block mining takes more time than block creation for all file sizes.
3. **Off-chain storage:** This part of the module consists of the report being stored in the IPFS by one of the peers, and it receives the content-addressed hash in response to that. The hash can be used to extract this report from the IPFS.
4. **On-chain storage:** The on-chain storage module consists of the consortium blockchain itself. It stores the content-addressed hash which is received upon uploading a report to the off-chain storage. The blockchain maintains data consistency and includes a timestamp from the machine's internal clock, diagnostic report hash, patient detail hash, and subsequent block hash. Availability of transaction by peers was tested and the paper explains that access time increases as report size is increased.

The paper presents the design of a framework using consortium blockchain and IPFS based off-chain storage, in an effort to maintain patient reports. Only the hashes of the reports are stored in the blockchain, which means the framework can handle scalability well. The model is decentralized, which differs from the currently used centralized storage mechanism used among healthcare providers. The framework does not rely on a third-party, and it provides fair service to authorized peers.

Another framework for storing data securely off-chain is presented in the article López-Pimentel et al. [2020], presenting a blockchain network for avocado supply chain services. While the main motivating factor behind creating this framework, is that storing large amounts of data on the blockchain would require too much computational cost, it does overlap with concepts of preserving data privacy as well. The paper instead proposes a



hybrid solution, with an audit mechanism, that saves all the events of a supply chain within a blockchain in a hashed form. This is the first instance. In the second instance the users of the supply chain will be able to query integrity, data provenance and traceability to blockchain, using an intermediate server. The intermediate server establishes communication between the blockchain and the supply chain. The proposal has been validated with a proof of concept.

López-Pimentel et al. [2020] wants to provide an audit mechanism for the blockchain system. The presented approach is an integration of various emergent technologies. It primarily consists of a blockchain and a Supply Chain (off-chain), which are coordinated by a Server Blockchain Interface, which receives its data from each Server Supplier. The proposed model consists of three general parts:

- *The Supply Chain System*, compound by a set of Suppliers. Each supplier in the Supply Chain System stores all information of each part of the supply chain. It uses stored procedures to implement *Traceability*. The suppliers might store the information by using a traditional relational database. In the system, it is essential that Suppliers establish communication with *The Server Blockchain Interface*, in order to provide auditing and reliability.
- *The Server Blockchain Interface* is the name of the general controller of the model described in the paper. It interacts with *The Supply Chain System*, by attending requests and emitting answers. The data information is sent to each supplier and to the *Blockchain*, based on the instructions sent by *The Server Blockchain Interface*.
- The *Blockchain* is the last of the general parts. In the model it acts as a software connector. It is used to stored the hashing data, which is used to validate the information stored in the off-chain. *The Server Blockchain Interface* can be used to validate the off-chain, utilizing the hashing data stored on the *Blockchain*.

The blockchain model in this system requires a) to define the Users and Roles that will have access to the blockchain and b) the smart contracts and the different operations it will have.

The Supply Chain System contains its own type of users. Within the blockchain context the system has established a set of particular roles, which limits the operations that each user can execute. The roles are Root, Administrator and Transaction User. The operations are implemented as smart contracts, which are linked to the user. Each of the operations are linked to the interface operations in The Server Blockchain Interface, being *Storing()*, *Auditing()*, *Provenance()* and *Traceability()*. The operations are as follows:

- $createRoot(K_p^+)$ : Creates a root, using the public key  $K_p^+$ . This is created when the general system is started. The function interacts with the *Storing()* interface and can be executed by Root users only.
- $addAdmor(K_p^+)$ : This function adds an administrator  $K_p^+$ . The function interacts with the *Storing()* interface and can be executed by Root users only.
- $addWriter(K_p^+)$  and  $addReader(K_p^+)$ : These functions add a Writer or Reader respectively, with the address  $K_p^+$ . The function interacts with the *Storing()* interface and can be executed by Administrator users only.
- $i = setData(K_p^+, D)$ : This function adds data  $D$  to the blockchain, and identifies if the user  $K_p^+$  may execute this operation. The function interacts with the *Storing()* interface and can be executed by Transaction users only.
- $D = getData(K_p^+, i)$ : This function returns data  $D$ , if the user  $K_p^+$  may consult the register  $i$  in the blockchain. The function interacts with the *Auditing()*, *Provenance()* and *Traceability()* interfaces and can be executed by Transaction users only.

As most organizations were created prior to blockchain, their transactions tend to be natively executed via off-chain. Presented in López-Pimentel et al. [2020] is an audit mechanism which uses blockchain to audit supply chains, it consists of three parts: a) a supply chain architecture; b) a server blockchain interface; and c) a blockchain. The general proposal is saving all events of part a) within the blockchain in hashed form.

### 3.3.2 Zero-Knowledge Proofs in Blockchain

While keeping data stored off-chain does limit who can access it, it is not an entirely perfect way of maintaining user privacy in a blockchain system. If database data were to leak, data could easily be linked to users. Thus, in order to ensure a higher level of privacy other studies have looked into implementing zero-knowledge proof methods for ensuring transaction unlinkability. Ben Sasson et al. [2014] is an article published in the 2014 IEEE Symposium on Security and Privacy, which attempts to improve upon the privacy of Bitcoin specifically and blockchain technologies more generally. The paper constructs a full-fledged ledger-based digital currency with strong privacy guarantees. *Decentralized anonymous payment schemes* (DAP schemes) are formulated, and they enable users to directly pay each other privately. In practice this means that the origin, amount and destination of the payment is hidden, which differs from traditional blockchain schemes.

The first digital currency to be introduced and achieve widespread adoption was Bitcoin. However, one drawback to Bitcoin is the fact that its transactions are not anonymous

by using just Bitcoin itself. Due to this, users attempt to obfuscate their transaction history by using mixes. Mixes are pools, which users can pay into, then coins can be mixed and transferred to their destination, making it less traceable than normal transactions. However, mixes still have certain limitations: Firstly, the coin value transferred have to be of a certain size; Secondly, the mix itself can trace transactions; Finally, mixes can also steal coins from users. This makes the solution suboptimal for a range of use cases. Zerocash, as presented in Ben Sasson et al. [2014], is a framework which attempts to do away with the need for mixes, to ensure privacy and security of transactions. The paper explains how a digital currency can create a decentralized mix using zero-knowledge proofs to prevent transaction graph analyses.

Zerocash utilizes zkSNARKS, detailed in section 2.6.2, to guarantee a full-fledged decentralized electronic currency with strong anonymity guarantees. The paper introduces a decentralized anonymous payment scheme. For private transactions coins are minted by having users sample a random serial number and a trapdoor, which are then used to compute a coin commitment. A corresponding mint transaction is sent to the ledger and appended only if the user has paid 1BTC to a backing escrow pool. Mint transactions work as certificates of deposit and derive their value from the backing pool. Thus, anonymity is achieved because the users can say they know a computation of a commitment which appears in the list of coin commitments. This is a zero-knowledge construction.

In addition, coin commitments are compressed to ensure better scalability, as the space complexity of protocol algorithms grows linearly. Coin commitments corresponding to already spent coins cannot be dropped to reduce cost, because they cannot be identified, due to the privacy aspects of the system. A collision-resistant hash function is used to avoid an explicit representation of the commitment list. An append-only Merkle tree over the growing commitment list is maintained, in order to reduce the space complexity from linear to logarithmic. This exponentially increases the size of the commitment list.

In order to avoid making transactions only available for single coins, pseudorandom functions are used to target payments and derive serial numbers. This means users will not have to commit only single coins, and potentially committing multiple times for larger transactions. Minting is thus redesigned for greater functionality, allowing for transactions of custom amounts of coins.

Ben Sasson et al. [2014] also analyses the efficiency of the algorithms through large-scale network simulations. The results suggests Zerocash transactions may take longer to spread through the network and block verification takes more time, but block verification is not necessarily an issue, seeing as Zerocash transactions can not be spent before they

make it onto the ledger. Blocks being verified at each hop before being propagated through the network causes nodes to waste CPU-cycles by mining out-of-date blocks. This affects the computational power of the network, which makes it easier to mount "51% attacks", however it is unclear whether this is a real concern. The results of simulations in the paper show that users must wait only one block before spending received Zerocash transactions.

Ben Sasson et al. [2014] provides a scheme and framework for creating unlinkable transactions, based on Bitcoin. It implements algorithms and data structures in order to guarantee a high level of privacy and hiding transactions and amounts in the system. This could potentially be an issue, as it hampers accountability, regulation and oversight. Still, the underlying cryptographic proof machinery can support a wide range of policies in a given blockchain network. It can let users prove they have paid their due taxes on all transactions, without having to reveal transactions and their amounts, and not even the amount of taxes paid.

# Chapter 4

## Research Method

This chapter will explain the research method to answer the research questions presented in chapter 1. The study was based on design science, as described in Johannesson and Perjons [2014], and 3 steps were conducted as a part of the research method:

**Step 1:** An explorative study using interviews and user testing to investigate the drivers of digital trust, perceived privacy, and perceived security in a blockchain-based supply chain system to answer RQ1 and RQ2. There are in total 10 preliminary prototypes in step 1, where there are 4 prototypes for the provider of the good, and 6 prototypes for the consumer of the good in the supply chain. All showing different features to investigate what enhances trust for the user.

**Step 2:** Designing a new prototype, as well as implementing the actual function, privacy and features of desires based on the interviews to answer RQ3.

**Step 3:** A re-interview of the same users to collect their feedback on two new prototypes that has been updated based on the finding in step 1. Here there was one prototype for the provider and one for the consumer in the supply chain.

These steps are explained in detail in this chapter.

### 4.1 Explorative Study to find Drivers of Trust

In this section, the research method details and data collection for step 1 of user testing are explained. Step 2, where the new prototype and the system was designed is based on the results found from the first step, which will be detailed in this section. The user tests are conducted using semi-structured interviews with a set of candidates. The interviews consist of a semi-structured conversation with the interview objects to uncover how they develop trust in technical systems. The user tests consisting of 10 clickable prototypes

are a big part of the interview where the interview objects to test and give their feedback on perceived trust on each of the prototypes. The goal of the user testing and interviews was to talk to potential users of a system built on blockchain, and attempt to gain a better understanding of what type of information, and trust signals, they would need in order to trust that their security and privacy are preserved. These prototypes are designed to help answer RQ1 and RQ2, and the foundation for many of the design decisions for the prototypes was based on the related work presented in chapter 3. This section consists of five main parts: The first part will provide researcher motivation for this interviews and user tests; The second part of this section will introduce the use case, as well as the different actors involved in the use case; The third part of this section will lay out the details and features of the proposed system. The fourth part will explain how the interactive prototypes were developed and how they differ from one another; Finally, the last part will explain how the interviews and the user tests were conducted and how data was collected and organized.

### 4.1.1 Research Motivation

The main objective of these interviews and the user testings was to collect data that can help answer the two research questions in this thesis:

- **RQ1:** What is important to a non-technical user when evaluating if a technical system is trustworthy?
- **RQ2:** What is the best way to explain a technical system to a user, to assure them that their security and privacy are preserved when using the system?

In this context, a technical system means a system that was built using new, or complex, technology which was unfamiliar to most of the potential users. Examples of this type of technology could be cryptography, blockchain, or machine learning. These research questions can help fill some gaps in the state of research into digital trust. RQ1 will add on to the findings from Seckler et al. [2015], Flavián and Guinalú [2006], and Shin [2019] where the goal was to find factors in digital spaces that affected perceived trust for users. The same was the objective of RQ1 where the goal also was to understand what the drivers of trust for consumers using technical systems. The main way RQ1 differs from those studies is that they are quantitative while ours was qualitative as well. Both methods have strengths and weaknesses, and this is the reason why our method adds to the findings of those studies. By using quantitative and qualitative analysis with interviews and rating of trustworthiness, we were able to get a sense of what prototype enhances trust best and to get more detailed answers by asking follow-up questions when interesting elements are mentioned. This gave data that is better suited to find the underlying factors of trust development like a user's feelings, their associations, and

other factors that are hard to capture in a survey. RQ2 on the other hand was filling a gap in current, more so than adding on current research. There was little research into how transparency into the technical details, the workings of an algorithm, or system explanations affect a user's trust in the system. Kizilcec [2016] is, to our knowledge, the only study that investigates this topic. This was also a quantitative study, and our research provides a qualitative expansion of some of the findings. In addition, Kizilcec [2016] only studies transparency into a pretty simple algorithm to calculate a score and not a complex solution like blockchain or zero-knowledge proof. The study also focuses on how to enhance trust when expectations are violated, while our work focuses on how to develop trust in a system and technology through explanations of the system. Kizilcec [2016] also focuses on measuring 3 levels of transparency and how that affects trust, not necessarily how the explanation itself affects trust. To the best of our knowledge, there are no studies investigating a user's preferred way to be explained a technical system to increase their perceived trust in system security and privacy, making RQ2 novel. Many studies focusing on digital trust studies e-commerce sites, our study focuses on blockchain usage in supply chain systems. When evaluating the data collected the results will be discussed based on the related work presented in chapter 3 and the model for digital trust presented in section 2.1 and the conceptual model for trust presented there.

### **4.1.2 Use case: Fairtrade**

The use case presented in the interviews and user tests focuses on the concept of Fairtrade by Fairtrade-International. Fairtrade is a non-profit organization which provides certification to products which pay their workers fair wages during production. Examples of such products are for instance cotton, coffee, or vegetables. The organization of Fairtrade serves as a trusted third party, to assure the end consumers that the premium prices they pay for a product actually goes towards a higher wage for the workers, and does not end up as profit for investors.

#### **Fairtrade - Status Quo**

If we take coffee as an example, we can describe a simplified system model, consisting of four main actors participating in the process of harvesting, distributing, and consuming the product, all serving different roles and purposes within the ecosystem.

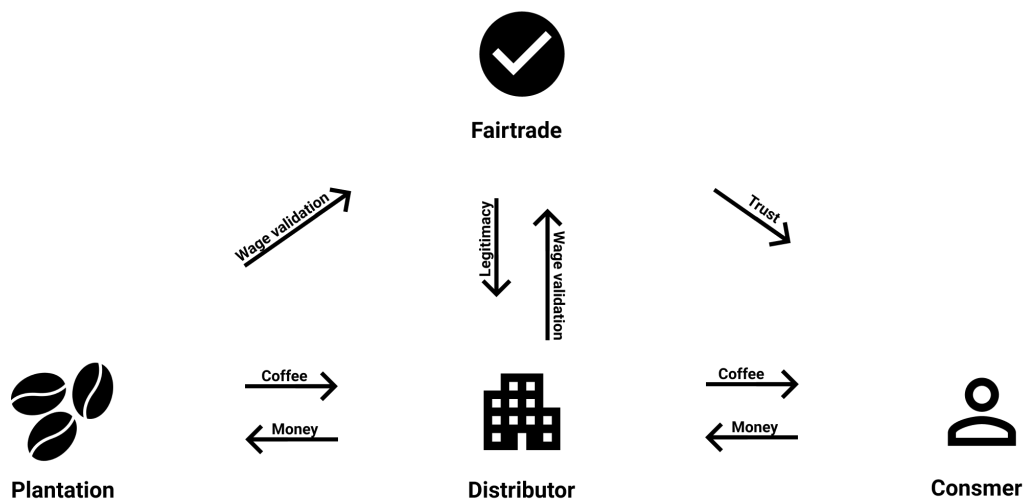


Figure 4.1: This figure illustrates how the four parties interact with each other, and how money, trust, information, and coffee flow in the ecosystem.

The four parties interacting in Figure 4.1 are as follows:

- Plantation:** This is the party responsible for harvesting the coffee, and which should be receiving a fair wage from the distributors. What is determined as a *fair wage* is decided by what is considered a living wage in the country where the worker operates, the global coffee market, and Fairtrade's guidelines.
- Distributor:** The distributor is the party which buys, roasts, and distributes the coffee to the consumers. This party has an economic incentive to label their coffee as Fairtrade, because this means they can usually put a markup on the products they sell. Additionally, the distributors have an economic incentive to pay the lowest price to the plantation workers as possible, in order to yield higher profit margins.
- Consumer:** This party is the endpoint for the coffee in the ecosystem. Examples of potential consumers could be a household, a hotel, or a university campus. When a consumer pays a premium price for a Fairtrade certified product, it is assumed that an important factor to them in this purchase, is ensuring that the markup actually goes to the plantation worker and not the distributors in the system.
- Fairtrade:** This is the fourth and final party in the ecosystem, and their work is to certify products and thus applying the Fairtrade label. This label signals to the consumers that the Fairtrade organization ensures that the workers harvesting coffee get paid fair wages for their labor. From the perspective of the consumer party, Fairtrade serves as a trusted third party which has systems in place to control



that this claim is legitimate. For the distributor in the ecosystem, Fairtrade is a well-known certifier that consumers mostly trust, which in turn gives the product legitimacy in the market and can therefore make it easier to sell.

### Fairtrade - Blockchain

In this thesis, the use case for data collection, attempts to utilize a blockchain and zero-knowledge proof system to replace the need for a Fairtrade organization certifying the products. The technical system details are explained and expanded upon in section 4.3. By eliminating the need for an organization like Fairtrade to certify a product, the actors' requirements in the ecosystem will be changed as follows:

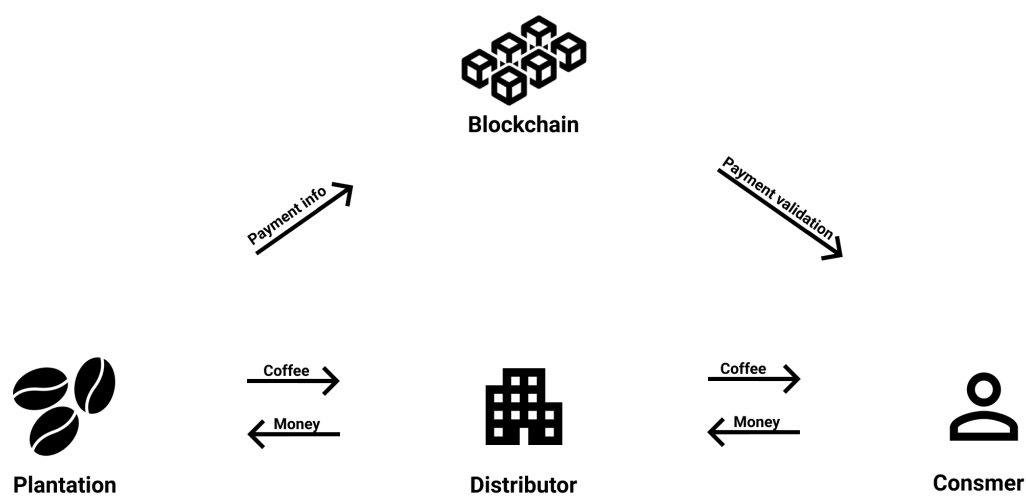


Figure 4.2: This figure shows how the system from Figure 4.1 can look if the trust from Fairtrade is replaced by an immutable blockchain ledger. Notably the Fairtrade party is removed entirely from the ecosystem.

The new model of the ecosystem, presented in Figure 4.2, now contains one less party and a blockchain model instead. In this new ecosystem model, the parties now interact as described below:

- **Plantation:** This party, consisting of the workers, now self-report what they get paid by the distributor per kilogram of delivered coffee. This data is stored on the blockchain, which ensures that it is immutable. The plantation workers would want to stay anonymous and have their privacy preserved, to make sure they do not face consequences from the distributors if they whistleblow about unfair payment for deliveries.
- **Distributor:** In this new ecosystem model, this party serves pretty much the same function and has the same needs as described in section 4.1.2. The main difference

this time, is that the validation that their workers are paid fair wages is provided to the consumers directly from a technical solution, instead of by a trusted third party.

- **Consumer:** The party of the consumer, instead of relying on the well-known logo of Fairtrade, would in this case have to use an input code or scan a QR-code on the product packaging. This code would then link them to the blockchain system and let them query the data directly from the distributed ledger. This would then result in output with information about the trade which has occurred in the ecosystem, and whether the workers were paid a fair wage for their labor or not. In this new ecosystem model, the user would have to trust the immutability of the blockchain network instead of the trusted third-party actor.

This ecosystem illustrated here was the basis for the prototypes that were developed for the user tests and interviews. It also served as the foundation for the technical solution that is presented in section 4.3. This system has some simplifications and assumptions, which were made in order to limit both the scope of the interviews and to be able to propose a minimum viable product.

### 4.1.3 Development of Clickable Prototypes

Based on the use case explained in section 4.1.2, a total of 10 prototypes are developed in the design software Figma. This is a software that makes it possible to create clickable high-fidelity prototypes, which are well suited for user tests in order to receive feedback, before starting to develop the system. The 10 prototypes which are created at this stage of the research, are an aid in helping answer RQ1 and RQ2, described in chapter 1. These 10 prototypes will help answer RQ1 and RQ2 by providing something graphical and concrete the users can use as a basis for their experience of trust. Since trust is subjective and very dependent on the context, it would be hard to have the interview objects just talk freely about what they perceive as trustworthy and not. The prototypes present different information and trust signals, and the interview objects comment on these elements as they click through the prototypes. This helps to make sure that each interview object comment on each of the elements that we want to check if affects trust. This semi-structured form of interviews based around the user tests of the prototypes provides a lot of feedback to answer RQ1, because the interview objects reflections on trustworthiness for each of the prototypes gave a varied and rich list of elements that affected trust for a user. The users were also asked to rate the prototypes from the most to the least trustworthy way of explaining the technical system. This rating helped answer RQ2 because it gave a way of measuring the preferred way to have the system details explained to enhance trust. This rating was complemented by more comprehensive

explanations and justifications for the answers given by the interview objects during the interviews which added to the overall understanding of the user's preferences for a technical explanation.

These 10 prototypes are split into two main groups. The first four of the prototypes are created for the data provider side of the system. The data provider refers to the farmers (the plantation party in the ecosystem) uploading the information about payment and deliveries. The remaining six prototypes are developed for what is referred to as data consumers. The data consumers refer to the users buying coffee (the consumer party in the ecosystem), who are querying the blockchain data to make sure fair wages were paid for the product.

When developing the prototypes the user tests, the prototypes, and interview questions were first tested in pilot interviews to make sure they were intuitive, that they stimulated the right type of conversations for the case, and that they did not have errors that would affect the flow of the user tests and interviews. This first round of pilot interviews was conducted on  $n = 3$  individuals after the first round of prototype and interview development. The questions and prototypes were edited and improved based on findings in these pilot interviews. After re-evaluating the prototypes and interviews, they were tested once more on  $n = 3$  new individuals. This time only minor errors and flaws were detected. These flaws were then addressed and then user tests proceeded with data collection for the study.

### **Features and GUI Developed for Data provider**

The core functionality of the four prototypes developed and tested for the data providers was the same. They all provide the test subjects with a form, consisting of three input fields and a submit button. Based on the use case, simplifications, and assumptions described in section 4.1.2, the 3 input fields are the weight for delivery in kilograms, the payment received for the delivery in dollars, and the plantation name. The information is then submitted by the plantation worker, and uploaded to the blockchain. The individual identity of the data producer is kept anonymous using a blockchain system with an off-chain database storage and a zero-knowledge proof implementation to ensure unlinkability of data transactions. The technical details are further expanded upon and explained in section 4.3. These four prototypes differ in the way in which they present information regarding what technology was used and how this affects ones security and privacy. This helps collect data, which can contribute to answering research questions 1 and 2. These prototypes let the interview objects compare the different ways of explaining the system, but also served as a basis for a discussion regarding what sort of presentation or additional information they require in order to experience blockchain system as trustworthy. This table shows an overview of the 4 prototypes designed for the

data providers:

Prototypes	Brief explanation	Logos	Graphical explanation	Written explanation
Prototype 1.1	-	-	-	-
Prototype 1.2	Yes	Yes	-	-
Prototype 1.3	Yes	Yes	Yes	-
Prototype 1.4	Yes	Yes	-	Yes

Table 4.1: This table shows an overview for what features prototypes 1.1-1.4 provides for the users. Brief explanation refers to a short written explanation of the system show at the first page for the users. Logos refers to logos and icons for companies and trusted third parties. Graphical and written explanation refers to a more detailed system explanation, explained by figures or words respectively.

Here is a more detailed presentation of the graphical user interfaces of the 4 prototypes show to the interview objects during the user tests for the data provider:

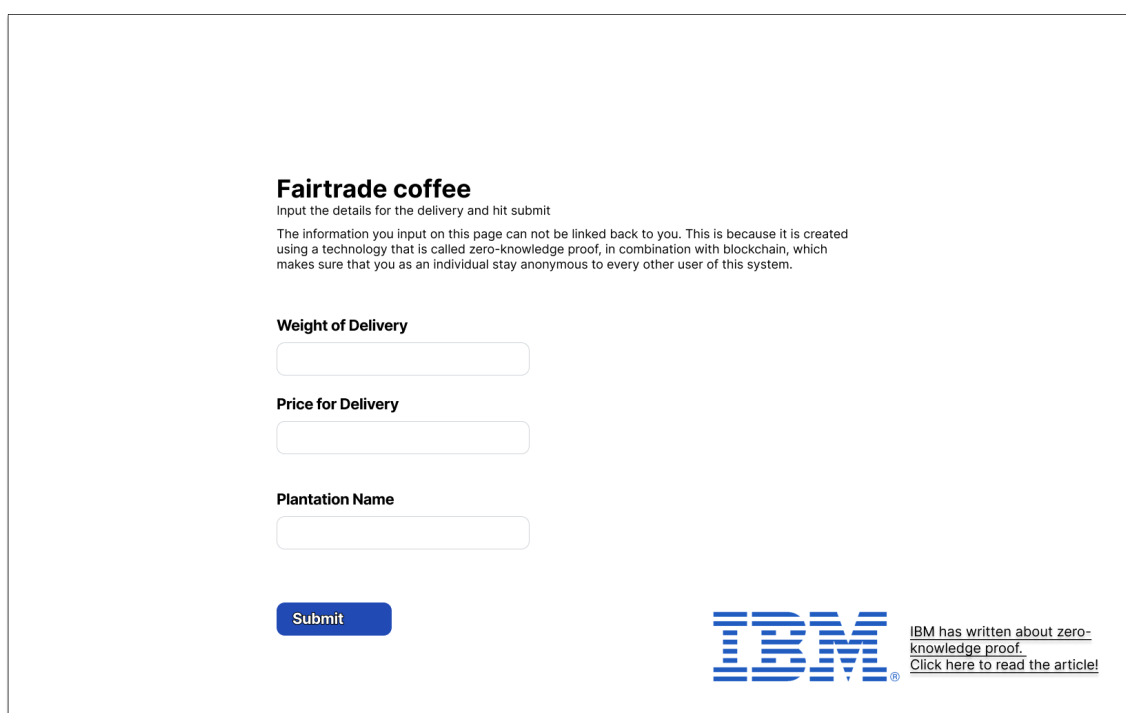
### Prototype 1.1

The screenshot shows a web form titled "Fairtrade coffee" with the subtitle "Input the details for the delivery and hit submit". The form contains three input fields: "Weight of Delivery", "Price for Delivery", and "Plantation Name". A blue "Submit" button is located at the bottom of the form.

Figure 4.3: Prototype 1.1: The simplest of the four prototypes developed for the data provider.

The first prototype shown in Figure 4.3 was the simplest of the four prototypes developed and presented to the interview objects on the data producer side. It simply consists of the input fields, a submit button, and finally a confirmation that the transaction has been completed, which was displayed to the user after they clicked the submit button. This prototype was developed to see how the users react when there is no information and no graphical elements enhancing trust. It serves as a baseline where the interview objects can reflect on what they would want to see to trust the system more. It also serves as a good comparison to the 3 other prototypes when discussing what features enhance trust for a user. Kizilcec [2016] slip their ways of presenting algorithms into low, medium, and high transparency. We have done something similar with these 4 prototypes where this would represent the low transparency into the technical aspects of the system.

## Prototype 1.2



**Fairtrade coffee**  
Input the details for the delivery and hit submit

The information you input on this page can not be linked back to you. This is because it is created using a technology that is called zero-knowledge proof, in combination with blockchain, which makes sure that you as an individual stay anonymous to every other user of this system.

**Weight of Delivery**

**Price for Delivery**

**Plantation Name**


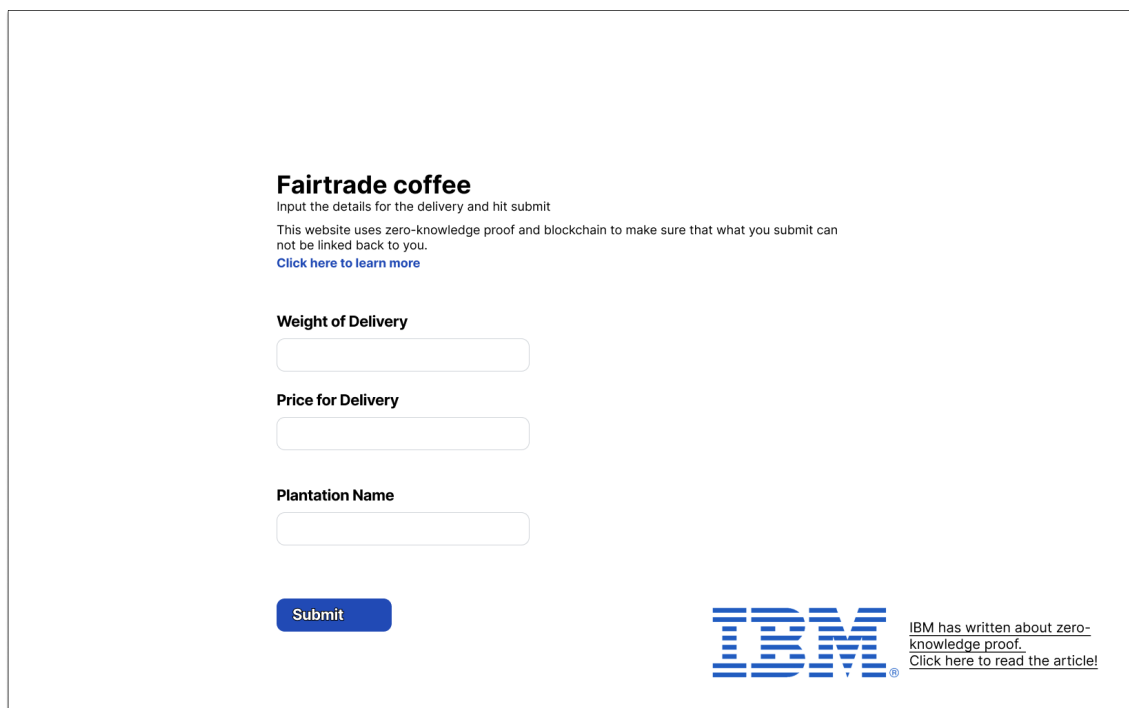
 [IBM has written about zero-knowledge proof. Click here to read the article!](#)

Figure 4.4: Prototype 1.2: An assurance of the type of privacy-preserving technologies used in the system was provided to the users in this prototype. An icon, as well as a link to an external article about the technology was also added.

The second prototype, as shown in Figure 4.4, was developed for the data providers and has a short paragraph assuring the user that their privacy and security is preserved through the use of zero-knowledge proof and blockchain. The users are invited to simply accept this statement as true. In addition to this paragraph, the logo of IBM was added

along with a link to a blog post on their website describing the concept of zero-knowledge proofs [Jones, 2019]. Adding a well-known logo was done based on findings from Seckler et al. [2015], where one of the conclusions was that logos from trusted, or well-known, companies could increase perceived trust. The reason why logos were added was to test if this increased trust. Based on findings from Seckler et al. [2015] logos, icons, and trusted third parties enhance trust. By adding the logo from a well know company we could test if brand familiarity increased trust, but also if links to articles written about the same technology by this trusted third party bettered the sense of trust for the interview object. Flavián and Guinalú [2006] discusses how trust increases if the user feels their privacy and security is handled well, based on this we add a sentence saying that their stay anonymous in the system to see if this affects trust for the interview objects. Again Kizilcec [2016] splits their test algorithms into low, medium, and high transparency. Prototype 1.2 will be similar to medium transparency into the technical details of the system.

### Shared GUI for prototypes 1.3 and 1.4



The screenshot shows a web form titled "Fairtrade coffee" with the following elements:

- Title:** Fairtrade coffee
- Instruction:** Input the details for the delivery and hit submit
- Disclaimer:** This website uses zero-knowledge proof and blockchain to make sure that what you submit can not be linked back to you. [Click here to learn more](#)
- Form Fields:**
  - Weight of Delivery:
  - Price for Delivery:
  - Plantation Name:
- Submit Button:** A blue button labeled "Submit"
- Logos and Links:** The IBM logo is displayed on the right side, accompanied by the text: "IBM has written about zero-knowledge proof. [Click here to read the article!](#)"

Figure 4.5: This display was the same for both Prototype 1.3 and 1.4.

Figure 4.5 presents a display that was used both by prototypes 1.3 and 1.4. The difference will be shown when the user clicks on "Click here to learn more". This display provides the same icons and logos as in prototype 1.2 along with a very brief explanation of what

technologies have been used and what they provide. Having more detailed information be provided if the user clicks on "Click here to learn more" was inspired by Kizilcec [2016] where the author said that providing more information to the users that that looks for it can work trust increasing. The logo of IBM was the same as in prototype 1.2.

### Prototype 1.3

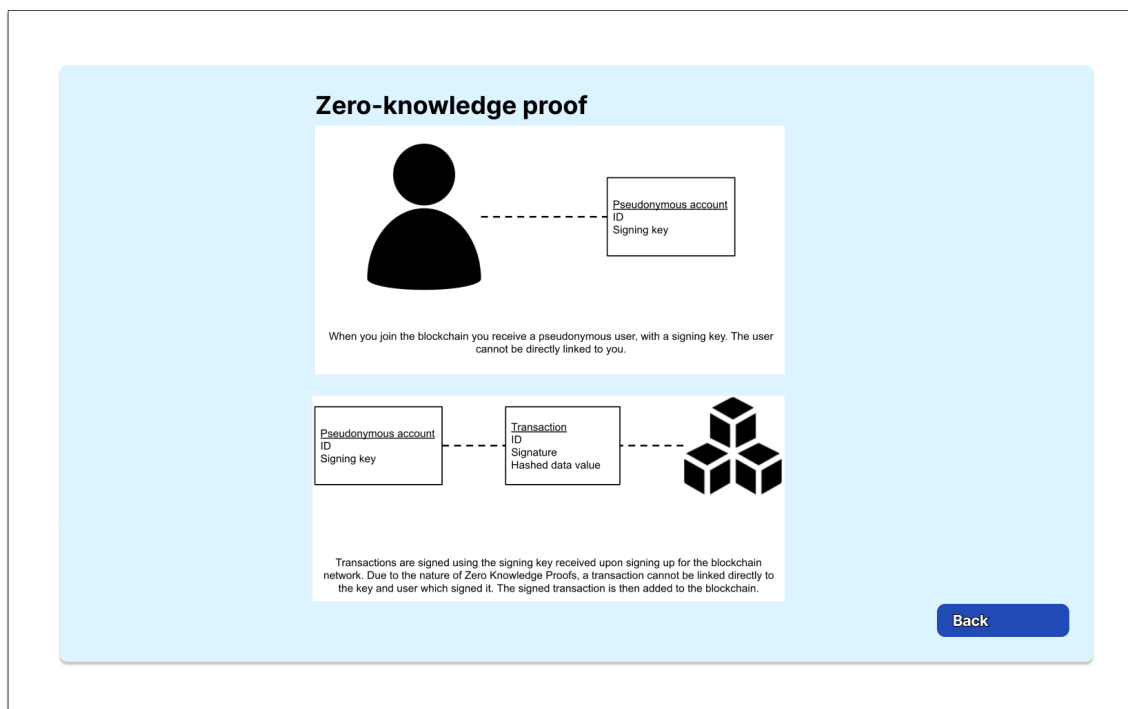


Figure 4.6: Prototype 1.3: Showing the pop-up presented in the third prototype if the user clicks on "Click here to learn more" in Figure 4.5.

The third prototype shown in Figure 4.6 shows the pop-up if the user clicks on "Click here to learn more" shown in Figure 4.5. This pop-up aims to explain the system in a graphical manner. The users were asked to overlook the low fidelity of the graphics due to this not being an important aspect of the study. Again Kizilcec [2016] splits their test algorithms into low, medium, and high transparency. Prototype 1.3 could be similar to something in between medium and high transparency into the technical details of the system. The main reasoning for providing a prototype explaining the technology graphically was to see if this way of explaining a system was trust enhancing or not.

## Prototype 1.4

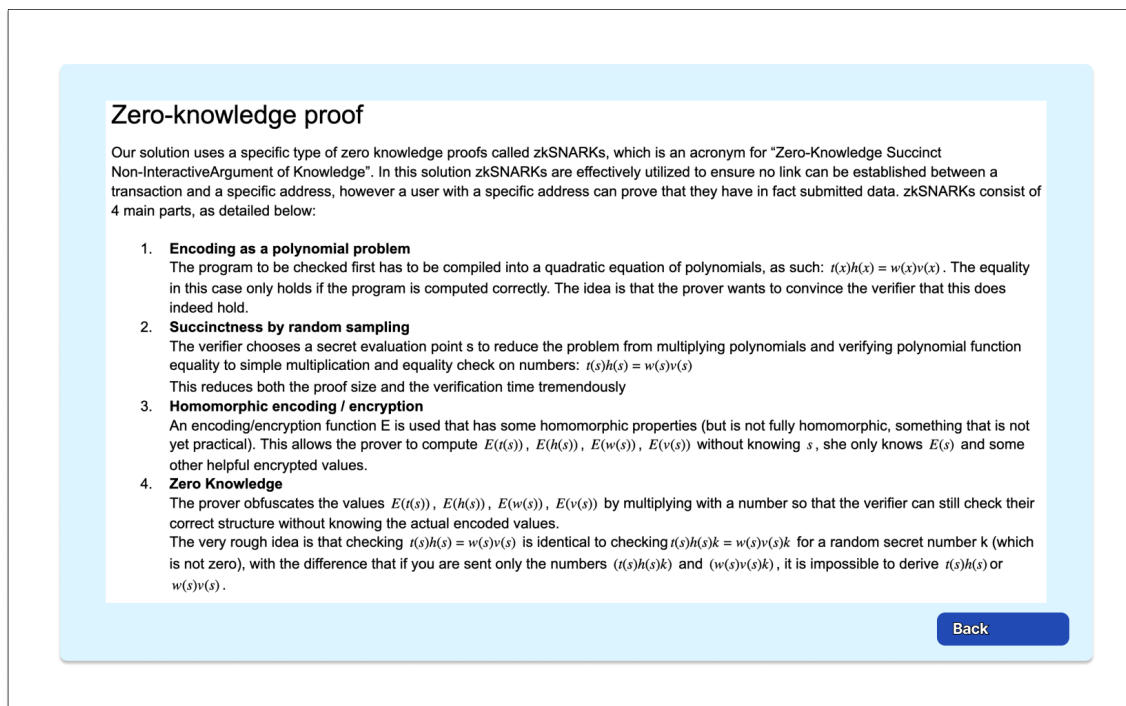


Figure 4.7: Prototype 1.4: Showing the pop-up presented in the fourth prototype if the user clicks on “Click here to learn more” in Figure 4.5.

The third prototype shown in Figure 4.6 presents this pop-up if the user clicks on “Click here to learn more” in Figure 4.5. The explanation of zero-knowledge proof was not explained using graphics and a flow chart as in prototype 1.3, but instead through a more technical and detailed description of the maths and logic of the system. This is a more mathematical description, and also a four step walkthrough was presented. Again Kizilcec [2016] splits their test algorithms into low, medium, and high transparency. Prototype 1.4 will be similar to high transparency into the technical details of the system. The main reasoning for providing a prototype explaining the technology graphical was to see if this way of explaining a system was trust enhancing or not.

Links to the four prototypes for the data providers can be found in the appendix found in section A.1. These prototypes are the same ones that were used for the user test. They are clickable and interactive.

## Features and GUI Developed for Data consumer

In this use case the data consumer is the individual or institution buying coffee. They consume the blockchain data by querying it to make sure that the plantation workers



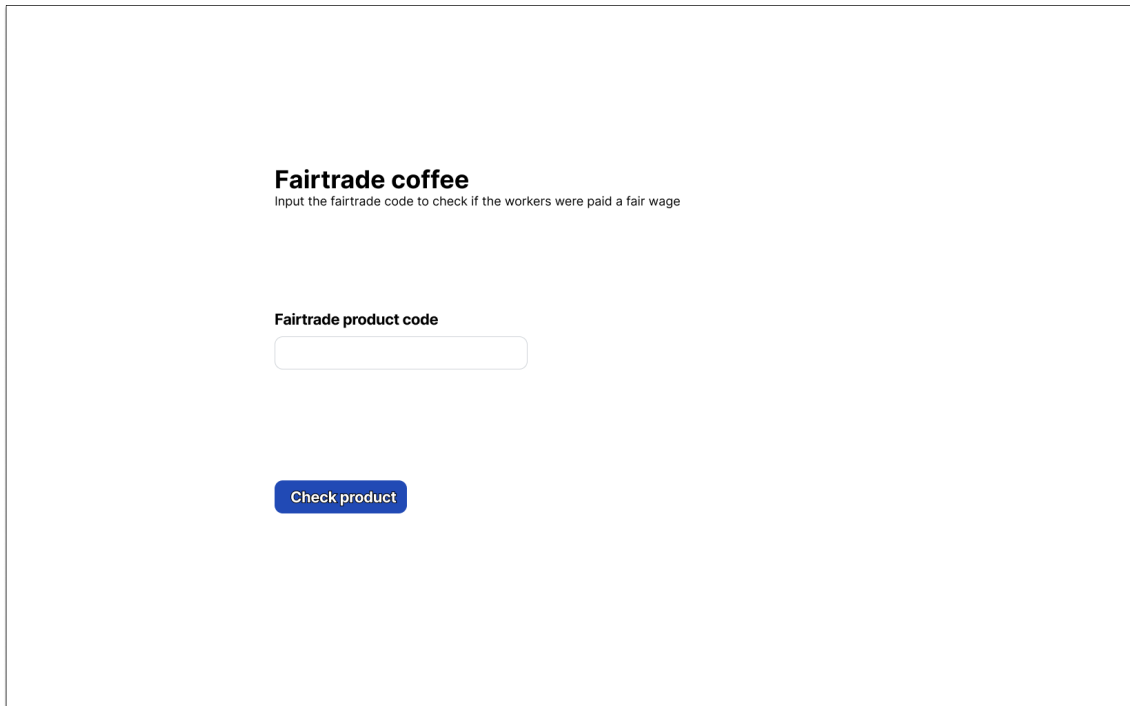
are being paid fairly for the coffee they harvest. In the prototypes, it was thought that the users would input a code provided product into a text field and hit a button to query the blockchain data, but it could also be developed using a quick response code or a bar code. All six prototypes have the functionality of taking a code as input and outputting whether or not the plantation workers were paid fairly. This table shows an overview of the 6 prototypes designed for the data consumer:

<b>Prototypes</b>	<b>Brief explanation</b>	<b>Logos</b>	<b>Graphical explanation</b>	<b>Written explanation</b>	<b>Blockchain hash value</b>	<b>Blockchain transaction</b>
Prototype 2.1	-	-	-	-	-	-
Prototype 2.2	Yes	Yes	-	-	-	-
Prototype 2.3	Yes	Yes	Yes	-	-	-
Prototype 2.4	Yes	Yes	-	Yes	-	-
Prototype 2.5	Yes	Yes	-	Yes	Yes	-
Prototype 2.6	Yes	Yes	-	Yes	-	Yes

Table 4.2: This table shows an overview for what features prototypes 1.1-1.4 provides for the users. Brief explanation refers to a short written explanation of the system show at the first page for the users. Logos refers to logos and icons for companies and trusted third parties. Graphical and written explanation refers to a more detailed system explanation, explained by figures or words respectively. Blockchain hash value refers to it being a hash value show to the user. Blockchain transaction means that the transaction for the given data was shown to the user.

Here is a more detailed presentation of the graphical user interfaces of the 6 prototypes show to the interview objects during the user tests for the data consumer:

## Prototype 2.1



**Fairtrade coffee**  
Input the fairtrade code to check if the workers were paid a fair wage

Fairtrade product code

Check product

Figure 4.8: Prototype 2.1: The simplest of the six prototypes for the data consumers.

This first prototype shown in Figure 4.8 does not have any information about how the system works. The user just inputs the code into a text field, hits submit and gets output that the plantation workers were paid fair wages. This prototype was developed to see how the users reacted when there was no information and no graphical elements enhancing trust. It served as a baseline where the interview objects can reflect on what they would want to see to trust the system more. It also served as a good comparison to the 5 other prototypes when discussing what features would enhance trust for a user. Kizilcec [2016] split their ways of presenting algorithms into low, medium, and high transparency. We did something similar with these 4 prototypes where this would represent the low transparency into the technical aspects of the system.

## Prototype 2.2

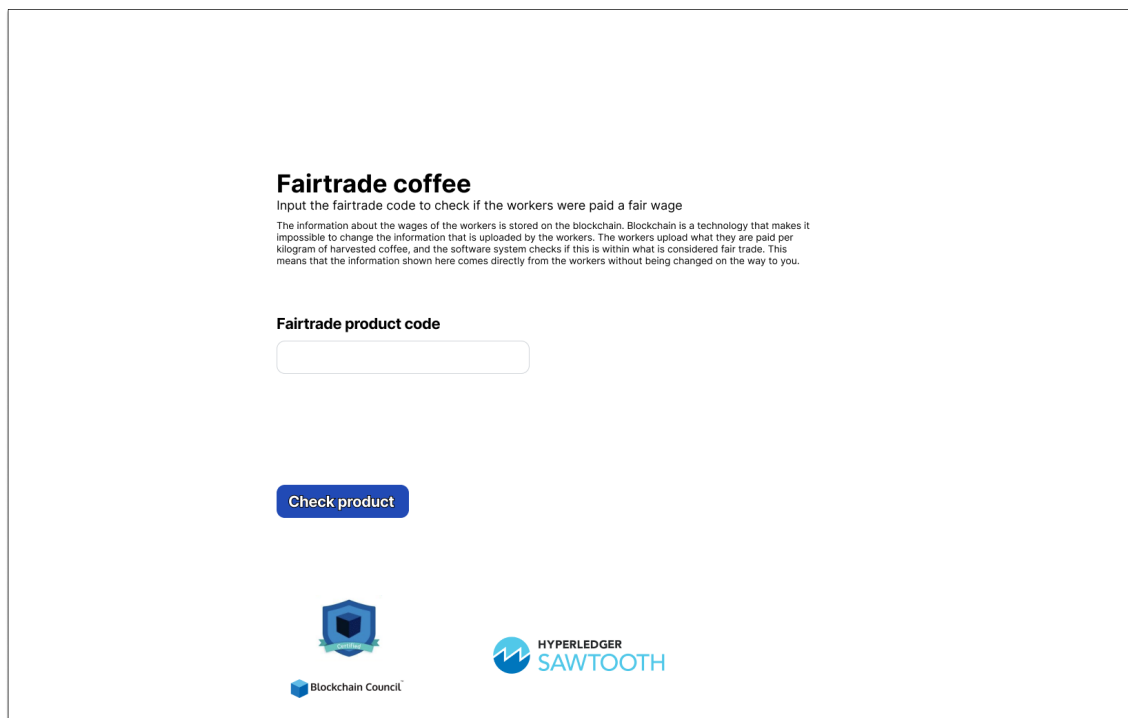


Figure 4.9: Prototype 2.2: An assurance that the data was tamper-resistant and that blockchain was used is presented in this prototype.

In the second prototype shown in Figure 4.9 there was a paragraph presented above the input field giving a short explanation of blockchain and how it provides tamper-resistant data. The user gets the same confirmation as in prototype 2.1 when they submit the query for the blockchain data. In addition, logos are added. One logo is from Hyperledger Sawtooth, which is a blockchain framework provided by the Linux Foundation [Hyperledger-Sawtooth, 2019]. The second logo is from the Blockchain Council with an icon saying “Certified” [Blockchain-Council].

Adding logos and icons was done based on findings from Seckler et al. [2015], where one of the conclusions was that logos and icons enhanced trust. One of the reasons why logos were added was to test if we could validate. Compared to the use of IBM in prototypes 1.2-1.4 these logos was less known, and did not provide a link to an article where more details could be found. This was done to see how well-known logos differed from lesser-known logos when a user decides if a system is trustworthy or not. Hyperledger Sawtooth was not self-explanatory, while the certification from Blockchain Council can be somewhat self-explanatory. These two different logos were added to see if the difference between them in self-explanatoriness had an impact on trust. Flavián and Guinalú [2006] discusses how trust increases if the user feels their privacy and security

is handled well, based on this we added a sentence saying that they stay anonymous in the system to see if this affected trust for the interview objects. Again Kizilcec [2016] splits their test algorithms into low, medium, and high transparency. Prototype 2.2 was similar to medium transparency in the technical details of the system.

### Shared GUI for prototypes 2.3-2.6

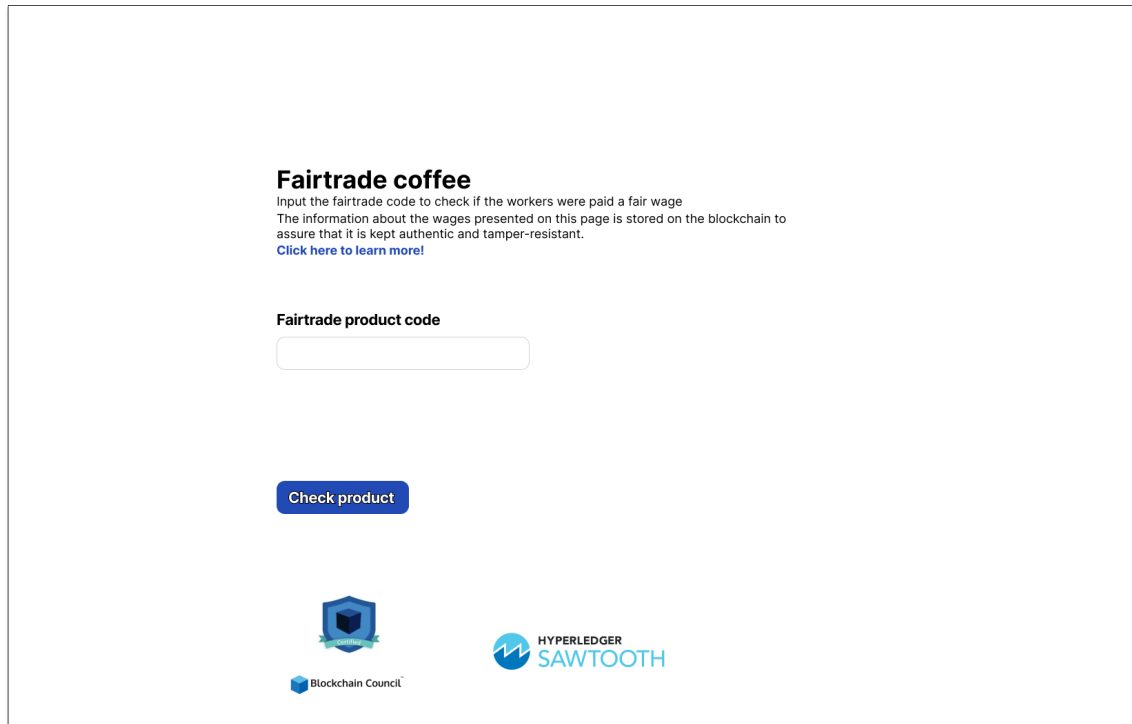


Figure 4.10: This display will be the same for prototype 2.3, 2.4, 2.5 and 2.6.

Figure 4.5 presents a display that was used both by prototypes 2.3, 2.4, 2.5 and 2.6. The difference will be shown when the user clicks "Click here to learn more!" or "Check product". This display provides the same icons and logos as in prototype 2.2 along with a very brief explanation of what technologies have been used and what they provide. Having more detailed information be provided if the user clicked on "Click here to learn more" was inspired by Kizilcec [2016] where the author explained that providing more information to the users who look for it can increase trust. The same logos from prototype 2.2 were used in prototypes 2.3-2.6 as well.

### Prototype 2.3

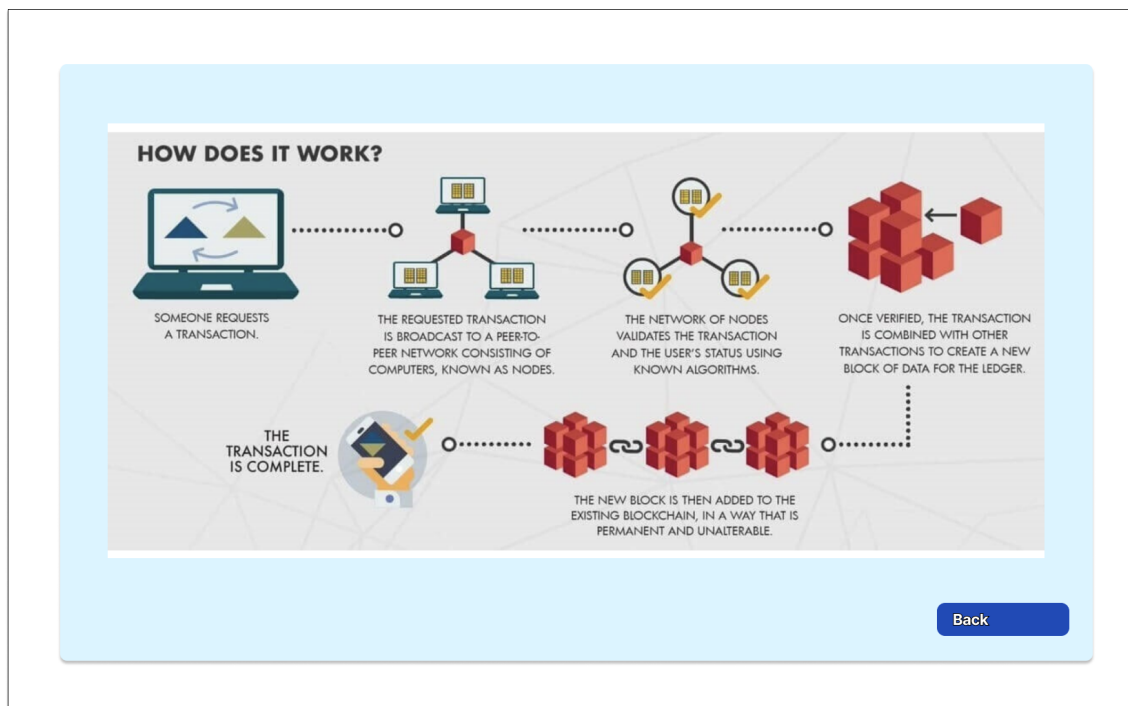


Figure 4.11: Prototype 2.3: Showing the pop-up presented in this prototype if the user clicks on "Click here to learn more" in Figure 4.10.

The third prototype shown in Figure 4.11 presents the pop-up in this prototype if the user clicks on "Click here to learn more!" in Figure 4.10. This pop-up aims to explain how blockchain works in a graphical manner. The users were asked to overlook the low fidelity of the graphics due to this not being an important part of this work. Again Kizilcec [2016] splits their test algorithms into low, medium, and high transparency. Prototype 2.3 could similar to something in between medium and high transparency into the technical details of the system. The main reasoning for providing a prototype explaining the technology graphical was to see if this way of explaining a system was trust enhancing or not.

## Prototype 2.4

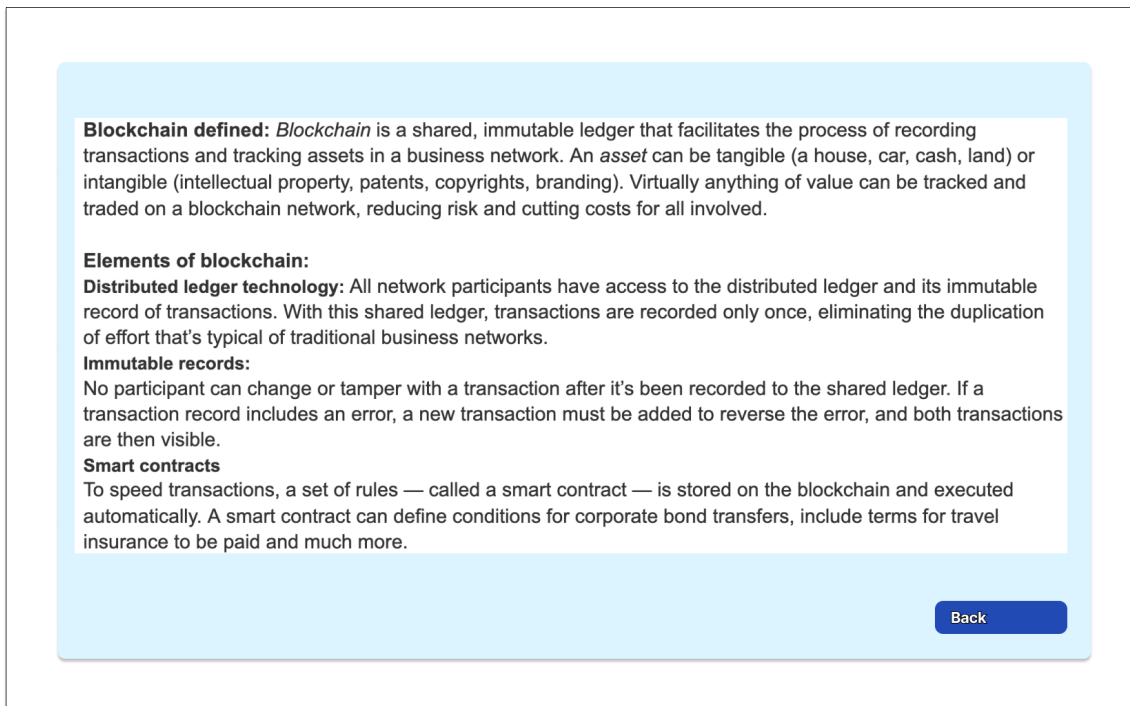


Figure 4.12: Prototype 2.4: Showing the pop-up presented in this prototype if the user clicks on "Click here to learn more" in Figure 4.10.

This prototype shown in Figure 4.12 presents the pop-up in this prototype if the user clicks on "Click here to learn more" in Figure 4.10. The users will be presented with a written explanation of blockchain. This explanation focuses more on the features blockchain provides to the user, and less on the technical details of how it works. This was in contrast to the similar prototype for the data consumer shown in Figure 4.7 where the technical details were in focus. This was done to check if the interview objects have a preference for how a written explanation should be. Again Kizilcec [2016] splits their test algorithms into low, medium, and high transparency. Prototype 1.4 was similar to high transparency into the technical details of the system. The main reasoning for providing a prototype explaining the technology graphical was to see if this way of explaining a system was trust enhancing or not.

## Prototype 2.5

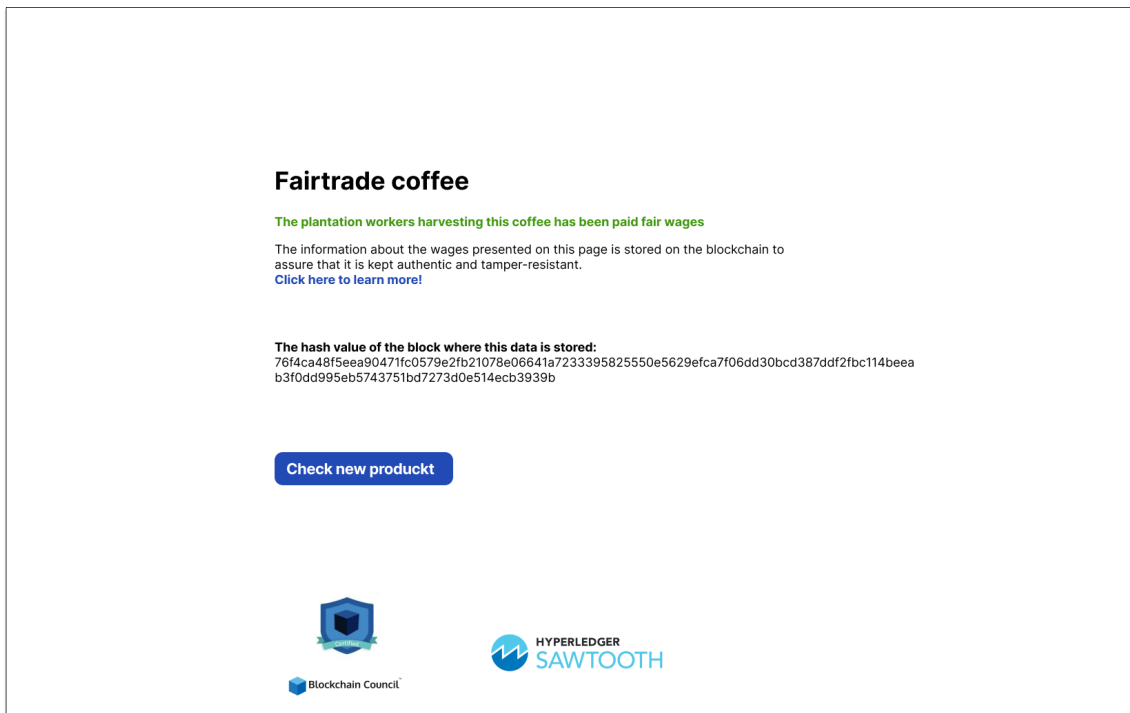


Figure 4.13: Prototype 2.5: Showing what the user was presented in this prototype after they click on "Check product". This prototype presented the hash value associated with the block this information is stored on.

This prototype shown in Figure 4.13 was a duplicate of prototype 2.4, the only change is that when the user submitted their code they, in addition to a confirmation about fair payment, get the hash to the block in the blockchain where the information about this coffee was stored. With this prototype, the goal was to see how the interview objects react when presented with blockchain data and if it enhances trust. This builds on ideas from Shin [2019] where the authors find that increased transparency increases trust in blockchain, but they did not test how users react to blockchain data if presented with it. Compared to prototype 2.4 this prototype has an even higher transparency level into the technical aspects based on Kizilcec [2016] with the hash value visible.





### 4.1.4 Interviews and User Testing

The interview and user tests were conducted both in-person and over digital meetings using video and shared screens. The interviews started with a presentation of the individuals conducting the interviews. An introduction to the Norwegian University of Science and Technology, the department this study was a part of and the goal of the study were also presented. Information about users' anonymity was also explained.

Before starting the user tests and interviews the use case from 4.1.2 was introduced. It was also informed that every comment on every prototype was welcome, but that comments on what strengthened or lowered trust were especially useful. It was also stressed that this would be an open conversation so that the interview objects would talk freely about every thought they had throughout the interview and user test. Since this work was not focused on the graphical and aesthetic part of user experience and user interaction, the test subjects were informed that detailed focus on graphs and aesthetics was not the crucial feedback wanted.

**Interviews** The user test has split into two main parts: one for the data provider prototypes and one for the data consumer prototypes. The interview objects clicked through prototype 1.1-1.4 and made comments and remarks about usability, trustworthiness, presentation of information, and so on. After the four prototypes in part 1 of the user test, the interview objects were asked to rate the prototypes from most to least trustworthy. The exact same process was conducted for the six prototypes for the data consumer.

In the interviews, we presented trust as in section 2.1 and stressed that it was their subjective experience regarding how trustworthy they perceived the system that was interesting. This means that we asked them to take us through their thought process when determining if something seems trustworthy to them. When discussing trust an individual needs to know what the individual should expect to be able to measure trust. In the interviews, the interview objects were informed that the most important features they should consider when determining trust were data integrity and data authenticity. In addition, privacy was important as the data provider.

The questions and discussions often related to both RQ1 and RQ2, so for some of them, it is hard to pinpoint what relates to what. This is the nature of the semi-structured interview where the conversation went where the interview object took it. The user testing of the prototype helped structure the interviews and pull the discussions back to RQ1 and RQ2. To answer RQ1 prototypes 1.1 and 2.1 served as a good basis because the interview objects freely reflected on what they needed to trust a system. The logos and icons used in prototypes 1.2-1.4 and 2.2.-2.6 also helped answer RQ1, but the logos

also related somewhat to RQ2 because they can be viewed as information to develop trust. Just clicking through 10 prototypes with a semi-structured interview provided many interesting perspectives. Rating the prototypes was useful when determining the most trustworthy ways to explain a system for RQ2. The rating also provided a good tool to make the interview objects reiterate what they thought was trustworthy and not and how that compares with the other prototypes, something that provided interesting findings to answer RQ2. The difference between prototypes 1.4 and 2.4 yielded good information to determine what information was important to users. The blockchain data in prototypes 2.5 and 2.6 worked as a catalyst for the interview objects to express what and how blockchain data should be presented to increase trust. For more details regarding the execution of the interviews and what questions were asked see the interview guide in ??.

There are no video or audio recordings of the interviews, but notes were taken throughout the interviews. After the interviews, these notes were presented to the interview objects to ensure the notes recorded were reflective the information and responses they gave during the interviews.

## 4.2 Re-interview and User Test of Improved Prototypes

In this subsection, the research method details and data collection for the second and third steps of user testing are explained. In step 2 a new prototype was designed based on the findings in step 1, and thus, the objective in step 3 was to verify the findings from the step 1, as well as the prototype developed in step 2. The method for step 1 is explained in section 4.1 while the results found when applying this method are presented in section 5.1. In the second step, the results from the first round were incorporated into two new prototypes, one for the data provider and one for the data consumer. In the third step, the same individuals were asked to test these new prototypes and answer the following questions: “Is the new prototype for the data provider more trustworthy than the previous 4 prototypes?” and “Is the new prototype for the data consumer more trustworthy than the previous 6 prototypes?”. These questions gave insight into whether RQ2 was properly addressed. Additionally, the interview objects were welcome to give a more thorough answer than “yes” or “no”, which would allow them to give additional answers to RQ1, besides what was uncovered in the first step of the research. The reasoning for this step was to make sure that the findings from the first step actually increase perceived trust for users when incorporated into prototypes.

Both these final prototypes were also developed in Figma, and based on the prototypes

from section 4.1.3 and the results from section 5.1. The new prototype for the data provider prototype is referred to as prototype 1.5 and the new prototype for the data consumer side is referred to as prototype 2.7.

### **4.2.1 Expanding the Graphical Explanation**

The interview objects from the first round expressed a want to be able to access information in a layered way, starting with a shallow explanation, then getting a more detailed explanation, and if they required a more in-depth explanation this should also be accessible. But the key factor that was expressed was that it should start with an easy explanation, and the user should be able to open more in-depth explanations if they thought it necessary.

Based on this feedback prototype 1.3 from Figure 4.6 served as a foundation for the development of prototype 1.5, and prototype 2.3 from Figure 4.11 served as a foundation for the development of prototype 2.7. Both prototypes 1.3 and 2.3 was expanded by adding the written explanation from 1.4 from Figure 4.7 and 2.4 from Figure 4.12, respectively. The way this expansion worked, was that there was a button redirecting from the graphical explanation to the written explanation, and back.

### **4.2.2 Presentation of Blockchain Data**

The interview objects also expressed that the blockchain data should be hidden behind a button, only to be shown when clicked on. Making it more readable was also an expressed want from the interview objects.

## 4.2.3 Improved Prototypes

### Prototype 1.5

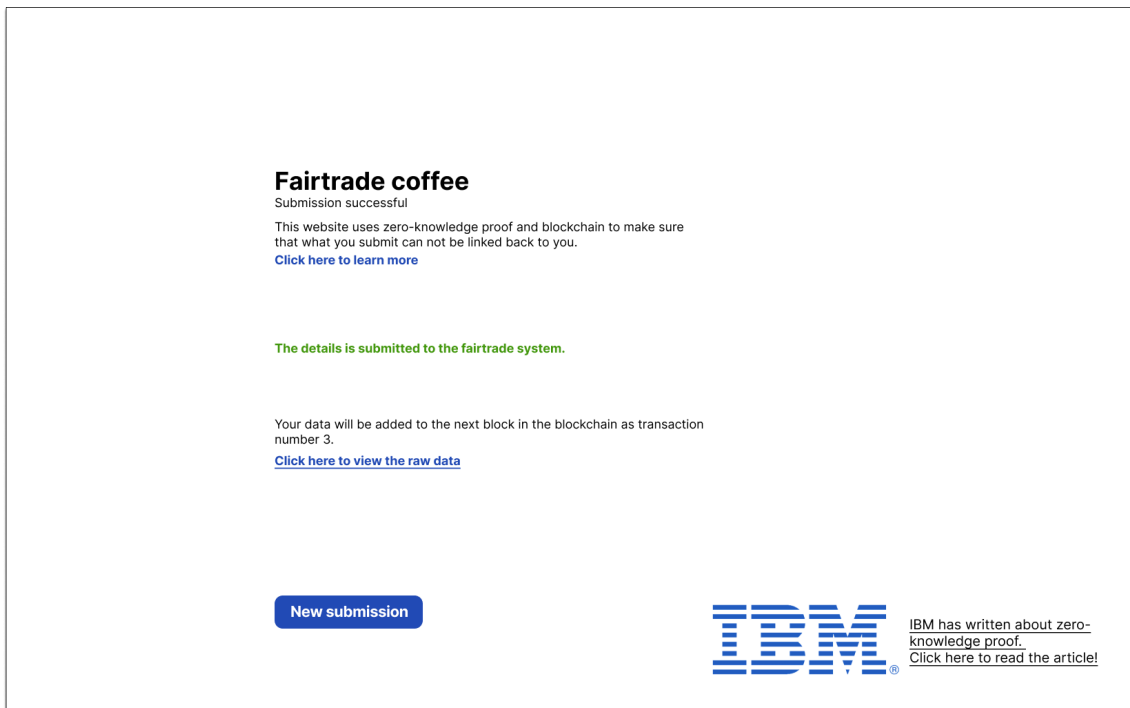


Figure 4.15: Prototype 1.5: The view a data consumer user gets after filling in the delivery details and hitting submit. A button redirection to the raw blockchain data was also added.

Figure 4.15 shows how a user can access the raw data for their blockchain transaction by clicking the button "Click here to view the raw data". This button will take them to a page where the pending blockchain transactions are displayed.

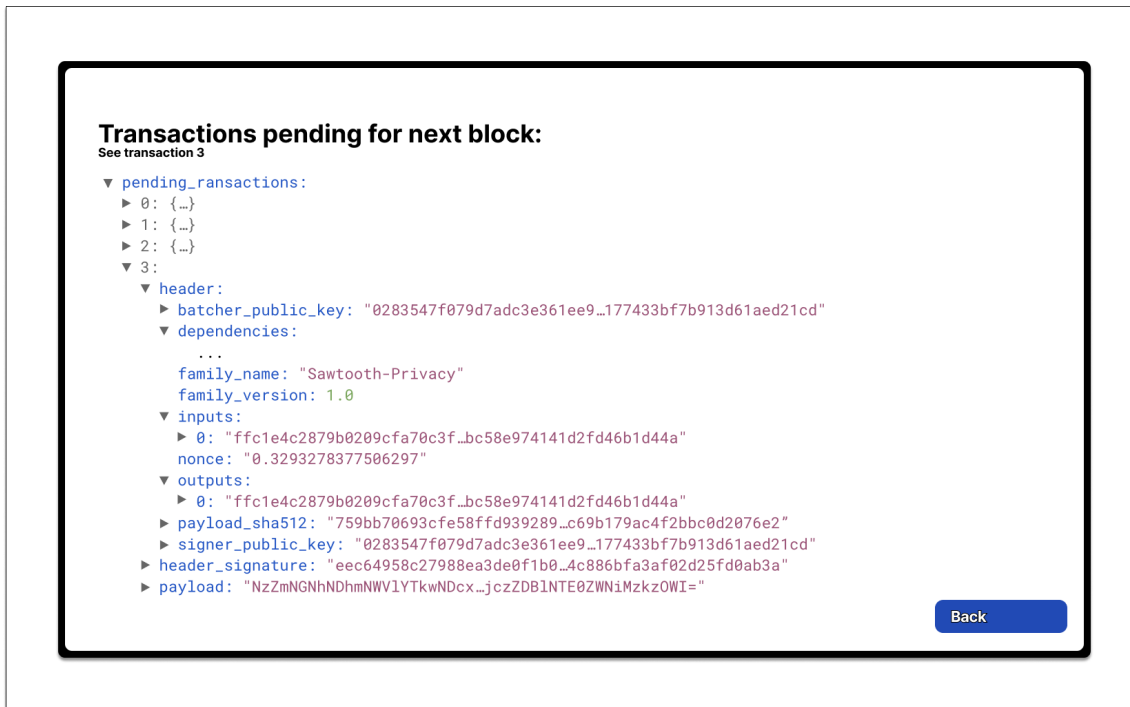


Figure 4.16: Prototype 1.5: The view of the raw data showing the pending transactions for the next block to be validated and mined.

Figure 4.16 shows the view a user would get from the pending transactions for the next block. One of these pending transactions would be the transaction that they just submitted to the system. The readability of the raw data has been approved by changing it from the standard JSON format.

## Prototype 2.7

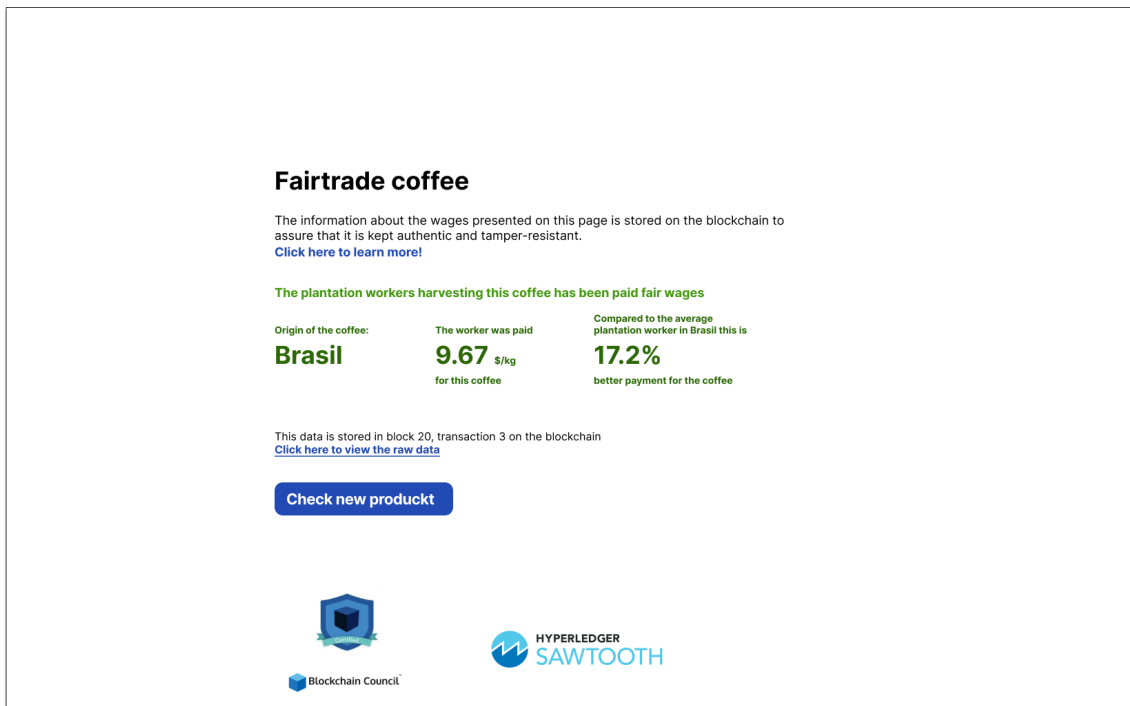


Figure 4.17: Prototype 2.7: The view a data provider user received after submitting a product code to check if it was fairtrade. In addition a more visual data representation about the coffee was presented. A button redirection to the raw blockchain data was also added.

Figure 4.17 shows how a user could assess the raw data for their blockchain transaction by clicking the button “Click here to view the raw data”. This button would take them to a page where they could view the transaction where the data about the product in question was stored along with the rest of the block.

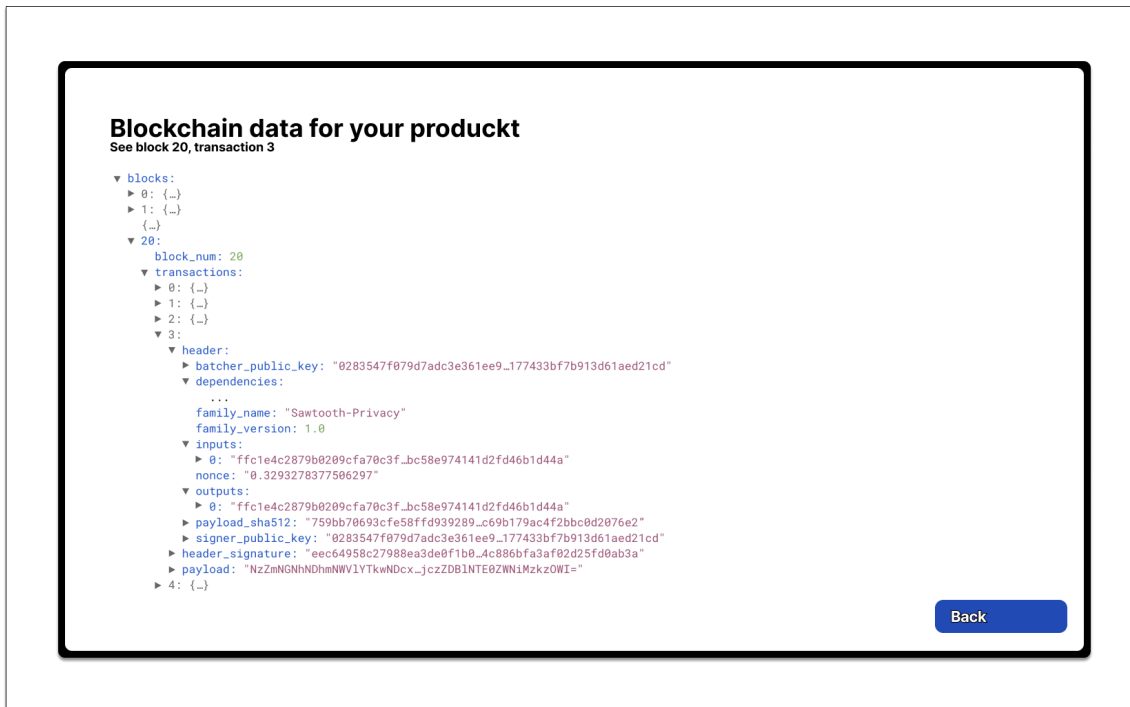


Figure 4.18: Prototype 2.7: The view of the raw data showing the transaction in question along with the rest of the transactions for that block on the blockchain.

This was also formatted to make it more readable for the users. Link to both prototypes 1.5 and 2.7 can be found in Appendix A.

**Data Visualisation** In section 5.1 need for more data and information about the actual product, payment, wages, and so on by the interview objects were presented. There was wide consensus among interview objects that this was an important improvement that should be made to the prototypes to increase trust. In Figure 4.17 the origin country was shown, the wages per kilogram coffee were presented, and how the wages compare to the average in the said origin country was shown.

### 4.3 Technical Implementation to Address RQ3

In addition to designing a second prototype, step 2 of the study consisted of designing the technical implementation. Based on the results of step 1, it was suggested that a supply chain system based on blockchain technology, utilizing off-chain data storage and zero-knowledge proof methods would be trustworthy.

As explained in chapter 2, an issue with storing personal data, such as employee salaries or payouts, on the blockchain is the notion of privacy. In the case of fair trade a potential

worker might have concerns about sharing this sort of information publicly, as it could result in negative consequences, for instance in the case of whistleblowing. Thus, this part of the study consisted of additional research into relevant literature, in order to create a model for blockchain privacy, which would satisfy research question 3, which was defined in section 1.3 as follows:

- **RQ3:** How could a privacy-preserving blockchain system be designed, providing unlinkable transactions and a high level of privacy for users?

### **4.3.1 Research Motivation**

Existing work in the field of privacy-preserving blockchain networks partially cover the use case for the thesis. While blockchain is pseudonymous, Goldfeder et al. [2017] has shown that users can be deanonymized. Thus, there has been conducted some research into utilizing methods for creating unlinkability, which are covered in detail in 3.3. These methods are less broad and tend to focus on limited use cases, which do not overlap completely with the use case presented in this thesis.

### **4.3.2 System Design**

The goal of the research question was to design and propose a system model, which was thus to be based on the interviews as well as related literature. The current state of the technology provided a theoretical foundation for designing the system. Implementations were to be made and tested on a small scale, seeing whether this could provide a potential foundation for further research and expansion in the realm of privacy-preserving blockchain networks.



# Chapter 5

## Results

### 5.1 Explorative Study to find Drivers of Trust

In total the user tests and interviews in step 1 of the study were conducted on  $n = 15$  individuals. Based on self-reported information, 7 of the interview objects were between 20-24 years old, 5 of the interview objects were between the ages 25-30, 2 of the interview objects were between the ages 51-60, and 1 interview object was between the ages 61-70. 7 of the interview objects identified as male, while the other 8 identified as female. 7 of the interviews were conducted in person, while the remaining 8 were conducted over video calls. 3 of the interview object said they had a superficial understanding of blockchain, but no more than a conceptual idea of how it works and the features it can provide. The reminding 12 had only heard of the term, specially related to cryptocurrency, but had not a good understanding of the technology. This was intended since the goal is to understand what non-technical individuals need to trust a technical system.

#### 5.1.1 Rating of the Prototypes

After each round of the interviews, the interview objects were asked to rate the prototype. The results from this rating are presented in this subsection. The rating of the prototypes will provide a basis for answering both RQ1 and RQ2, since its provides a average rating for the prototypes presented to the interview objects. Even though it is useful when discussing RQ1, it is most closely related to answering RQ2, since the rating was based on what the interview objects found the most trustworthy way of explaining the system details.

### Data Provider

The interview objects were presented with prototypes 1.1, 1.2, 1.3, and 1.4 and asked to rate them from most trustworthy to least trustworthy.

Interviewee	Prototype 1.1	Prototype 1.2	Prototype 1.3	Prototype 1.4
Interviewee 1	1	2	4	3
Interviewee 2	1	3	4	2
Interviewee 3	2	1	4	3
Interviewee 4	1	2	4	3
Interviewee 5	1	2	4	3
Interviewee 6	1	2	4	3
Interviewee 7	1	2	4	3
Interviewee 8	4	2	3	1
Interviewee 9	1	2	4	3
Interviewee 10	1	4	2	3
Interviewee 11	1	2	4	3
Interviewee 12	1	2	4	3
Interviewee 13	1	2	4	3
Interviewee 14	1	2	4	3
Interviewee 15	1	2	4	3

Table 5.1: The reported ratings for the four different prototypes for the data provider. The score is 4 if the interviewee found it most trustworthy, 3 to the second place, 2 to the third place, and 1 to the least trustworthy.

The ratings are presented in Table 5.1 for each of the interviewees. The rating 4 represents the most trustworthy, 3 represents the second most, 2 represents the third most, and 1 represents the least trustworthy of the prototypes.

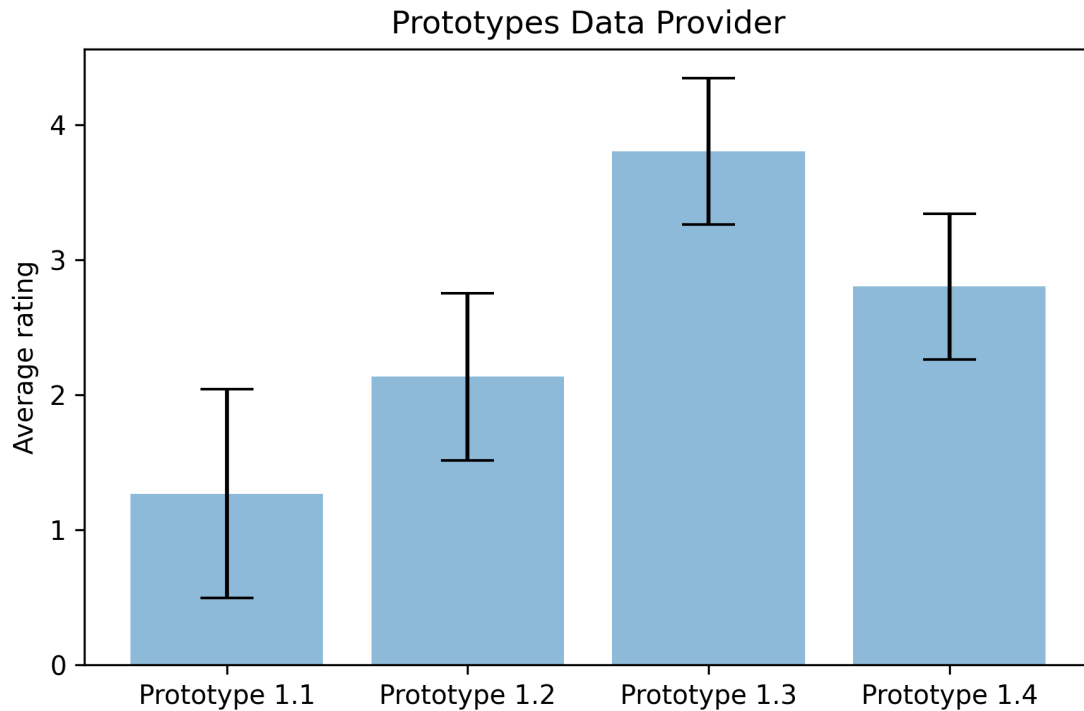


Figure 5.1: Plot showing most to least trustworthy prototype for the data provider in the following order: 1.3, 1.4, 1.2, and 1.1. The rating was calculated based on giving a prototype score of 4 if the interviewee found it most trustworthy, 3 to the second place, 2 to the third place, and 1 to the least trustworthy. An average of this score across the 15 interviews is plotted here. The error bars is plotted with standard deviation.

Figure 5.1 shows the average ratings for 4 prototypes across the 15 interviews presented in Table 5.1. It shows a clear favor to prototype 1.3 with an average score of 3.80, prototype 1.4 comes in second with an average score of 2.80, prototype 1.2 has an average score of 2.13, and the least trustworthy is prototype 1.1 with an average score of 1.27. This order is in line with how the majority rated these 4 prototypes. In fact, 11 out of the 15 interview objects rated the prototypes in the same manner as the rating based on the average, showing wide consensus among users that this rating is representative. Interviewee 8 from Table 5.1 is a noticeable outlier with their rating of prototype 1.1 as the most trustworthy. Other than this outlier, the reminding 3 interview objects only had small variations to the ordering based on the average. It is also worth noting that both Interviewee 8 and 10 from Table 5.1 were in the high age range and it might be possible that their unrepresentative ordering can be explained by a higher age than the rest of the group.

### Data Consumer

The interview objects were presented with prototypes 2.1, 2.2, 2.3, 2.4, 2.5, and 2.6 and asked to rate them from most trustworthy to least trustworthy.

Interviewee	Prototype 2.1	Prototype 2.2	Prototype 2.3	Prototype 2.4	Prototype 2.5	Prototype 2.6
Interviewee 1	1	4	6	5	3	2
Interviewee 2	1	4	6	5	3	2
Interviewee 3	1	4	2.5*	6	5	2.5*
Interviewee 4	1	3	5	6	4	2
Interviewee 5	1	2	3	5	6	4
Interviewee 6	1	2	6	5	4	4
Interviewee 7	1	2	4	3	6	5
Interviewee 8	5	4	3	2	6	1
Interviewee 9	1	3	6	4	5	2
Interviewee 10	1	5	6	4	3	2
Interviewee 11	1	2	4	3	6	5
Interviewee 12	1	2	3	4	5	6
Interviewee 13	1	3	5	4	6	2
Interviewee 14	1	5	6	4	3	2
Interviewee 15	1	2	3	5	4	6

Table 5.2: The reported ratings for the 6 different prototypes for the data consumers. The score is 6 if the interviewee found it most trustworthy, 5 to the second place, 4 to the third place, 3 to the fourth place, 2 to the fifth place, and 1 to the least trustworthy. \* interviewee 3 did not manage to decide on rating between 2.3 and 2.6, hence the half score.

The ratings are presented in Table 5.2 for each of the interview objects. The rating 6 represents the most trustworthy, 5 represents the second most, 4 represents the third most, 3 represents the fourth most, 2 represents the fifth most, and 1 represents the least trustworthy of the prototypes.

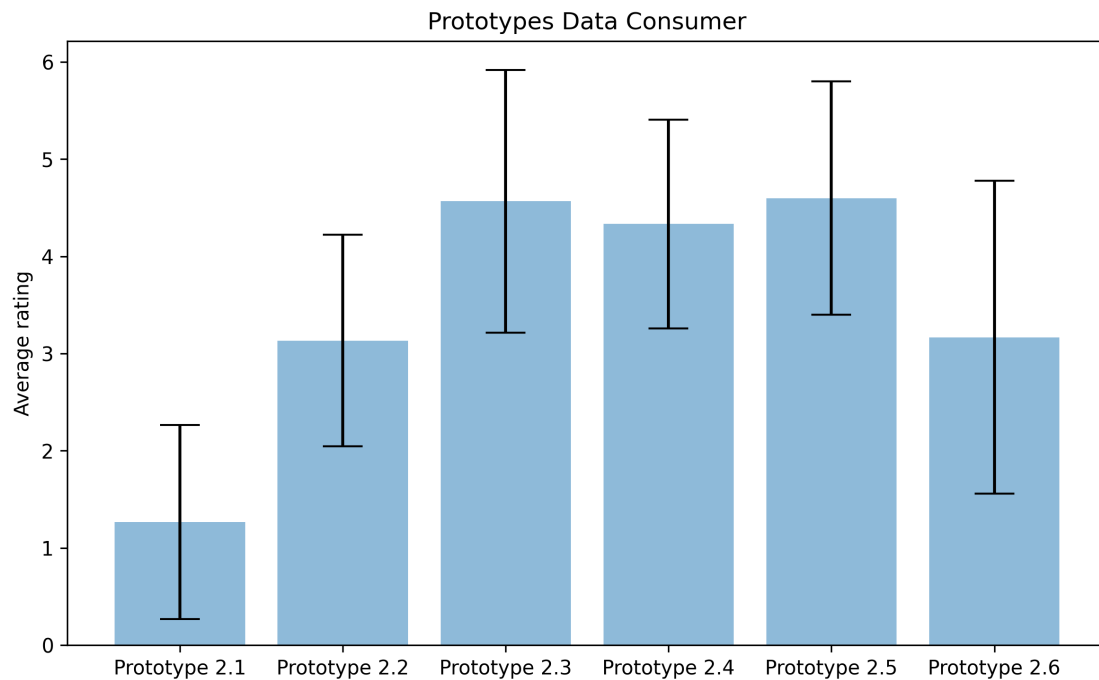


Figure 5.2: Plot showing most to least trustworthy prototype for the data consumer in the following order 2. 5, 2.3, 2.4, 2.6, 2.2, and 2.1. The rating was calculated based on giving a prototype score of 6 if the interviewee found it most trustworthy, 5 to the second place, 4 to the third place, 3 to the fourth place, 2 to the fifth place, and 1 to the least trustworthy. An average of this score across the 15 interviews is plotted here. The error bars is plotted with standard deviation.

Figure 5.2 shows the average ratings for the 6 prototypes across the 15 interviews presented in Table 5.2. It shows favor to prototype 2.5 with an average score of 4.6, prototype 2.3 comes in second with an average score of 4.57, prototype 2.4 comes in third with an average score of 4.33, prototype 2.6 comes in fourth with an average score of 3.17, prototype 2.2 has an average score of 3.13, and the least trustworthy is prototype 1.1 with an average score of 1.27. This exact order is not represented with interviewees having the same order as with the data providers in Table 5.1. This might be due to there being more prototypes and therefore more possible orderings. It might also be due to prototypes 2.3, 2.4, and 2.5 being all quite popular with the interview objects and there being no clear favorite among them.

The average rating for prototypes 2.3, 2.4, and 2.5 has an average rating so similar that it can not be told by this data sample which one is the interviewee's favorite. The same is true for prototypes 2.2 and 2.6 where it is hard to tell what prototype comes in fourth and fifth due to the close average rating. The only clear trend to be seen from Figure 5.2 is that prototype 2.3, 2.4, and 2.5 is the ones that are rated most trustworthy

by the users, prototype 2.2 and 2.6 is less trustworthy than those 3, and it is clear that prototype 2.1 is by far the least trustworthy out of the 6 prototypes.

### **5.1.2 RQ1: Elements that Enhance Perceived Trust from Step 1**

This section will present the findings related to answering RQ1 from the interview. Elements that affect trust, that are not explicitly related to system explanation but more general trust enhancing elements, are presented in this section.

#### **Logos and Icons as Trust Signifiers**

Every prototype except 1.1 and 2.1 had icons and logos. Prototypes 1.2, 1.3, and 1.4 all had a logo from IBM with a link to an article written by IBM about zero-knowledge proof [Jones, 2019]. Prototype 2.2-2.6 all had the Hyperledger Sawtooth logo and a logo from the Blockchain Council which also said certified [Blockchain-Council]. Please refer to section 4.1.3 for a reminder of the logo used in the prototypes.

11 of the interview objects said that icons and logos like this enhanced their perceived trust in the system on a general basis. The reasoning for this was mostly because they felt that the brand on the logo somehow had endorsed the system and therefore this made it more legitimate. 3 out of those 11 interview objects also said that the aesthetic factors of adding logos and icons enhanced trust because the website looked more professional. The reminding 4 said logos and icons did not enhance trust, they also said that it did not decrease trust either. This means that it was no negative impact on trust to add icons or logos.

The interview objects that expressed indifference to the use of logos and icons said that it was because they did not know the company from the logo used, or that they did not understand how an association with that company could increase legitimacy to the system. In contrast, the 11 interview objects that found that logos and icons increased trust also expressed an increase in trust even though they did not know the company. As stated before this was in some cases purely aesthetic, but for some also just an automatic response to the logos and icons that the interview objects found hard to explain. After some follow-up questions, it seems like this increase in trust stems from the interview objects making their own assumptions about why the logos and icons are there based on what they internally find to be a logical explanation. This can best be illustrated by the logo from Blockchain Council Certified where the interview objects had associations to the words blockchain, council, and certified, but had never heard about Blockchain Council or any certifications from this organization. This did not stop them from drawing the conclusion that blockchain is an up and coming technology, Blockchain Council must

be a council charged to maintain good practices in this emerging technology, and if this council certified this system that must mean it is trustworthy. This is a conclusion which was drawn by 6 of the interview objects regardless of their familiarity with the organization at all.

### **Other Findings**

In addition, the 13 interview objects said that more details regarding the specific coffee and what it would mean that they were paid fair wages would increase trust. Information about for example region of harvest, how much the farmer is paid, pictures of the farmer, how much is considered a fair wage, and how much coffee there was in this transaction would increase the trust of consumers.

7 interview objects also expressed that trust was increased by color, nice layout, or good user experience. Colors like green and blue increased the trustworthiness of a website, but red made it seem like it was an error. Ease of use also increased trust, along with what the interview objects called a professional look.

### **5.1.3 RQ2: Technical Details and Explanations to Enhance Trust**

This section will present the findings related to answering RQ2. The findings giving insight into preferred ways of providing an overview of a technical system to enhance trust are presented in this section. This includes both explanations, but also technical details.

#### **System Explanation to Increase Trust**

Regarding preferences on how the technical aspect should be explained to increase trust, it was clear consensus among 13 of the interview objects. This consensus was that the graphical explanation from prototypes 1.3 and 2.3, and the written explanation from prototypes 1.4 and 2.4 (2.5 and 2.6) was the most trustworthy way of explaining the system. For the data provider it was a solid advantage to graphical explanation, while for the data consumers there was no such clear trend between the graphical and written explanation.

During the interviews, it was clear that the majority of the interview objects preferred a structure for how the system was explained based on layers. 13 out of the 15 interview objects found this way of presenting information more trustworthy. This layered way is when the first layer had just a few details, and the user could click into a new layer showing more details, as in prototype 1.3, 1.4, 2.3, 2.4, 2.5, and 2.6. Seemingly it is ideal to hide detailed explanations by default, with buttons that could bring you more

details. This led to a conversation with the interview objects regarding how detailed explanations they would prefer, where 13 of them expressed interest for as many details as possible, but presented in a way that gave them as the users the option of not having to read them. This led to the suggestion of expanding prototypes 1.3 and 2.3 to have a third layer where a written and more detailed explanation was accessible from the graphical explanation.

When comparing the two different ways to explain the system done in 1.4 and 2.4 (2.5 and 2.6) there was a clear preference to the way the details are explained in 2.4. The difference between 1.4 and 2.4 is that in 1.4 it was a focus on details on how it worked and in 2.4 the focus was on what features this technology provided. This indicates a clear preference for information about why the technical solution is used and what they provide, instead of a more formal definition and explanation on how the technical solutions work. All 15 interview objects prefers the explanation focusing on the features, if they had to choose between those two stiles of explanation.

The last interesting finding regarding the explanation of the system was that 3 interview objects experienced increased trust even though the technical explanations were presented in a way that went over their heads. When trying to uncover why this was the case, the explanations received was along the lines that it would be harder to lie when this many details are presented, and if they lied some expert in the field would react and it would reflect badly on the company. Some also expressed the thought that this was trustworthy because if they wanted they could understand it by using more time reading up on the details. The majority still felt that an approachable explanation was the most trustworthy.

### **Presentation of Blockchain Data**

The feedback from the interview objects when it comes to how blockchain data was presented in prototypes 2.5 and 2.6 was that it was quite confusing in the beginning. This confusion came from the interview objects not being used to this way of representing data. For the hash value in prototype 2.5, 8 interview objects rated this prototype amongst their top two most trustworthy because they liked the extra transparency, but for prototype 2.6 the consensus was that this seemed like an error message and decreased trust. It was 4 interview objects that rated prototype 2.5 amongst their top two, meaning the consensus was not complete. It was a disagreement among the interview objects whether or not blockchain data was trust enhancing, interestingly this does not necessarily reflect the technical background of the interview objects.

There was consensus among the users that hiding this blockchain data behind a button would be better, whether or not they thought blockchain data increased trust. 5 of



the interview objects also mentioned that it could be trust-enhancing to have a way for the user to see all the blockchain data for all the blocks and all the transactions, and precisely where the data they provided or consumed was stored.

Additional comments were that if the data was more readable it would be more accessible and therefore increase trust in the system. 4 of the interview objects also mentioned that if they were a data consumer having two bags of coffee and they used prototype 2.5 it would increase trust greatly if the hash value changed when checking the two different products.

## 5.2 Re-interview and User Test of Improved Prototypes

The results presented in this subsection are collected from the same  $n = 15$  individuals that provided the results presented in section 5.1. These results are collected using the method explained in section 4.2. The goal with this final step is verifying the findings from step 1 and the new prototype created in step 2.

### 5.2.1 Results for Prototype 1.5

For prototype 1.5 14 out of 15 users confirmed that this was more trustworthy than all prototypes 1.1-1.4 discussed in the previous round of interviews and user testing. The reasoning for why this prototype felt more trustworthy for users was that the combination of the graphical and the written explanation gave them the feeling that the system and technology used were transparent. Some interview objects also expressed that adding the pending blockchain transactions as shown in Figure 4.15 and Figure 4.16 increased trust because it felt as it gave them the possibility to check and validate that the information presented actually was stored on the blockchain.

The one interviewee that did not find prototype 1.5 more trustworthy was the same individual that rated the prototypes 1.1-1.4 very different from the rest of the group. This interviewee's rating can be found in Table 5.1 Interviewee 8. Here it is shown that prototype 1.1, the simplest one, was rated most trustworthy. Based on this it is not surprising that this interviewee rated the even more complex model less trustworthy than prototype 1.1-1.4. The answer is still an outlier from the rest of the responses.

### 5.2.2 Results for Prototype 2.7

Most of the same was true for prototype 2.7. All 15 interview objects felt this was more trustworthy than prototypes 2.1-2.6 presented in the first round of interviews. The

combination of the graphical and written explanation increased trust as in prototype 1.5, and hiding blockchain data behind a button by default also increased trust for the interview objects. As with prototype 1.5, they felt it was possible to control the information provided on the page because of access to the blockchain data.

All the interview objects also greatly appreciated the more detailed information about wages, the origin of the coffee, and how much better the wages of this farmer were than the average wage in the given country because of Fairtrade. It seems like the reason why the interview objects felt this was more trustworthy was that it could be controlled somehow so that it would be harder for the companies to lie if they presented more information about the product. 9 interview objects also expressed an increased trust in the blockchain in and of itself because data was presented this way.

## 5.3 Technical Implementation to Address RQ3

This section covers the results of research question 3 and the study as described in 4.3. Relevant papers, as well as open source code and research, was used to design the system model. Besides the work conducted in Ben Sasson et al. [2014], important work uncovered in the literature included the blockchain framework Hyperledger-Sawtooth [2019]; the Rust implementation of zkSNARKs called bellman, detailed in Zero-knowledge Cryptography in Rust [2021]; the Identity Mixer implementation described in Hyperledger [2020]; and the zkSNARK system described in Ben-Sasson et al. [2013]. The system design is limited and is not a full-fledged production prototype, but it provides a potential framework for the functionality privacy-preserving blockchain system. Link to the repositories included in this part of the research and results can be found in Appendix C.

### 5.3.1 System Model

Based on findings in step 1 of the research, as well as existing literature, a system model was thus drafted and designed. In order to maintain privacy, the system was designed as a conceptual blockchain model utilizing an off-chain database for storing data, as well as zkSNARKs in order to create unlinkability. While the off-chain database does provide a level of privacy and makes the system more scalable, there are still privacy concerns if the database is breached. Database leakage would make all transactions and data directly linkable to an address in the network, which, as explained in Goldfeder et al. [2017], can be efficiently traced back to an individual's identity. In order to ensure privacy, zkSNARKs are utilized so that a user can create unlinkable transactions, which will be still be verified as with all blockchain transactions. Thus, the user can be sure that even if database data leaks, the transaction cannot be directly traced back to them.

## System Overview

The system design features two main additional components on top of a regular blockchain network. These two are an *off-chain database* for storing data associated with the blockchain and a *zero-knowledge proof* implementation which serves the function of making transactions unlinkable. Both of these will be detailed in the following subsections.

This system was designed and tested with an implementation of the *Hyperledger Sawtooth* framework [Hyperledger-Sawtooth, 2019]. However, the system design is explained in detail here, so it can be generalized to fit with any blockchain framework. It also uses an open source Rust-implementation of zkSNARKs, called *bellman*. Additionally, the system and implementation draws inspiration from Ben Sasson et al. [2014].

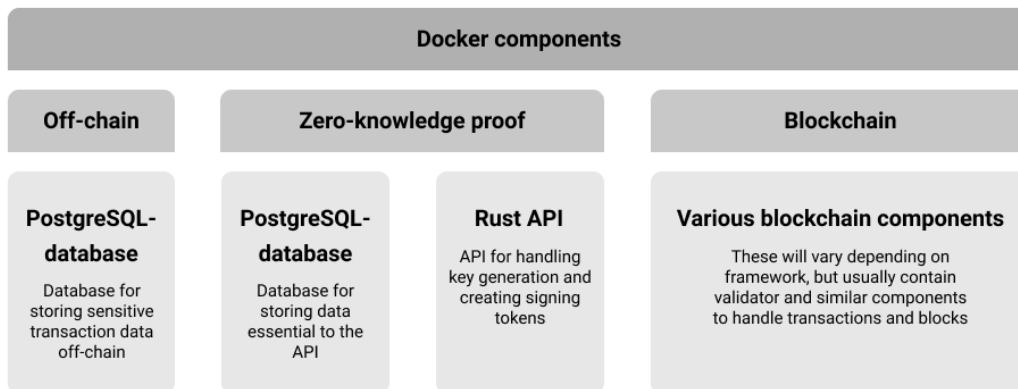


Figure 5.3: An overview of the various Docker components used in the system design.

The following subsections will explain each of the system components in detail.

### Off-Chain Database

This blockchain network uses an off-chain database to store all the data submitted to the blockchain. There are several reasons as to why storing the raw data in an off-chain database is ideal. Firstly, it makes the blockchain network more scalable, as less raw data is stored directly on the blockchain. To still maintain the immutability aspects of blockchain networks, a hash of the raw data is stored directly on the blockchain, which can then be used to check and verify entries in the off-chain database.

**Hashing** The hash value stored on the blockchain is in the form of SHA-512, as detailed in section 2.3.1. The data input is hashed using the SHA-512 scheme. The raw data is then inserted into the database, and the hash value is placed on the blockchain itself. Using this approach one can validate data integrity of the off-chain database by hashing the raw data and comparing it to the hash value from the blockchain.

**Advantages** While storing data off-chain does require some extra overhead, as well as a centralized database, it can be incorporated with a blockchain system to still maintain most of the advantages of a decentralized system. Using an off-chain database also has specific advantages, which are useful for our hypothetical use case, as well as others.

**Scalability:** One major advantage of storing most of the data off-chain relates to scalability. With systems that require a lot of data storage, it is inefficient to store all of it on the blockchain itself, as it requires a lot of computational power. New peers who join the network will also have to generate a copy of the entirety of the blockchain, which makes scalability a big issue in cases where a lot of data has to be stored and processed.

**Privacy:** With systems that require a high level of privacy, due to sensitive information, it is not ideal to store all of this on the blockchain. The data stored on the blockchain can be accessed by any peer in the network, which can be a potential privacy issue. Seeing as this proposed solution attempts to maintain the privacy of the data providers, it is essential to keep data securely stored. By storing the data off-chain, the system can guarantee a higher level of privacy for the data providers through using proper access control. As mentioned earlier, data immutability is still maintained, seeing as the off-chain data can be hashed and verified by comparing it to the hash values on the blockchain.

## Implementation

The resulting implementation shows that storing data off-chain is unproblematic and can be easily integrated with any existing blockchain solution. This type of solution can be applied to a wide variety of blockchain system. The drawbacks of this implementation is that having a centralized database defeats some of the purpose of using blockchain technology. This introduces a single point of failure. This issue can however be amended, by storing the database in multiple locations. The data integrity aspects of the blockchain networks are still maintained, by storing the hash value on the blockchain. This means any data stored off-chain can be easily verified by simply hashing the data and checking its corresponding transaction stored on the blockchain. A strength of this solution is the focus on privacy. Storing raw data on the blockchain can impede the privacy of the user making the transaction, as it is exposed to everyone in the network. By storing

it off-chain one can limit who can access to said data, in order to ensure privacy for everyone in the blockchain network.

An example of how data can be stored in an off-chain database and its related hash-value can be stored on the blockchain is presented below. This is from a system implementation using the Hyperledger Sawtooth implementation and a PostgreSQL database.

<b>Id</b>	<b>Weight</b>	<b>Price</b>	<b>Region</b>
...			
20	36 KG	\$250	Brazil
...			

Table 5.3: A comparison of the different algorithms in the SHA family and their parameters.

In Table 5.3 an example input in a PostgreSQL-database is presented. The corresponding JSON of the Hyperledger Sawtooth transaction is presented in Listing 1. The interesting part of the JSON-code, is the "payload"-field. This includes a hashed value based on the input in the PostgreSQL database. The data input is first hashed using SHA512, then, due to the structure of Hyperledger Sawtooth transactions, it is encoded using Base64. When data is fetched from the blockchain and the off-chain database, the blockchain payload is first decoded using Base64, resulting in the SHA512 hash value. The off-chain data is then hashed using SHA512 and compared against the data fetched from the blockchain, in order to ensure it has not been manipulated.

```

1 {
2   "header": {
3     "batcher_public_key":
4       ↪ "0283547f079d7adc3e361ee9080eef2931ca691ef5b177433bf7b91
5       ↪ 3d61aed21cd",
6     "dependencies": [],
7     "family_name": "Sawtooth-Privacy",
8     "family_version": "1.0",
9     "inputs": [
10      ↪ "ffc1e4c2879b0209cfa70c3f464ab38177341707edac6b2bc58e974
11      ↪ 141d2fd46b1d44a"
12    ],
13     "nonce": "0.3293278377506297",
14     "outputs": [
15      ↪ "ffc1e4c2879b0209cfa70c3f464ab38177341707edac6b2bc58e974
16      ↪ 141d2fd46b1d44a"
17    ],
18     "payload_sha512":
19       ↪ "759bb70693cfe58ffd9392895943c64886f3bd69d386da457b3d93a
20       ↪ 3f94e61a567c65e7c1a4aa082235487cd86a6123945705e392c69b17
21       ↪ 9ac4f2bbc0d2076e2",
22     "signer_public_key":
23       ↪ "0283547f079d7adc3e361ee9080eef2931ca691ef5b177433bf7b91
24       ↪ 3d61aed21cd"
25   },
26   "header_signature":
27     ↪ "eec64958c27988ea3de0f1b0f3574c24478acf29fb1a6e1c247052ee9a6
28     ↪ da9b0497dd0374f89a62966e77889bdf75413c8b41b5cb4c886bfa3af02d
29     ↪ 25fd0ab3a",
30   "payload":
31     ↪ "MGM3YjJmNjU1ZTQwYjEOMDZmNzkzZTI1M2M5NTQ5N2ExMGN1Mzc4YTkyMjZ
32     ↪ hYWI5MmMwYTZjNGQ0ZD11ZjcwNDc0NmY0NTczYjI1ZTRhYjg4NmU5NzRjNzA
33     ↪ OYzQ10TMyMmFjNzU3YzQzNWM4OTdmMzIyYmVlZjQzNGMxYTg1NTk="
34 }

```

Listing 1: An example of a transaction in Hyperledger Sawtooth. The "payload"-field value corresponds to the hash of the database data.

### Zero-knowledge proof

In addition to using an off-chain database to store data, this system uses an implementation of zkSNARKs, a type of zero-knowledge proof described in section 2.6.2. zkSNARKs makes it possible to create unlinkable transactions, meaning that the origin of the transaction can not be traced back from the transaction itself. This is an essential aspect of the system, which attempts to preserve privacy. In traditional blockchain systems, all transactions are linkable, meaning you can find the source of the transaction. Although users in a blockchain network only have pseudonymous addresses, it has been shown that one can find the real identities of users by analysing transactions in a blockchain network Goldfeder et al. [2017]. Thus, by using zkSNARKs one can avoid this privacy risk by making transactions unlinkable, adding another layer of security on top of storing the data off-chain. This implementation of a zkSNARK is inspired by the protocols defined by Ben Sasson et al. [2014] and Hyperledger [2020], as well as Ben-Sasson et al. [2013].

The zero-knowledge proof aspect of the implementation presents a framework for signing unlinkable transactions. This is more complicated to integrate with existing blockchain networks, due to a number of factors. Firstly, the keys generated based on the key agreement scheme, as well as the signing tokens, have to be generated off-chain. This is in order to ensure privacy and security in the system. Then the verification scheme for transactions and blocks may have to be altered in order to allow for transactions to be signed using signing tokens instead of the users personal address. Seeing as the system presented in this paper does not focus on monetary transactions, efficiency is not a part of the scope. However, the efficiency of blockchain systems utilizing zkSNARKs for transactions has been studied in Ben Sasson et al. [2014].

**Key generation** A zkSNARK requires a one-time trusted setup for public parameters [Ben-Sasson et al., 2013]. This should be done using secure multi-party computation. The public parameters for this model include a public verification key  $vk$  and a public proving key  $pk$ .

Peers in the network generate a signing key,  $a_{sk}$ . Using the signing key, a transmission key,  $addr_{pk}$  and an incoming viewing key,  $ivk$ , are generated for each user. The transmission key consists of  $(a_{pk}, pk_{enc})$ , and the incoming viewing key consists of  $(a_{pk}, sk_{enc})$ . There are a set of functions used to derive the keys, namely a pseudo random function,  $PRF_{ax}^{addr}(t)$ , and a key agreement scheme,  $KA$ , with associated functions. In the following definitions  $SHA256Compress$  is, as might be intuitive, a SHA-256 compression function. Additionally,  $Curve25519$  denotes an Ed25519 ECC, as described in section 2.4.1.  $clamp_{Curve25519}(x)$  is a function which takes a 32-byte sequence and clears bits 0, 1, and 2 of the first bytem clears bit 7 of the last byte, and sets bit 6 of the last byte Bernstein

[2006]. These functions are defined as follows:

$$\text{PRF}_{a_x}^{\text{addr}}(t) := \text{SHA256Compress}\left(\begin{array}{|c|c|c|c|} \hline 1 & 1 & 0 & 0 \\ \hline \end{array} \parallel \begin{array}{|c|} \hline \text{252-bit } x \\ \hline \end{array} \parallel \begin{array}{|c|} \hline \text{8-bit } t \\ \hline \end{array} \parallel \begin{array}{|c|} \hline [0]^{248} \\ \hline \end{array} \right)$$

$$\text{PRF}_{a_x}^{\text{addr}}(t) := \text{SHA256Compress}()$$

$$\text{KA.FormatPrivate}(x) := \text{clamp}_{\text{Curve25519}}(x)$$

$$\text{KA.DerivePublic}(n, q) := \text{Curve25519}(n, q)$$

$$\text{KA.Agree}(n, q) := \text{Curve25519}(n, q)$$

$$\text{KA.Base} := 9$$

KA.Base is the public byte sequence representing the Curve25519 base point. Using these definitions, the definitions for how to derive the transmission key and the incoming viewing key can be written as:

$$a_{pk} := \text{PRF}_{a_{sk}}^{\text{addr}}(0)$$

$$sk_{\text{enc}} := \text{KA.FormatPrivate}(\text{PRF}_{a_{sk}}^{\text{addr}}(1))$$

$$sk_{\text{enc}} := \text{KA.DerivePublic}(sk_{\text{enc}}, \text{KA.Base})$$

**Transactions** In order to create an unlinkable transaction, a user generates an unlinkable signing token, using their derived certificate. The token is used to sign the transaction, which will then be verified and accepted to the blockchain. This subsection will detail how signing tokens are generated, and how they can be used to create transactions.

Signing tokens are generated as follows:

$$\text{SigningToken}_{\text{rcm}}(a_{pk}, v, \rho) := \text{SHA-256}\left(\begin{array}{|c|c|c|c|c|} \hline 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array} \parallel \begin{array}{|c|} \hline \text{256-bit } a_{pk} \\ \hline \end{array} \parallel \begin{array}{|c|} \hline \text{64-bit } v \\ \hline \end{array} \parallel \begin{array}{|c|} \hline \text{256-bit } \rho \\ \hline \end{array} \parallel \begin{array}{|c|} \hline \text{256-bit rcm} \\ \hline \end{array} \right)$$

Additionally  $\text{SigningToken.GenTrapdoor}()$  can be used to generate the uniform distribution on  $\text{SigningToken.Trapdoor}$ .

It is essential that signing tokens are only used once.

**Proof and Verification** The proving algorithm uses the proving keys  $\text{ZK.ProvingKey}$ , and the transaction inputs  $\text{ZK.SatisfyingInputs}$  and is of the form:

$$\text{ZK.ProvingKey} \times \text{ZK.SatisfyingInputs} \rightarrow \text{ZK.Proof}$$



The prover takes a proving key,  $pk$ , as an input in order to produce a proof  $\pi$ , as defined in Ben-Sasson et al. [2013], which is written as follows:

264-bit $\pi_A$	264-bit $\pi'_A$	520-bit $\pi_B$	264-bit $\pi'_B$	264-bit $\pi_C$	264-bit $\pi'_C$	264-bit $\pi_K$	264-bit $\pi_H$
-----------------	------------------	-----------------	------------------	-----------------	------------------	-----------------	-----------------

The proof can then be verified. The verifying algorithm consists of the verifying key  $ZK.VerifyingKey$ , a primary input  $ZK.PrimaryInput$ , and the proof generated by the proving algorithm  $ZK.Proof$  and is of the form:

$$ZK.VerifyingKey \times ZK.PrimaryInput \times ZK.Proof \rightarrow \mathbb{B}$$

The verification of the proof is done by checking to see that it matches the conditions defined by Ben-Sasson et al. [2013], as well as checking that the lead byte is of the required form; that the remaining bytes encode a big-endian representation of an integer in  $\{0..q_{\mathbb{S}}\}$  or  $\{0..q_{\mathbb{S}}^2\}$ ; and that the encoding represents a point in  $\mathbb{G}_1^{(r)*}$  or  $\mathbb{G}_2^{(r)*}$ , and that it is of order  $r_{\mathbb{G}}$ .

# Chapter 6

## Discussion

This section will discuss the two main parts of this paper. First, a discussion regarding what elements effect perceived trust in blockchain, zero-knowledge proof, and information online is discussed. Secondly, a section discussing the technical aspects of the system presented in section 4.3 and how it effects privacy and security is presented. In addition, a section discussing the strengths, weaknesses, and limitations of this work is presented.

### 6.1 Perceived Trust in a Technical System

From both the related work presented in chapter 3 and the results of this work presented in section 5.1 and section 5.2 it is clear that many factors effects perceived trust in a system. Everything from perceived privacy and security to colors and logos effects how trustworthy a system feels to a user. In this section the results of this study will be discussed and compared to the related work. The potential implications of this for academia and industry will also be presented.

#### 6.1.1 RQ1: Elements that Enhance Perceived Trust

This section will discuss the results related to RQ1. The main finding is that visual factors play a big role for users when developing trust. Logos and icons from trusted third-parties are also an important factor for users when determining how trustworthy they perceive a system. In addition, is the effect on perceived security and privacy, and how it affects trust discussed.

### Signifiers and Graphical Elements Effect on Trust

Signifiers and graphical elements refer to the visual components of a website. This is logos, icons, pictures, colors, fonts and so on. From the results collected for this paper it is clear that this is an obvious factor that effects trust greatly. This is in line with the related work by Seckler et al. [2015], where the authors found that these visual elements all effected the users perceived trust and their attitude toward the site. This is also in line with the findings presented in section 5.1 where a majority of the interview objects expressed increase trust by the use of logos and icons. The interview objects also explained how colors like blue and green increased trust, while red could decrease it. This is also in line with the findings from Seckler et al. [2015].

Professionalism is one of the elements of the trust model presented in section 2.1. Professionalism is a wide term, but in this case it refers to the perceived professionalism a user feels toward a company or brand, and this is in most cases tied together with visual cues like the usability of an app or the quality of the photography used. Conceptual model of trust presented by Mahmood [2006] states that increased professionalism will increase trust for the users. This is similar to the findings form Seckler et al. [2015]. This statement is also supported by our findings in the interviews.

The use of third-party actors is shown to increase trust both in this work, but also in Seckler et al. [2015] and Flavián and Guinalú [2006]. This is shown in our work by logos used from IBM, Blockchain Council, and Hyperledger Sawtooth that multiple users felt that by having logos there that the given company had endorsed the system or participated in the development. This increased perceived trust for the interview objects.

Fairtrade also needs to be mentioned when talking about trusted third parties. As an independent trusted third party, the brand is self carries integrity and trust among the consumers, this is also true for the  $n = 15$  interview objects we talked to. That being said, the proposed solution in section 4.1.2 suggests a way where the trust can be placed in a technical solution instead of the manual organization of Fairtrade. The research design explained in section 4.2 is developed in such a way that one of the factors that will be investigated is how trust in a purely technical solution compares to an independent third party based on manual work conducted by employees in the organization. All the interview objects expressed trust in Fairtrade, but several flaws were also presented like it is hard for one single organization to track all deliveries and all payments all the time, and therefore it might be possible that some products get the Fairtrade certificate when the farmer did not get paid fair for the product. Even though many interview objects saw potential issues with Fairtrade, they also said that they feel a strong trust in the brand. When asked how trustworthy they consider a technical system that, based on

self-reported information from the farmers, gave information about fair trade or not the interview objects expressed that they would find this trustworthy, but many also expressed that they still think they would trust Fairtrade more. The reason for this seems to be that the interview objects are more trusting of humans than machines. They did still say they would experience trust towards the technical system if they could trust that the information actually came directly from the farmer, and was not generated by the distributors. This identifies a crucial element to consider when developing systems for trust, and that is how important it is that the users of that system understand enough to internally conclude that the system is trustworthy.

The implications for signifiers and graphical elements are clear for the industry. If a company or brand wants to increase their trust among users in digital spaces an easy way to do this is to improve their visual profile, the user experience, and the user interfaces of their platforms. They can also work to improve how professional they are perceived by the users. This can be done with the improvement mentioned above, but can also be done by marketing efforts to increase the perceived trust in the brand that in turn will increase the trust in the digital services they provide.

### **Perceived Privacy and Security Increase Trust**

The results also indicate that when interview objects perceived something as secure, or that they perceived that their privacy was handled in a satisfying way this increased their trust in the system. What elements that made an interviewee perceive this to be true varied. For some just mentioning that they stayed anonymous to every other user in the system was enough and they perceived this system as private and hence an increase in trust towards the system. In other interviews, the interview objects said that the usage of blockchain made them perceive the system as secure and this again made them trust the system. Other variations of this sort of reasoning were also expressed by other interview objects.

This shows an interesting finding, and that is that users of a system will use their perception of security and privacy to determine if they trust a system or not. From an individual standpoint with limited knowledge about what security and privacy this perception, and the following conclusion regarding trust, can be far off. This might be the only accessible way for a user to determine trust in a system, even though it's not necessarily based on a correct perception of security and privacy. Shin [2019] has a similar finding for the effect of perceived security and privacy on trust. The author also shows that perceived security and privacy in addition to trust have an effect on attitude to blockchain, and this attitude has an effect on the user's intention to adopt blockchain technology. This means that if the user perceives something as secure and private this would increase the trust in the system, and this will lead to a better attitude toward the

technology and faster adoption. This has clear implications for cases where the goal is to increase trust in blockchain or improve adoption in blockchain solutions.

### **6.1.2 RQ2: Technical Details and Explanations to Enhance Trust**

This section will discuss the results related to RQ2. Firstly, a discussion related blockchain as a basis for supply chain systems and how this relates to perceived trust for a user is presented. Afterwards, a thorough discussion related to presentation of technical details and explanation of the system is presented. Here the key finding is that users prefer to be able to access all the information, but it has to be done in a way where they can get a brief explanation first and they click into more details later. This is to prevent information overload, which seems to decrease trust.

#### **Supply Chain Transparency**

The key motivation to use blockchain in supply chains is that it increases transparency and integrity regarding the origin, production, and transportation of a product. This is true for our work, but also for work like Montecchi et al. [2019] and Yeh et al. [2019]. The reason why blockchain can provide these features is explained in section 2.5, but how this transparency and integrity effects trust in the product and supply chain is reviewed in both Montecchi et al. [2019] and Yeh et al. [2019]. Both works point to potentially lower risk for consumers to buy a product because more aspects of the product's life are accessible to the consumer, this in turn can lead to higher purchasing intent with consumers.

The current work on this paper did not focus specifically on how transparency into the life cycle of a product increases trust in the supply chain, product, or brand, but rather how transparency increased trust in the technology itself. For the first round of interviews, there was no indication that increased product transparency increased trust in the technology, but when prototypes 1.5 and 2.7 were tested 5 of the interview objects expressed that the way data was presented increased trust in the underlying blockchain system. They said that both the data visualization where origin and payment were shown, and the transaction data from the blocks increased their trust in the integrity of the blockchain. The same is argued by Yeh et al. [2019].

Yeh et al. [2019] points to two important issues to be able to succeed with blockchain usage in the supply chain. The first is for both consumers and companies to find value in using blockchain. It is argued that providing transparency increases purchasing intent with the consumers and that gives value for blockchain usage for companies. For consumers, the value with blockchain comes from lower risk and increased trust in the product, but this is dependent on the consumers trusting blockchain. Therefore it is im-

portant to find out what drives consumer trust in blockchain. This development of trust is the second important factor illustrated by Yeh et al. [2019] to succeed with blockchain. Our work supports the idea from these other blockchain based supply chain systems regarding the fact that increased transparency and tractability, through a technology like blockchain, increase the trust in the good.

### **System Explanation Influences Trust**

As mentioned previously, our findings show it is important to provide enough information for the users so they are able to themselves conclude whether or not a system is trustworthy. What a user needs to make this conclusion is widely different. 5 of the interview objects were satisfied with it just being stated as a fact while 4 interview objects did not trust any of the features before they understood all the details.

Our findings show that most of our interview objects had a preference for an approachable explanation of the technical aspects of the system. With that being said it was also clear that a wide majority, 13 out of 15, of the interview objects also thought that the more information accessible about the workings of the system the better. This was clear in the expressed demand for a combination of prototypes 1.3 and 1.4, and 2.3 and 2.4 so that the users could view an approachable explanation first and take a deep dive if they wanted. This was again confirmed with the consensus amongst the interview objects that the new prototypes 1.5 and 2.7 were more trustworthy than the previous one because of this more comprehensive explanation. The use of blockchain data also increased trust towards the system because the users felt they could get a more in-depth understanding of the data and how it was stored if they felt this was necessary.

This finding echoes some of the findings from Kizilcec [2016] where the authors show that more transparency into the system increases trust. This increase in trust only happens when the user's expectations for the system were violated, something that is not tested in our research. Still, the same trend with increase in trust if the users get enough information is there. Where our work and Kizilcec [2016] differs is that our work indicates that more information about the workings of the system means more trust in the system, while Kizilcec [2016] has results that indicates that too much transparency again starts to decrease the trust a user feels towards the system. As the author self points out, this can be because of the way the research is designed with the highest level of transparency showing what grades their peers gave them in a peer grading system, and because of potential shame in the results from their peers, this can lower trust. Our research does not have any possibilities of too much transparency reflecting badly on the user, and this can be one possible explanation for the different results. The two works also differ in the way that Kizilcec [2016] has a violation of expectations when testing, while our work does not. Investigating how a violation like this would effect

our results could be interesting. This could be done with for example giving half the interview objects the output that the coffee was not Fairtrade.

Both our and Kizilcec [2016] work imply that information transparency into how a system and algorithm works increases trust. Our work differs from related work with the finding that it seems like users feel increased trust the more information and details they get, something that is different from Kizilcec [2016]. This need for transparency and details came with the need for the information to be presented in a way that did not give information overload by presenting layered information where it starts with an overview and then can go into more details if they want. This find is, to our knowledge, novel. All 15 interview objects also preferred the way of explaining the system in prototype 2.4 over prototype 1.4 because they had increase trust when the focus was on the benefits of the technology, and not the math and technical details. This seems also to be a novel finding that has implications to increase trust in emerging technologies by focusing on why it is used, and not how it works. Presenting transaction data from the blockchain increased trust in the system too, if it was presented in a way that did not scare the users off by looking like an error message. This finding that blockchain-specific data can enhance trust is, to our knowledge, also a novel finding because the impact on blockchain data and details impact on trust has not been studied.

This has implications for the industry for many new technical solutions like blockchain. If adding approachable learning material is a way to increase trust because users are then able to draw their own conclusion about the trustworthiness of the system then this is an easy way to better trust. Our work also indicates that approachable explanations are the most trustworthy, so interactive graphics or videos could potentially increase trust even more.

### **6.1.3 RQ3: Unlikable Transactions and High Level of Privacy with Blockchain**

Throughout the research and following system design, it has come clear that the methods for implementing such a privacy oriented system as in this thesis exist and are being studied. However, it is also clear that the scope of existing systems are limited or focus on different use cases with different requirements. The various aspects of these systems and how they compare to the solution in this thesis will be discussed in this section.

The main contributions relating to the third research question are as follows:

- A research on the current state of privacy-preserving methods in blockchain systems has been conducted with a focus on zero-knowledge proof and off-chain data storage, in order to supplement findings from the interviews.

- This research uncovered that the methods needed for such a system exist, however they needed to be tailored to fit the use case in this thesis.
- A system for implementing unlinkable transactions and storing data in an off-chain database has been designed.
- The system has been tested on test networks on a limited scale.

Existing research shows that there are clearly methods for increasing privacy and security in blockchain systems, however, it can come at the cost of efficiency or decentralization, as described in Goldfeder et al. [2017]. These aspects have however not been covered in detail in this thesis. There are several additional challenges which such implementations, notably ensuring that they are secure, and that they do not break the logic of the blockchain.

Storing data off-chain is a relatively simple process. It can definitely be expanded upon in several ways, using a variety of frameworks and models for database storage. These aspects have been discussed in related works, as described in Kumar et al. [2020].

Related works on the usage of zero-knowledge proofs in blockchain is limited, and the most influential implementation is detailed in Ben Sasson et al. [2014]. While this research gives a lot of insight into the use of zero-knowledge proofs in blockchain systems, the scope differs quite a bit from what has been done in this thesis. Most notably, the implementation in this thesis is not concerned with the monetary value in transactions, as is the case for Ben Sasson et al. [2014]. This fact reduces the complexity of the system in handling of transactions, making it potentially more easily implementable in other systems. However, it does not notably increase system efficiency, but it might reduce overhead comparatively. Compared to traditional blockchain systems such as Nakamoto [2009] and Buterin [2013], the privacy aspects add additional layers of proof and verification to the overall system.

## 6.2 Limitations and Assumptions

This section will cover the limitations and assumptions made throughout the thesis for the research conducted and the results presented.

### 6.2.1 Interviews and User Tests

There are limitations for this work into perceived trust. The limited size for the interviews is one. All interview objects were Norwegian, and a majority were from a similar age range. The research was also conducted in a specific use case. To address these limitations similar user tests should be conducted on a bigger sample size outside of



Norway and in a bigger age range. Similar research should also be conducted in different use cases to see how trust is developed in other scenarios.

### 6.2.2 Use Case: Fairtrade - Blockchain

There are also simplifications done to the system with plantation workers, distributors, and consumers. These simplifications are done to make the system more understandable for the interview objects make it easier to focus on the important factors of the user testes which is what affects trust. The main simplifications done in this ecosystem are:

- The way the proposed system works now is that the plantation worker is the only one that provides the information of how much they get for the coffee. This can be a potential problem if this system is to be used in a real supply chain because there could be a scenario where the plantation worker lie about the payment and there would be no efficient way to catch this lie. To make this system robust to this potential problem the distributor would also have to upload how much they paid for the given coffee, and if the payment value provided by the plantation worker and the distributors is not the same that transaction would be labeled as a potentially faulty transaction.
- In this system it is assumed that the distributors and consumers would be fine with the plantation worker providing unlinkable information in transactions to the blockchain. We have not tested if this assumption holds, but this assumption does not affect the user tests and interviews even if it was wrong. It would have to be addressed if this system was to be used in an actual supply chain.
- There is no functionality proposed in the system to prevent distributors from just printing a product code from a fair batch of coffee on all bags. This is an issue that needs to be addressed in this use case for blockchain. One possible way to address this is to have the product codes be generated based on how much coffee they buy. For example, if they buy 4 tons of coffee they get enough valid codes to pack an equivalent amount of coffee. This loophole was mentioned by 3 interview objects, but they were asked to assume that there was a fix for this so it did not have a noticeable impact on the results. It would have to be addressed and fixed before launching this blockchain-based supply chain.

These simplifications and assumptions did not affect the user tests and interviews noticeable. The presented use case for the two roles would stay the same for these interview objects even if these simplifications were addressed. But these assumptions and simplifications must be addressed if this system is gonna be used in a real supply chain with real transactions.

### **6.2.3 System Implementation**

The system design is still a proposed model with limitations in terms of scope and also generalizability. Based on existing research it is assumed that the system is scalable. In order for unlinkability to be as useful as possible in a system like this it, it is also required that the system is of a certain scale.

# Chapter 7

## Conclusion and Future Work

Throughout this study the three research questions presented in 1.3 have been addressed. This results of this study are structured into two sections, one concerning perceived trust and one concerning system design. The perceived trust section addresses whether users would trust this system design and what would be required for them to use it to submit potentially sensitive data. The system design addresses the need for privacy-preserving methods in blockchain networks and how this can be utilized.

The results show that for RQ1 there are many and varied answers to what affects a user's trust in the system. The most important factors were found to be all the visual components, branding, third-party endorsements, perceived security and privacy, and the user's understanding of the system and technology. All these factors can be used to improve the perceived trust of a system giving the findings clear applications for industry. RQ2 is a deep-dive into one of the findings from RQ1 regarding the user's understanding of the system and technology. From the results, the conclusion is that the more transparent a system is into the inner workings the more trustworthy a user perceives the system. It is also clear that there is a potential for information overload for the users, so there is a preference for what can be referred to as layered information. This means that users prefer to first be presented with a brief overview, and then be able to click into more in-depth information if needed. It was clear that having all the information accessible was trust increasing for the users since they did not feel anything was hidden from them. This conclusion is supported by the improvement for prototypes 1.5 and 2.7 from the second step of the interviews. There needs more research into how transparency into technology, systems, and algorithms affects trust.

The same preference for the details to be hidden by default can be seen by the feedback received regarding the blockchain data. In prototypes 2.5 and 2.6 where the blockchain data was presented by default, a majority of the users commented that it was interesting

and useful information, but that it should be hidden and only displayed if the user wanted it. This was supported by the strong approval for prototypes 1.5 and 2.7 where blockchain data was hidden by default and the users could access it by a button. This strengthens the conclusion that information and transparency increase trust.

The system implementation, while limited and not ready for a large scale implementation, shows promising results when it comes to dealing with privacy issues in blockchain systems. Hiding sensitive data from the users of the system is applicable to a wide variety of blockchain systems. This combined with unlinkability is a viable solution to a range of privacy issues related to blockchain. This solution is still able to utilize a lot of the strengths of blockchain systems, in particular.

In the future this model could be more generalized for a variety of blockchain systems and implementations. Additionally, one could explore whether these methods or similar methods could be applicable in other fields. Other types of future work could be doing large scale testing of system implementations. This tests could check for efficiency, throughput, overhead load and similar properties. Testing could also cover issues related to security attacks, such as 51% attacks.

In this thesis an overview of a potential privacy-preserving blockchain model for supply chain networks has been presented. The study has looked into both the technical aspects such a network would require, as well as whether users would trust such a system to appropriately handle their data and what it would require for them to do so. Future work has been addressed as well as limitations and potential improvements.

# Bibliography

- Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct non-interactive zero knowledge for a von neumann architecture. Cryptology ePrint Archive, Report 2013/879, 2013. <https://ia.cr/2013/879>.
- Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474, 2014. doi: 10.1109/SP.2014.36.
- Daniel Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. volume 2, pages 124–142, 09 2011. ISBN 978-3-642-23950-2. doi: 10.1007/978-3-642-23951-9\_9.
- Daniel J Bernstein. Curve25519: new diffie-hellman speed records, 2006.
- Daniel J. Bernstein, Simon Josefsson, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. EdDSA for more curves. Cryptology ePrint Archive, Report 2015/677, 2015. <https://ia.cr/2015/677>.
- Blockchain-Council. Blockchain Council Home Page. URL <https://www.blockchain-council.org/>. Accessed: 2021-12-31.
- Vitalik Buterin. Ethereum whitepaper, 2013. URL <https://ethereum.org/en/whitepaper/>.
- Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance, 1999.
- Mingxiao Du, Xiaofeng Ma, Zhe Zhang, Xiangwei Wang, and Qijun Chen. A review on consensus algorithm of blockchain. volume 2017-January, pages 2567–2572. Institute of Electrical and Electronics Engineers Inc., 11 2017. ISBN 9781538616451. doi: 10.1109/SMC.2017.8123011.
- Ethereum. Ethereum mainnet for enterprise, May 2021. URL <https://ethereum.org/en/enterprise/>.

- Fairtrade-International. Fairtrade International Home Page. URL <https://www.fairtrade.net/>. Accessed: 2021-12-31.
- Figma. Figma Home Page. URL <https://www.figma.com/>. Accessed: 2021-12-31.
- Hal Finney. Reusable proofs of work, 2004. URL <https://nakamotoinstitute.org/finney/rpow/index.html>.
- Carlos Flavián and Miguel Guinalú. Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management amp; Data Systems*, 106:601–620, 6 2006. ISSN 0263-5577. doi: 10.1108/02635570610666403.
- Nguyen Giang-Truong and Kim Kyungbaek. A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, 14(1):101–128, 02 2018.
- Steven Goldfeder, Harry A. Kalodner, Dillon Reisman, and Arvind Narayanan. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *CoRR*, abs/1708.04748, 2017. URL <http://arxiv.org/abs/1708.04748>.
- Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 1994. doi: 10.1007/BF00195207.
- Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *J. ACM*, 38(3): 690–728, July 1991. ISSN 0004-5411. doi: 10.1145/116825.116852. URL <https://doi.org/10.1145/116825.116852>.
- Barbara Guttman and E Roback. An introduction to computer security: the nist handbook, 1995-10-02 1995.
- Hyperledger. MSP Implementation with Identity Mixer. <https://hyperledger-fabric.readthedocs.io/en/release-2.2/idemix.html>, 2020.
- Hyperledger-Sawtooth. Hyperledger Sawtooth Home Page, 2019. URL <https://sawtooth.hyperledger.org/>. Accessed: 2021-12-31.
- Paul Johannesson and Erik Perjons. *An introduction to design science*. Springer, 2014.
- Daniel Jones. A zero-privacy to zero-knowledge society, 2019. URL <https://www.ibm.com/blogs/blockchain/2019/07/a-zero-privacy-to-zero-knowledge-society/>. Accessed: 2021-12-31.
- S. Josefsson and I. Liusvaara. Edwards-curve digital signature algorithm (EdDSA). 1 2017. doi: 10.17487/RFC8032. URL <https://www.rfc-editor.org/info/rfc8032>.

- René F. Kizilcec. How much information? Effects of transparency on trust in an algorithmic interface. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 2390–2395, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450333627. doi: 10.1145/2858036.2858402. URL <https://doi.org/10.1145/2858036.2858402>.
- Randhir Kumar, Ningrinla Marchang, and Rakesh Tripathi. Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and Blockchain. In *2020 International Conference on COMMunication Systems NETWORKS (COMSNETS)*, pages 1–5, 2020. doi: 10.1109/COMSNETS48256.2020.9027313.
- Juan Carlos López-Pimentel, Omar Rojas, and Raúl Monroy. Blockchain and off-chain: A solution for audit issues in supply chain systems. In *2020 IEEE International Conference on Blockchain (Blockchain)*, pages 126–133, 2020. doi: 10.1109/Blockchain50366.2020.00023.
- Omer Mahmood. Trust: From sociology to electronic environment. *JITI Journal of Information Technology Impact*, 6:119–128, 2006.
- Matteo Montecchi, Kirk Plangger, and Michael Etter. It's real, trust me! Establishing supply chain provenance using blockchain. *Business Horizons*, 62:283–293, 5 2019. ISSN 0007-6813. doi: 10.1016/J.BUSHOR.2019.01.008.
- Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at <https://metzdowd.com>*, 3 2009. URL <http://www.bitcoin.org/bitcoin.pdf>.
- Giang Truong Nguyen and Kyungbaek Kim. A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, 14:101–128, 2018. ISSN 2092805X. doi: 10.3745/JIPS.01.0024. URL <https://doi.org/10.3745/JIPS.01.0024>.
- Christian Reitwiessner. zkSNARKs in a nutshell. *Ethereum blog*, 6:1–15, 2016.
- Fahad Saleh. Blockchain without waste: Proof-of-stake. *The Review of Financial Studies*, 7 2020. ISSN 0893-9454. doi: 10.1093/rfs/hhaa075. URL <https://academic.oup.com/rfs/advance-article/doi/10.1093/rfs/hhaa075/5868423>.
- Mirjam Seckler, Silvia Heinz, Seamus Forde, Alexandre N. Tuch, and Klaus Opwis. Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior*, 45:39–50, 4 2015. ISSN 0747-5632. doi: 10.1016/J.CHB.2014.11.064.

- Don D.H. Shin. Blockchain: The emerging technology of digital trust. *Telematics and Informatics*, 45:101278, 2019. ISSN 0736-5853. doi: <https://doi.org/10.1016/j.tele.2019.101278>. URL <https://www.sciencedirect.com/science/article/pii/S0736585319307701>.
- William Stallings. *Cryptography and network security : principles and practice, seventh edition*. Harlow, Pearson Education, 2017.
- Kuttimani Tamilmani, Nripendra P. Rana, Samuel Fosso Wamba, and Rohita Dwivedi. The extended unified theory of acceptance and use of technology (utaut2): A systematic literature review and theory evaluation. *International Journal of Information Management*, 57:102269, 2021. ISSN 0268-4012. doi: <https://doi.org/10.1016/j.ijinfomgt.2020.102269>. URL <https://www.sciencedirect.com/science/article/pii/S0268401220314687>.
- Zheng Yan and Silke Holtmanns. Trust modeling and management: From social trust to digital trust. <https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-59904-804-8.ch013>, pages 290–323, 1 2008. doi: 10.4018/978-1-59904-804-8.CH013. URL <https://www.igi-global.com/chapter/trust-modeling-management/6870>[www.igi-global.com/chapter/trust-modeling-management/6870](https://www.igi-global.com/chapter/trust-modeling-management/6870).
- Jen-Yin Yeh, Ssu-Chi Liao, Yu-Ting Wang, and Yin-Jia Chen. Understanding consumer purchase intention in a blockchain technology for food traceability and transparency context. pages 1–6, 2019. doi: 10.1109/SITIM.2019.8910212.
- Zero-knowledge Cryptography in Rust. bellman. <https://github.com/zkcrypto/bellman/>, 2021.
- Kaiwen Zhang and Hans-Arno Jacobsen. Towards dependable, scalable, and pervasive distributed ledgers with blockchains (technical report). 2018.
- Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14:352, 10 2018. doi: 10.1504/IJWGS.2018.095647.
- Botao Zhong, Wu Haitao, Lieyun Ding, Hanbin Luo, Ying Luo, and Xing Pan. Hyperledger fabric-based consortium blockchain for construction quality information management. *Frontiers of Engineering Management*, 7, 08 2020. doi: 10.1007/s42524-020-0128-y.



# Appendix A

## Link to Clickable Prototypes

### A.1 Data provider

Prototype 1.1:

<https://www.figma.com/proto/MMiDMMH16UbtLSJnSYtQ05/Data-Provider-%7C-Barebone?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

Prototype 1.2:

<https://www.figma.com/proto/7byfVssCVF46bfWHtY70U2/Data-Provider-%7C-Simpel?node-id=104%3A5&scaling=scale-down&page-id=0%3A1&starting-point-node-id=104%3A5>

Prototype 1.3:

<https://www.figma.com/proto/XPk8ruyHMYiPz7PGKHRj9J/Data-Provider-%7C-Graphics?node-id=102%3A2&scaling=scale-down&page-id=0%3A1&starting-point-node-id=102%3A2>

Prototype 1.4:

<https://www.figma.com/proto/nIabrJLTVSYc3SSXHRvQzU/Data-Provider-%7C-Tech-details?node-id=102%3A2&scaling=scale-down&page-id=0%3A1&starting-point-node-id=102%3A2>

Prototype 1.5:

<https://www.figma.com/proto/Zkj0GHXI4aReX4ybmyWR1r/Prototype-1.5?node-id=102%3A2&scaling=scale-down&page-id=0%3A1&starting-point-node-id=102%3A2>

## A.2 Data consumer

Prototype 2.1:

<https://www.figma.com/proto/4zbpZt5TyWHdZxmowlrRUu/Data-Consumer-%7C-Barebone?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

Prototype 2.2:

<https://www.figma.com/proto/3GrRuUZdHBFz39jddb821/Data-Consumer-%7C-Simple?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

Prototype 2.3:

<https://www.figma.com/proto/85vVUXDn2PdtdzVX0cht1Y/Data-Consumer-%7C-Graphics?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

Prototype 2.4:

<https://www.figma.com/proto/BycTn0SaX00C0yugn3a8sh/Data-Consumer-%7C-Tech-details?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

Prototype 2.5:

<https://www.figma.com/proto/WIWL7J9xrVbH9X5byBvIXf/Data-Consumer-%7C-Raw-data-1?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

Prototype 2.6:

<https://www.figma.com/proto/gGwglbmFLC3fJabPWbf0Lq/Data-Consumer-%7C-Raw-data-2?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

Prototype 2.7:

<https://www.figma.com/proto/OXRSPeTDoK0ghvZGRrTLsC/Prototype-2.7?node-id=1%3A38&scaling=scale-down&page-id=0%3A1&starting-point-node-id=1%3A38>

# Appendix B

## Interview Guide

The interview guide was originally in Norwegian and has been translated into English to be added to the appendix for reproducibility.

### B.1 Explorative Study to find Drivers of Trust

The objective of the interviews is to collect information to help answer RQ1 and RQ2. This is done through semi-structured interviews where the interview objects are free to talk about what they find relevant to the topic at hand, and the interviewers ask follow-up questions and guide the conversation to the more relevant topics. The 10 prototypes gave structure and format for the interviews.

The interviews start with introducing the following:

1. Introduction of the interviewers: name, occupation, and field of study.
2. The interview object presents them self.
3. Context and format of the interview are presented. Duration: 45-60 minutes; will not be recorded; will stay anonymous; notes will be taken and they get to read the notes later to confirm they are correct; and that their time is appreciated.
4. The use case is presented. The use case explained in ?? is the use case presented for the interview objects.
5. The format of the interview is explained. Definition of trust; the interview objects should say what comes to mind and not filter themselves; that feedback related to fidelity of the prototypes is welcome, but not the most important; and that they will click through 4 prototypes for the data provider and 6 for the data consumer.

The interviews and user test was designed for the interview objects to talk more or less freely. And in most cases, they provided answers to all our questions without us having to ask them. When they did not we had to ask open questions to get them going. Under is a list of all the 10 prototypes and a brief, not full-fledged, list of the key topics we wanted the interview object to touch on.

### **B.1.1 Data Provider**

Reiterate the role of the farmer/data provider in the system.

#### **Prototype 1.1**

Have the interview object reflect on what they think they need to have increased trust in the system. Reflect on what about this prototype that lowers trust, if any. This prototype provides a basis to compare the rest of the prototypes.

#### **Prototype 1.2**

Have the interview object reflect on how the logo and the link to an article about the given topic affect their trust in the system. We also wanted them to comment on the sentence that was added, especially how they felt about the fact that they were just invited to accept this as a fact and how it affected trust.

#### **Prototype 1.3**

Have the interview object comment on the brief explanation of the system over the “Click to learn more”-button. Have the interview object talk about the way of representing first a brief explanation and then a button where they can learn more, and how this affects trust. Have the interview object reflect on the graphical way of representing the system and how this affects their trust in the system, technology, blockchain, and zkp.

#### **Prototype 1.4**

Have the interview object reflect on the written way of representing the system and how this affects their trust in the system, technology, blockchain, and zkp.

The interview object rates the 4 prototypes from most to least trustworthy. Encourage them to formulate why they ordered the prototypes in the given way.

### **B.1.2 Data Consumer**

Reiterate the role of the consumer/data consumer in the system.

**Prototype 2.1**

Have the interview object reflect on what they think they need to have increased trust in the system. Reflect on what about this prototype that lowers trust, if any. This prototype provides a basis to compare the rest of the prototypes.

**Prototype 2.2**

Have the interview object reflect on how the logo and icon used affect their trust in the system. Especially interesting is how the interview object experience these two lesser know logos compared to the logo from IBM. It is also interesting to find out what associations they get to Certified Blockchain Council and how this relates to trust in the system. We also wanted them to comment on the sentence that was added, especially how they felt about the fact that they were just invited to accept this as a fact and how it affected trust.

**Prototype 2.3**

Have the interview object comment on the brief explanation of the system over the “Click to learn more”-button. Have the interview object talk about the way of representing first a brief explanation and then a button where they can learn more, and how this affects trust. Have the interview object reflect on the graphical way of representing the system and how this affects their trust in the system, technology, and blockchain.

**Prototype 2.4**

Have the interview object reflect on the written way of representing the system and how this affects their trust in the system, technology, and blockchain. During this prototype, the interview object was encouraged to reflect on their preference for what to focus on during an explanation of the system and what way was most trustworthy. The difference is that prototype 1.4 is very much focused on the details and math, while 2.4 is more focused on what features this technology provides.

**Prototype 2.5**

In this prototype, the goal was to see how the interview object reacted when presented with blockchain data in the form of a hash value and how this affected trust. If they think the additional data is trustworthy then why is it trustworthy, and if it is not more trustworthy then why? And what would make it more trustworthy?

### **Prototype 2.6**

In this prototype, the goal was to see how the interview object reacted when presented with blockchain data in the form of transaction data and how this affected trust. If they think the additional data is trustworthy then why is it trustworthy, and if it is not more trustworthy then why? And what would make it more trustworthy?

The interview object rates the 6 prototypes from most to least trustworthy. Encourage them to formulate why they ordered the prototypes in the given way.

## **B.2 Re-interview and User Test of Improved Prototypes**

The goal of this round of interviews is to check if the improved prototypes based on findings from the explorative study actually increased trust for the interview object. The format was a short interview of 10-15 minutes where two new prototypes were presented: one for the data consumer (prototype 1.5) and one for the data provider (prototype 2.7). The main question to be answered was if they found prototype 1.5 more trustworthy than all prototypes 1.1-1.4, and if they found prototype 2.7 more trustworthy than all prototypes 2.1-2.6. Follow-up questions regarding why, what they found more trustworthy, what they found less trustworthy, and so on were added when needed.

# Appendix C

## Link to Code Repository

The repositories in which coding work on this thesis was conducted can be found in the following Github-project:

<https://github.com/Blockchain-Privacy-Thesis>

This project consists of two repositories, one for the blockchain and one for the zk-SNARKs respectively:

<https://github.com/Blockchain-Privacy-Thesis/blockchain-off-chain>

<https://github.com/Blockchain-Privacy-Thesis/zksnark>

