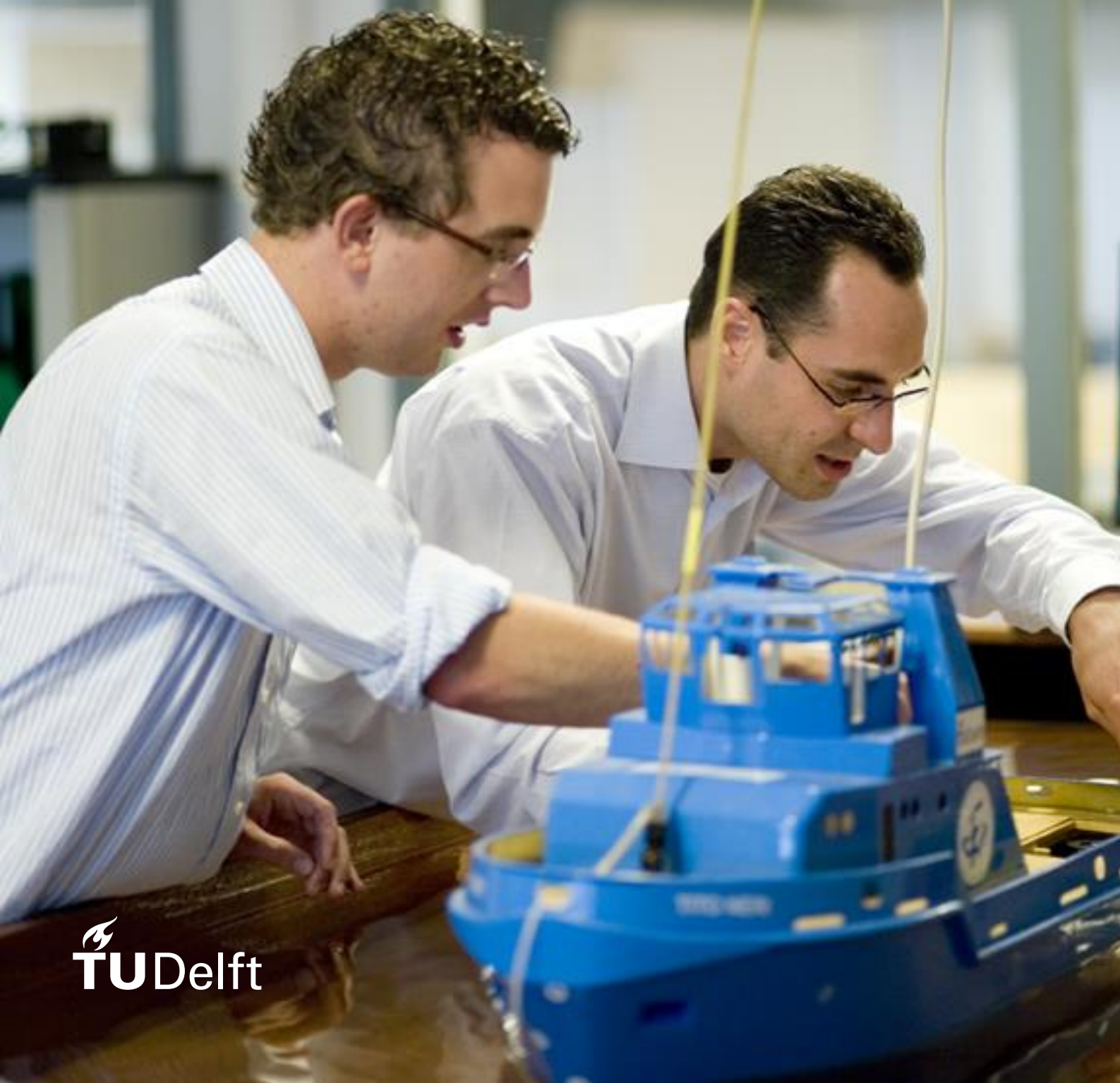


Opportunities of Blockchain In Certification Management



-This page is intentionally left blank-

Opportunities of Blockchain in Certificate Management

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in Complex Systems Engineering and Management

Faculty of Technology, Policy and Management

by

Aravindakshan Ramesh

Student number: 4627423

To be defended in public on 23rd September 2020

Graduation committee

Chairperson & First Supervisor : Prof.dr.ir. I.R. van de Poel, Ethics/Philosophy of Technology
Second Supervisor : Dr. A.Y.Ding, Information and Communication Technology
Daily Supervisor : Dr. P. Hayes, Ethics/Philosophy of Technology

-This page is intentionally left blank-

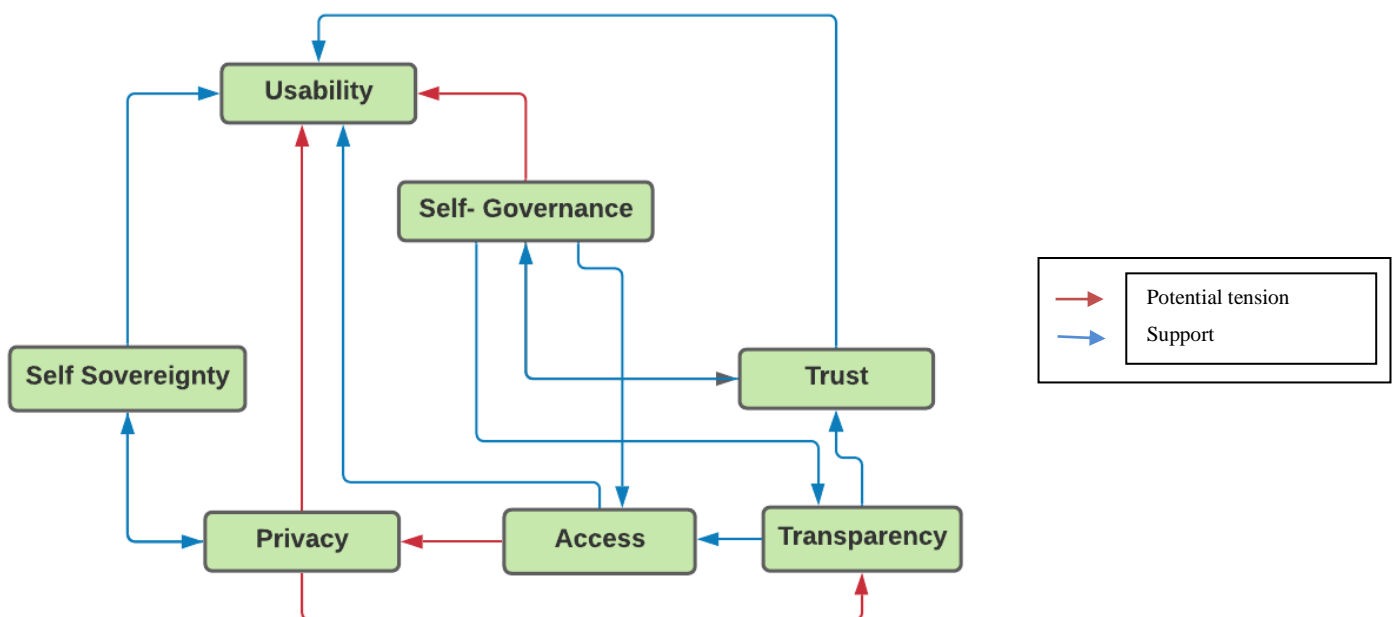
Executive Summary

Recent developments in information technology such as artificial intelligence and machine learning allow the storage and processing of gigabytes of personal data allowing the possibility of a range of negative effects. Centralized digital solutions have proved to have massive data leaks in the past. Blockchain technology is proposed as a solution that allows shift of ownership of data to an individual level through its decentralized architecture. Certification/credential management of educational data was chosen as the use case to understand the merits and demerits of blockchain technology on a conceptual level. The objective of the research is to provide guidelines and design principles that meet the value criteria for the relevant stakeholders. The research question that was answered in this study was

” What are design principles for blockchain for administrative educational purposes that help to meet relevant values?”.

To answer this main question, the research followed the sequential steps of Value Sensitive Design and the data to curate the methodology stemmed from literature review and expert interviews. The rationale to use VSD to evaluate the design process is that efforts to regulate or influence a technology leads to a dilemma. An information problem where impacts cannot be anticipated without a widespread use of the technology and a power problem where control is complicated when the technology has become established. This is called a Collingridge dilemma. Hence integrating values in design seeks to improve the functionality of new design by formulating relevant design principles. The Value Sensitive Design (VSD) methodology is broken down into three stages (Empirical, Conceptual and Technical Investigations).

The empirical stage relies on inputs from stakeholders and are the main building blocks to achieve the design principles needed for a blockchain enhanced certificate management. The value inputs from stakeholders are relied upon to form the objectives to accomplish in the final design. Three values privacy, transparency and trust are the most important values for this research according to the stakeholder perspective. The benefits and challenges of using blockchain as a tool of certification management is presented in Table 3. These predefined values were contested with a literature review to compare and contrast the philosophical understanding of these values with its implication in the use context of blockchain. This gives rise to the value relations given in the figure below. A detailed explanation of these values is mentioned in the conceptual Investigation chapter.



The result of the conceptual investigation lay the foundation of the design principles which are important for the design of this application. The main design principles are provided in the table below.

| Design Principles |
|--|
| The system must promote access to the application |
| The system must promote transparency of information |
| The system must promote data identity |
| The system must promote the needs of privacy and security |
| The system needs to promote trust |

The technical investigation was used to fulfil the design. In the technical investigation (chapter 7), the application design is showcased as an example to build blockchain enhanced certification management system. Since the objectives of the design and blockchains technical complexity entail fundamental differences, the application is divided into three layers (the application layer, the database layer and the network layer) to achieve the relevant design principles mentioned above. The blockchain is used as appliance to promote trust between stakeholder and users and occupies the network layer of the application. Permission rules are embedded in the database layer in accordance with the network layer. Finally, the application layer provides the interface for users and stakeholders to use the application.

The blockchain layer uses the proof of stake as an algorithm to calculate trust between parties. The formula is presented below.

$$b = \frac{||\{C...\}||}{\sum_i |dist(R,C) - m|} , B_i = (C,D)$$

where

- b is the block relevance
- B is a list of all trust relations in the block
- C is the trusting party of entry I in list B
- D is the trusted party of entry i in list B
- $||\{C...\}||$ is the amount of different trusting parties in the block
- $dist$ is the graph distance function
- R is the root node
- m is the average graph distance to the root node of the current blockchain

The conclusion of the thesis was presented in chapter 8. Blockchain has a high complexity of technologies that does not provide solutions to all the challenges specified by the stakeholders. Hence different applications have to be used in consortium with blockchain to achieve the objectives presented. The database layer uses a distributed hash table which is built on centralized databases to leverage data mismanagement. This again poses a single point of failure resulting in further challenges.

My reflection will be that blockchain is indeed in its infancy, utilizing existing technology with blockchain brings back the issues that blockchain addresses in the first place and thus a conundrum. Legal regulations on privacy also pose problems on the decentralized nature of blockchain. As stated before, blockchain has a lot to offer in terms of its versatility of functions however at the moment public blockchain do not offer a great extent of value and also restricts usability. Private blockchain can be an immediate solution. A blockchain consortium of universities could be set up and new nodes can be added, to what extent would institutions trust and add other education providers such as online mediums remain to be questioned and studied. Limitations and recommendation of further research is also made in the conclusion chapter.

Table of Contents

| | |
|--|----|
| Executive Summary..... | v |
| List of Figures | ix |
| List of tables | ix |
| Chapter 1 - Introduction | 1 |
| 1.1 Problem Identification..... | 1 |
| 1.3 Research Approach | 2 |
| 1.4 Research Problem | 2 |
| 1.5 Knowledge Gaps..... | 3 |
| 1.6 Research Design | 4 |
| 1.8 Research Questions..... | 5 |
| 1.9 Thesis Structure..... | 6 |
| Chapter 2- Theoretical Background | 8 |
| 2.1. Blockchain | 8 |
| 2.1.1. Background and definition | 8 |
| 2.1.1. How blockchains work..... | 9 |
| 2.2. Educational Administration:..... | 11 |
| 2.2.1 Process Involved in Certification | 11 |
| 2.2.2 Limitations of (non-Blockchain) Digital Certificates | 11 |
| 2.2.3 Digital Certificates using Blockchain Technology..... | 12 |
| Chapter 3- Value Sensitive Design (VSD) – Methodology..... | 13 |
| Chapter 4- Empirical Investigation | 17 |
| 4.1 Stakeholder Analysis..... | 17 |
| 4.2 Data Analysis of Values | 18 |
| Chapter 5- Conceptual Investigation..... | 22 |
| 5.1 Conceptualization of Values..... | 22 |
| 5.1.1 Transparency: | 22 |
| 5.1.2 Privacy: | 24 |
| 5.1.3 Trust:..... | 25 |
| 5.1.4 Usability: | 26 |
| Chapter 6- Design Principles | 29 |
| Chapter 7- Technical Investigation..... | 32 |
| 7.1 Application Layer: | 32 |
| 7.2 Database Layer:..... | 32 |
| 7.3 Blockchain Layer:..... | 33 |
| 7.3.1 Trust chain: | 33 |
| 7.3.2 Proof of Stake: | 35 |

| | |
|-----------------------------|----|
| Chapter 8- Conclusion | 38 |
| Bibliography | 44 |
| Appendix | 50 |

List of Figures

| | |
|---|----|
| Figure 1 Use of technologies in education (Source: HolonIQ)..... | 3 |
| Figure 2 Research Strategy | 7 |
| Figure 3 Working structure of blockchain (Adapted from [60])..... | 9 |
| Figure 4 Value Set for Respondents | 14 |
| Figure 5 Data Collection for Conceptual Investigation..... | 15 |
| Figure 6 Stakeholders Adapted from [60]..... | 17 |
| Figure 7 Stakeholder Analysis | 17 |
| Figure 8 Relation of transparency (Source: [47])..... | 23 |
| Figure 9 Trust Chain | 34 |

List of tables

| | |
|---|----|
| Table 1 Repsondents Interviewed..... | 14 |
| Table 2 Values in blockchain | 18 |
| Table 3 Benefits and challenges of values of blockchain in certification management | 21 |
| Table 4 Research themes for design | 28 |
| Table 5 Design Goals | 29 |
| Table 6 Design Principles | 40 |

Chapter 1 - Introduction

1.1 Problem Identification

Recent developments in information technology such as artificial intelligence and machine learning allow the storage and processing of gigabytes of personal data allowing the possibility of a range of negative effects [5]. Even though the age of Big Data has provided a quantum leap in the way we communicate and interact, it has also given rise to a declining clarity and agreement on privacy and ambiguous conceptual understanding of policy, law, and ethics concerning information. Identity of an individual can be traced with very minimal information thus posing a big risk on the data security. Blockchain technology is proposed as a solution that allows shift of ownership of data to an individual level through its decentralized architecture [56].

Certification management of educational data is chosen as the used case to understand the merits and demerits of blockchain technology on a concise level. The rationale for choosing this field is two folds. Firstly, schools and colleges face high number of data breaches as students create tons of data daily ranging from different resources. Due to lack of proper treatment and protection, personal information stored in data centres risk misused management of data and data theft [57]. Secondly, education certificates are of paramount importance to individuals, and that the society has also an interest in checking their credibility. For example, the Syrian refugee crisis has created the global displacement of people, highest since the Second World War. Refugees already facing impoverished standards of living in host countries are forced to accept low wages because of the absence of official academic documents, which further aggravates their existing condition [14]. A system where people are able to prove their credentials without relying on centralised databanks, such a system would have enabled refugees to get access to the work they deserve.

1.2 Problem Background

This research investigates the practicality and limitations of blockchain applications aimed at educational certificates. Hence it is of importance to understand why blockchain could be used and how educational certificates can benefit from this novel technology.

There is a growing area of interest for blockchain technology for many businesses and institutions. It is a novel and a disruptive technology which is projected to create new business models and transcend day to day interaction [60]. Blockchain has various definitions, Meijer uses a description that combines two important features distributed computing and distributed databases. The definition states “ *A blockchain is a distributed, shared, encrypted, chronological, irreversible and incorruptible database and computing system (public/private) with a consensus mechanism (permissioned/permission less), that adds value by enabling direct interactions between users.*” ([61], pp. 6-7)”

In order to describe blockchain technology it can be compared to a spreadsheet in the sky, and each person has the most recent edition of the document, and everyone can check it. Users need to reach a shared agreement to identify its content, and each user holds a copy of the blockchain locally on their device instead of centrally storing it by one organization.

Sharples et al. positions blockchain technology as a resource of student empowerment and a prospect to re-engineer the conventional educational model [16]. Respondent D, an enterprise architect of Studielink, an organization responsible for enrolling students in educational programmes also envisaged a similar viewpoint. The respondent added that the centralized template of the current educational model is not sustainable and disintermediation of the educational arrangement is inevitable.

Blockchain can facilitate micro-accreditation thus enabling informal learning through various mediums allowing learners to use a plug and play model – studying courses at different settings either through on-premises or through an online medium. Blockchain can also act as tool for life-long learning [73].

Currently there are no applications that enable accreditation across different platforms of education. Another issue encountered during the literature survey was that validation of trust in academic credentials entails huge costs. Blockchain can serve as intermediary that promotes trust in the system. Blockchain is identified as one of the technologies that could solve this problem. However, these statements cannot be taken at face value and have to be studied in detail to understand the benefits and challenge of this technology in credential management system. The three most important values according to this research are privacy, transparency and trust. The rationale as to why these values are important and its implications on the design process is argued and explained upon in chapter 4 and chapter 5.

1.3 Research Approach

Efforts to regulate or influence a technology has a twin dilemma. An information problem where impacts cannot be anticipated without a wide spread use of the technology and a power problem where control or change is complicated when the technology has become established. This is called a Collingridge dilemma [58]. Hence, integrating values in design can be sought after as a procedure to improve the usability and functionality of a new technology and the ethical acceptability of the technology.

The Value Sensitive Design (VSD) literature contains one of the most widespread approaches to design values in technology [43]. VSD has a theoretically built method that considers values in the design process of technologies [44]. It contains a tripartite methodology that has integrated conceptual, empirical, and technical investigations to understand values for design.

VSD methodology has aided scientists and scholars to develop design principles through its tripartite approach. VSD aims to account human values such as privacy, autonomy, transparency in computer technology.[43] Empirical research helps researchers understand the stakeholder's sentiment to the technology and application context. Conceptual investigation includes theoretically exploring values making use of the data collected in the empirical research to find the values measured based on the interaction amongst respondents and the technology. The conceptual investigation also provides a basis for conceptualising the values. This is followed by the technical investigation where the technology of context is studied with an objective to comprehend how technical characteristics facilitate, assist or impede the identified values in the conceptual investigation. This step can enable the technology's design or re-design to help support the values by prescribing alternatives or design improvements. [44]

Usability and human values work in tandem, depending on the ethical importance of the values and the functionality that the system should possess. In the literature of Friedman et al. four such relationships are observed. Firstly, design for *functionality and values*, in the application of browser management, privacy and informed consent was seen to promote privacy and consent with efficient cookie management system [44]. Secondly, *design of human values at the loss of functionality*. Two factor verification design supports privacy and security at the expense of being inconvenient for users. Third, *design for good functionality in order to support human values*. To conduct a fair election process, computerized polling machines require voters of all age demographic to use the system. Forth, *design for functionality at the loss of human values*. Bitcoin an efficient decentralized currency system is speculated to support illegal activities at the loss of trustworthiness [44]. The research examines the educational credential management's empirical and conceptual values using blockchain's technical architecture.

1.4 Research Problem

The multi-stakeholder and technological complexity make the stakeholders responsible for making innovations in the field of education conscious of technology, governance, and the legal ramifications of decentralized architecture on public environments. The technical uncertainty refers to the ambiguity and the reliability of the technology and institutional uncertainty concerns the regulations and legislations. The increasing positive attitude of companies to adopt blockchain technologies, as stated by an Respondent E working as a distributed ledger engineer at Sogeti, "Companies are always looking for technologies that disrupt existing business processes and blockchain provides a better alternative to assign control for

organization and users alike.” However, the decision-making structures in blockchain trickle down to the lowest vertical of organizations due to its distributed consensus mechanism and hence, experimentation with this technology with data exchange is of paramount importance before a market-wide implementation of the technology.

Funding on educational research has been decreasing when compared to the investments in technology in the field of healthcare, insurance, and banking [17]. Respondent D when asked about why the funding on technology in the field of education is lesser, answered that the inflow of private funding is considerably lesser and there isn't a *one size fits all solution in the field of ed-tech*. Respondent D also stated that more emphasis on experimentation with an iterative process is accepted rather than a wide-scale implementation that is generally observed with technologies in other sectors.

Advanced Education Technology Expenditure 2018-2025, USD Billions

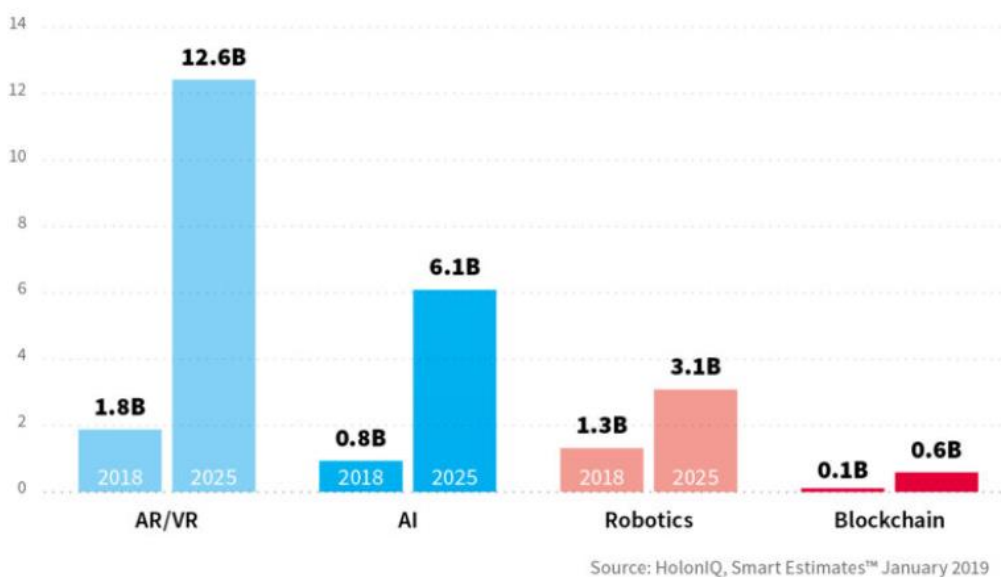


Figure 1 Use of technologies in education (Source: HoloniQ)

The objective of this research focuses on the ethical values of certification management and the effect of these values on the design of educational applications using blockchain technology. The methodology to structure these values and thus translate them into design principles was Value Sensitive Design. The deliverables of this research are overview of empirically identified values that influence the design of blockchain application in education. It provides insights on conflicting values leading to design trade-offs and demonstrates values embedded in design space. The outcome of this research is to contribute to design principles for the acceptance of this technology in the field of education both ethical and social.

1.5 Knowledge Gaps

First, the distributed nature of blockchain seems to challenge the traditional ways of registration and facilitation of information exchange by educational institutions, and this hypothesis hasn't been significantly tried and tested.

Second, insight into technological and multi-actor complexity is not made explicit in literature. The implementation of blockchain in the educational sector garners several complexities both technical and institutional. The conflicts with the principles of General Data Protection Regulation(GDPR)¹ and

¹ One approach towards regulating what happens to our personal data and the human right of privacy was taken by the European Union (EU) in order to harmonize data protection across Europe and strengthen its digital single market strategy [10]. The General

blockchain applications for education needs to be studied further to avoid unintended outcomes in blockchain experimentation in education [16].

The prevalence of an one dimensional view in research investigating design in blockchain use cases in education is present. There is a paradox that blockchain is a solution searching for a problem. However, there isn't a one size fits all solution because blockchain can differ in terms of openness of participation to openness in validation. To fully understand the impact of blockchain in educational processes, the design feature of blockchain and the values it should embody needs to be studied.

The scope of this thesis is restricted to the administrative aspect of educational institutions and using blockchain to notarize academic records, the need to request records from a central educational authority is replaced with blockchain by creating a new arrangement of trust.

There is a potential clash between the demands of the modern organization for more accountability and the independence culture of academics and teachers. The preparation of meaningful learning experiences requires changes in governance and re-think how to deliver the materials best using blockchain technology. With blockchain creating new paradigms, it is important to look at these topics to assess how they can benefit and not hinder each other to reach their full potential and intended purposes in the field of education.

1.6 Research Design

The research is qualitative and design oriented as it proposes to build design principles that would support the experimentation of blockchain technology in education. The goal is to develop design principles using existing knowledge and theories and exploring the environment in which such designs will be functioning. [17]

The design guidelines are generally applicable rules, standards, biases and design requirements that designers incorporate with discretion. Experts from many fields –e.g. behavioral psychology, sociology– have laid the framework for design concepts through their combined expertise and practice [83].

You apply it when selecting, designing and organizing elements and features in your work. The principles of design reflect the collective experience of scholars and design practitioners in related fields.

Quantitative research is generally used when the focus is on data where variables are correlated to form hypothesis that answers questions which are obvious and unambiguous for example to offer statistical validation to [54]. In contrast qualitative research is used to understand viewpoints and meaning from the position of the participants for example strengths and weaknesses of products/brands.

Since this research is exploratory and if focussed towards understanding the implications of blockchain technology in certification management, the study uses a qualitative research. One of the data collection methods of qualitative research is semi-structure interview.

Semi-structured allow the researcher to develop a keen understanding on the topic of interest. It includes open ended questions identified at new ways of understanding the topic at hand.

1.7 Stakeholder Scenario

Governmental Organizations that are important in promoting and implementing innovation in the field of education are key stakeholders in this research. The objectives of the research should be aligned with their

Data Protection Regulation (GDPR) that has been put into place in May 2016 and its enforcement will prevail after May 25th, 2018. The GDPR aims to significantly increase the value of personal data and shift the ownership of it back to the individual [10].

vision and goals. These are gathered through exploratory interviews conducted in a semi-structured set up. This helps in proposing policy recommendations and also sets the scope for further research. Also, companies who are keen on building such a system should be employed as another key stakeholder to validate design principles created through this research. The research strategy giving a brief explanation of the steps taken to reach the final goal.

The rationale behind using a qualitative or quantitative research depends on the form of data that is being analysed.

The actors identified for semi-structured interviews are Studielink, MIT Media Labs and TU Delft. Studielink links institutions of higher education in managing enrolments and diploma certificates across the Netherlands and an important organization to realize goals and objectives from a technological standpoint. MIT Media Lab plays a key role in developing services for blockchain in certification management and would influence the functionality of the system concerning the relevant technical architecture. TU Delft handles thousands of applications for its study programs, and a lot of time and effort is spent in scrutinizing applications for authenticity and an ideal match to validate the design principles created. This is explained in chapter 4 under feedback of university section.

1.8 Research Questions

Based on the identified knowledge gaps from the literature overview, the main research question is:-

What are design principles for blockchain for administrative educational purposes that help to meet relevant values?

To answer the main question, three sub questions are presented as an approach to structure this thesis.

1. What is the current known potential of blockchain?

Blockchain offers technical and institutional modernization in educational applications. It also encompasses ethical complexities which can make adoption of this technology difficult. Blockchain is still in its novelty phase with a technology readiness level² of 4 [1]; a case study describes blockchain in the field of education that can be adopted by 2034. Hence it is important to understand what the technology has to offer and the implications of the technology on a micro level in educational administration. Demarcating the technology also allows us to differentiate the values on a technical level.

2. What are the values needed to be incorporated into the design of blockchain application for educational administration?

In this research the pragmatic source to identify ethical values was taken from academic literature and stakeholder interviews. Literature on values on academic certification management is studied. Reviewing such literature gives an insight into values that improve reliability and decrease researcher's bias in understanding the used case. Value laden statements and concerns are analysed from stakeholder interviews and their interpretation of value to derive ethical values that can be associated with their viewpoints.

3. How can blockchain be used as an ethical or value sensitive application of certification management?

² Technology readiness levels [TRL] are measurement indexes to assess the maturity level of a particular technology.

The algorithms of blockchain are analysed in relation to the values identified. The resulting design principles are possible guidelines to be over for blockchain in certification management.

1.9 Thesis Structure

The thesis is divided into eight chapters. The first phase is completed after introducing the research topic, problem background, research objective and research question within this chapter. The second phase where theoretical background is given on the concerned technology and legislation involved (chapter 2). The third phase is analytical and provides explanation for research methodology (Chapter 3), descriptive results of stakeholder analysis and specific challenges and requirements of the application context is elaborated (Chapter 4). Conceptual investigation (Chapter 5) gives rise to main values of contention for this research and how these values effect or impact the technology also, how the values stemming from blockchain has an impact on the application context of this research is analysed and descriptive results are provided. The fourth phase is where the design principles are formulated (Chapter 6) and presenting dimension to the values at stake and how value definition and conceptualization are used to interpret the relevant results in technical architecture (Chapter 7). An overall conclusion (Chapter 8) is given in order to answer the research question and achieve the objective of this study, taking into account the scientific and practical contribution and also the limitations and recommendations for further research.

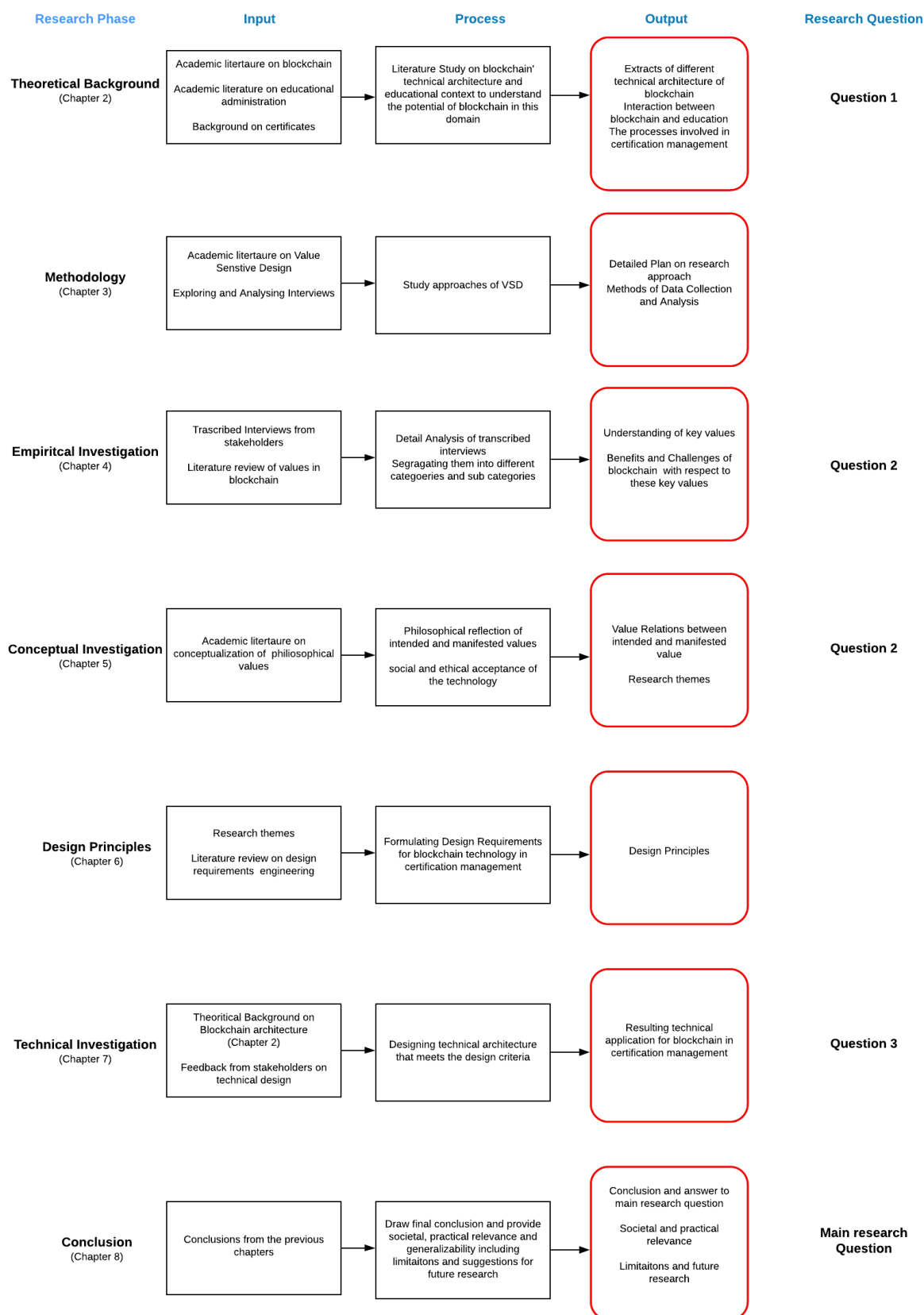


Figure 2 Research Strategy

Chapter 2- Theoretical Background

Blockchain has been hyped as a disruptive technology that can revolutionize business processes. Whether blockchain is set to revolutionize education is still to be seen. Blockchain offers versatility of features such as decentralized architecture, transparency devoid of an trusted intermediary, etc. The wide-ranging scale and promising scope that is offered by blockchain has uses in education [21] and certification management [79] and also other entries in educational administration such as copyright management [81], improving student career decisions [73], etc.

This chapter analyses the architecture of blockchain and its versatile features. It also explains the use context of this research which is certification management in education, the merits and demerits of blockchain in this application context is also explained.

This is done with the help of an extensive literature review which also lays the theoretical foundation for this research. The focus of this research is on the main terms that are related to blockchain (also called “distributed ledger” technology by some part of the ecosystem, coupled with the term “Education”, “certificates”, “credentials” to view the use case of blockchain technology). This chapter provides a theoretical background to the concepts that are discussed through the research.

2.1. Blockchain

The following part will firstly dive into the explanation of blockchain and its main concepts before it summarizes existing privacy solutions that are applied or conceptualized for existing blockchains.

2.1.1. Background and definition

To stay within the scope of this thesis this part will be limited to the main concepts and definitions. The first two sections will look at a brief background and detailed definition of a blockchain.

Background

The evolution of blockchain technology began in 2008 with a whitepaper – introduced in a private mailing list called cypherpunks – by an anonymous author or group of authors, who called themselves Satoshi Nakamoto: “*Bitcoin: A Peer-to-Peer Electronic Cash System*” [29], [30]. The first use case of blockchain was digital money, also called cryptocurrency (because of the cryptographic technology used for it) [31]. It was created to solve the problem, that individuals must trust centralized financial institutions to manage all digital payments and keep transactions, funds and privacy secure [28], [32]. Trust is the essential element here. The new concept introduced direct digital interactions without trust towards a central intermediary [31]. After other attempts before Bitcoin, it was the first to succeed finally [31].

The second main innovation in the blockchain field followed 6 years later in 2014, by proposing the concept of a decentralized worldwide super computer that can be used for more than just digital money transfers. Intelligent computer algorithms were introduced that can execute code autonomously – a concept called “Smart Contracts” – was presented by Vitalk Buterin and the founders of Ethereum [31], [33], [34]. Along the roads of these two major innovations, it was understood that the underlying technology “blockchain” and thought-concept following it, could be used for decentralizing and decoupling intermediaries in any industry or sector [35].

Definition

Blockchain technology is still under very active development, as for why a formal definition of the terminology has not been established yet. Another challenge presented is the different perspectives blockchain can be viewed from.

The datalogical layer uses a technical view that describes blockchain as a data structure in a technical sense. The infological layer helps to abstract the data structure level by adding information that makes it more accessible for a nontechnical point of view [36]. The term “distributed ledger technology” (DLT) is an example of this layer and adds a new, arguably financially motivated, aspect to it by abstracting the linked list of transactions to a “ledger” [27]. The term DLT is often used interchangeably with blockchain. The essential layer is what is created directly or indirectly by communication, meaning it can present the business, legal or process improving an aspect of a blockchain. In the resulting definition of blockchain, one can implicitly find the aforementioned ontological approach again.

The image below presents a visual representation of blockchain.

Note 1 to entry: A blockchain has a tree shaped structure where each element in the tree is a block that starts with the genesis block at the root, with each block potentially having multiple child blocks. Each child block, besides the genesis block, contains a hash-value of its parent block.

Note 2 to entry: Since adding a child block to the tree involves calculating a new hash over its parent, no block in a tree path can be changed without invalidating the hash of the child block.

Note 3 to entry: Practically immutable means that within the confines of current technology and known attack vectors records are immutable.

Note 4 to entry: Usual blockchain applications connect child and parent blocks to lists, which is only a specific form of the more general tree.

The next section will explore how the blockchain works in more detail, adding more context to the definition.

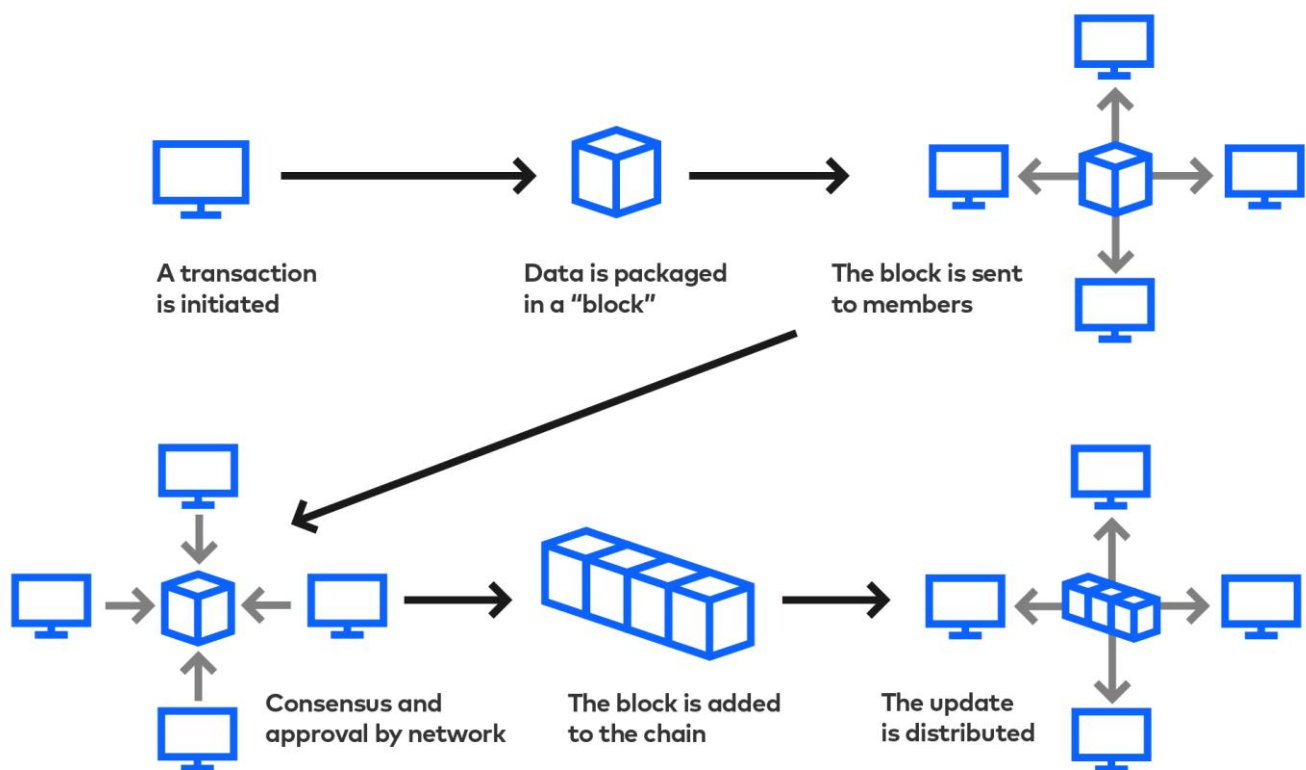


Figure 3 Working structure of blockchain (Adapted from [60])

2.1.1. How blockchains work

This section will take a systematic approach to describing how a blockchain works in more detail. To sum up the previous definition, a blockchain is an innovation that itself relies on three concepts: **peer-to-peer networks**, **cryptography**, and distributed **consensus** using the resolution of a randomized mathematical riddle. None of these concepts is by itself new but in combination allowed for the computing breakthrough of the blockchain.

2.1.1.1. Exchange of digital values

Decentralized **peer-to-peer (P2P) networks** have existed with Freenet or BitTorrent [37]. The blockchain now enables an exchange of values (often referred to as a token), instead of media [31], [38], [39]. These P2P networks are distributed systems that must solve a difficult computer science problem: the resolution of conflicts, or reconciliation [40]. Traditional databases, like relational or object-oriented databases, offer referential integrity, but in a distributed system this does not exist [40]. To arrive at a consistent value, the system needs to have rules in place to determine which value is considered valid. One of the toughest problems to solve is the double spending problem, in which one instance sends the same value to the network twice, but only the one arriving first will be accepted as such [32]. The other one will be made invalid. To guarantee integrity within a P2P network, every participant needs, to, therefore agree on the order those values arrive [29]. For that, a consensus mechanism is required. Consensus algorithms for distributed systems have been actively researched for decades (e.g. Paxos and Raft algorithms). The blockchain uses different **consensus algorithms**. Currently, the most used algorithm is called proof-of-work consensus, using mined blocks based on electricity power [29].

2.1.1.2. Hashes and blocks

A blockchain functions by storing its transaction data (e.g., transfer of value) in digital containers called blocks [29]. Each block is linked to its parent block through unique digital fingerprints termed hashes [29]. A hash is a simply a **cryptographic** function that maps data of any arbitrary size to a fixed size, called hash value (or hash) [29].

There is currently no known way to reverse engineer the original input from the cryptographic hash (hashes can be broken, but it is assumed that they are developed along the same time line as the algorithms able to break them) [33], [38]. Blocks uses timestamped hashes in a header at the top of each block of information [41].

This history of transactions stored in the blocks is linked back to the initial or genesis block (for a Bitcoin specific consensus algorithm called proof of work an additional string called nonce is used together with a hash function) [29]. The information stored in blocks is to its current measures highly tamper resistant (practically immutable) even by those who store and process the information. This is made possible by independent validation nodes that come to a decentralized consensus for every transaction that has occurred [29], [42]. Consensus algorithms ensure that the participants of the P2P network agree on one truth [29], [42].

2.1.1.3. Public, private, permissioned and permission less

Just like a database, a blockchain can be private or public and permissioned or permission less [39].

A public blockchain (e.g. Bitcoin or Ethereum) is characterized by being open to any entities that want to join the P2P network, on the other hand, a private blockchain only allows pre-selected participants in the P2P network [39].

The other differentiate the entities that are authorized to conduct the consensus process. In a permissioned blockchain, these entities are pre-selected, whereas in the permission less blockchain anyone is allowed to participate in that process (e.g. Bitcoin miners) [39].

To list a few examples, a group of the largest banks around the world is working on a private, permissioned blockchain that enables global payments for its internal use, called Ripple [40]. Another blockchain network called Interplanetary Database (IPDB) offers a permissioned public blockchain with the aim of allowing anyone to store data immutably, but by pre-selecting the consensus processing nodes to provide fair governance.

Governance is one of the big pain points of existing blockchain solutions, as it becomes difficult to make a bad actor accountable for his behaviour in a fully decentralized system. This directly relates to the issue of privacy. Since the invention of blockchain in 2008 many approaches and potential solutions have been thought of to solve the issue of privacy, the next section will explore which ones

2.2. Educational Administration:

Certification is described as the process of providing an official document attesting to a level of achievement. In education, certification is classified under attainment of learning outcomes, an educational institution or a lesson having a standard criterion and an accreditation body being sanctioned to provide certificates [53] .

The pitfalls in the current system is that it limits new pathways of learning in particular to those who do not have access to it. Another challenge is that not all learning happens at the university level, for example, a person is able to acquire certain skills through online courses and other forms of learning, the existing credential system make it highly difficult to translate the learning into jobs because of the lack of credentials affirming the skill and experience.

Below the process involved in digital certification is explained.

2.2.1 Process Involved in Certification

Certification mainly involves three processes [3]:

Issuing: this is the method of logging the claim, applicant, proof, receiver and signature onto a certificate. This information is documented: in a centralized claims database; on a document received by the user.

Verification: this is the method by which an intermediary validates the legitimacy of the document. Three methods of doing this is listed below:

Authentication using privacy features that are built in the document: this could include procedures like verifying the legitimacy of a stamp, specific security document, sign etc.;

Another form of authentication of the document is by checking with the initial issuer, whereby the initial issuer is contacted by the intermediary, confirming whether they issued the document. (Here the initial issuer might refer to their centralized archive or verify the privacy features that are present on the certificates).

The third form of verification is in comparison to the centralized archive. The list of the documents issued in an intermediary archive would permit parties to check this archive and copies of all documents issued between them, is compared. Diploma register maintained by the third party (DUO) is an example of this type of verification.

Sharing: this is the procedure by which the owner of the document shares it with an intermediary. This can be achieved by three ways:

- a) documents can be sent to the intermediary directly through emails or by presenting the document to the intermediary in person.
- b) the document can be stored by a guardian who's is legitimised to share it with people entrusted by the you (e.g. private will is stored by a notary who discloses its contents to the recipients of the will, after the death of the person);
- c) distributing the document, by placing it on a public archive, and permitting people to refer to it.

2.2.2 Limitations of (non-Blockchain) Digital Certificates

Digital certificates have several benefits over paper certificates: they would require lesser resources to be issued, managed and used, since [3]:

- The validity of certificates can be verified against the archive automatically, without human interference.
- If an intermediary wants to use a certificate, it can be automatically compiled, checked and even recorded if it is given in a structured format.
- The security of the document stems from the reliability of the cryptography algorithms, which guarantee that the certificate is cheap to manufacture but exceedingly costly to duplicate, by all but the issuer.

- The issuer can revoke certificates

However, digital documents still have major drawbacks, namely [3]:

- They are incredibly easy to counterfeit without the use of digital signatures.
- Where digital signs are used, they require the intervention of intermediary authentication suppliers to ensure the legitimacy of the contract –these intermediaries have tremendous influence over any element of the validation and verification process that may be violated.
- In certain countries, there is no widely accepted guideline for digital signatures, leading to documents that can be checked only in the framework of particular application environments.
- deleting electronic records is easier however maintaining the security requires complex, multi-tier storage mechanisms that are vulnerable to failure.
- If the database fails, the documents themselves become useless and, unlike the paper certificates, they do not have any inherent value without the database.
- digital certificate databases are vulnerable to massive data breaches.

2.2.3 Digital Certificates using Blockchain Technology

Blockchain technology is suitable as a digital platform for protecting, exchanging and checking academic credentials. In the case of certifications, a blockchain can hold a list of issuers and recipients of each document along with its sign (hash) in a shared ledger (blockchain) that is kept in hundreds of devices spread across. Digital credentials, which are thereby encrypted with the blockchain, have major benefits over 'standard' digital documents, in that regard [3] :

- They can never be manipulated – it is feasible to prove with confidence that the documents was initially given and obtained by the same individuals identified in the document.
- certificate authentication can be carried out by anybody who has access to the blockchain, using freely accessible open source tools – no third party is needed.
- since no third entity is required to verify the document, the document can be certified even though the agency that authorized the certificate no longer exists or has no access to the released record.
- the archive of documents given and obtained on the blockchain can only be lost if every copy on every device in the world running the database is deleted.
- the hash is merely a means of generating a 'connection' to the original certificate owned by the recipient. This ensures that the aforementioned procedure requires the publication of a document to be signed without the need to publish the document itself, thus safeguarding the privacy of the records.

Conclusion:

This chapter provides the basis of the potential of blockchain in education. The versatile features of blockchain is explained here. The literature review goods a good basis of understanding of blockchain which will be useful in analysing and dissecting the technology in the later investigations. What can be observed here is that blockchain has a multi technology infrastructure that can accommodate different domains of education. The potential of blockchain in education is one of the important findings of the research and is elaborated upon in the conclusion chapter (Chapter 8).

Chapter 3- Value Sensitive Design (VSD) – Methodology

Value Sensitive Design is a tripartite methodology that aims to diminish possible harmful effects of technologies [70]. Value sensitive design combines stakeholder's acceptable values and the values identified in the technology. VSD incorporates three phases of investigation- empirical, conceptual and technical. A short description of these three forms of investigation with a comparison trade-off of functionality and human values is given in chapter 1. The rationale to use VSD is that it makes the stakeholder values clear and thus enables better embeddedness of these values in technology design.

This chapter discusses the methods used to conduct the above-mentioned investigations.

Empirical investigation:

This study uses semi-structured interview approach as the main tool to comprehend the stakeholder values that influence the technology. A diverse set of respondents were chosen to encourage distinct set of ideas and opinions. The profile of the respondents ranges from enterprise architect, blockchain application specialist and recruiters.

The conditions used for selecting the participants were: -

- Awareness of technology, benefits and challenges of values associated with it
- Knowledge of the application context (educational certification management)
- Sufficient experience working in the field with an understanding of different domains of the technology

To prevent preconceptions in the respondent's answer and to enhance the clarity of the interview process, methods from Sekaran et al. [71] and Adams [72] were used.

Interview Guide – open-ended question to the stakeholders are asked to give an idea of the situation, this technique makes the interview process engaging and versatile.

Unbiased Questioning – Making sure that impartial questions are asked to eliminate the bias in the answers.

Clarity on Issues – It is prudent to refocus or rephrase the information given by the stakeholder to ensure that the information presented by the stakeholder is well realized and is consistent with the study.

Helping stakeholders to reason over the issues – Answering the concerns in a clear manner and presenting specific context to help the stakeholder comprehend the problem and the concern posed.

Recording the interview and taking notes – It is known that the memory recollected information is imprecise and sometimes inaccurate which may contribute to further bias in the study. Keynotes were then made and interviews were conducted after the consent of the respondents was received.

Value Set – A set of values were present to the respondent in the form of a sheet. The explanation for these values were chosen from scientific literatures and articles in the field of blockchain and education. Particularly, the literature of Alammary et al. [73] and Chen et al. [75] where a study on the culmination of blockchain in education was done. Inputs on the values relevant to the architecture of blockchain and values relevant to education (certification management) was taken and presented in the form of value set to the respondents (Figure 3). The findings of the empirical study is presented in Chapter 4.

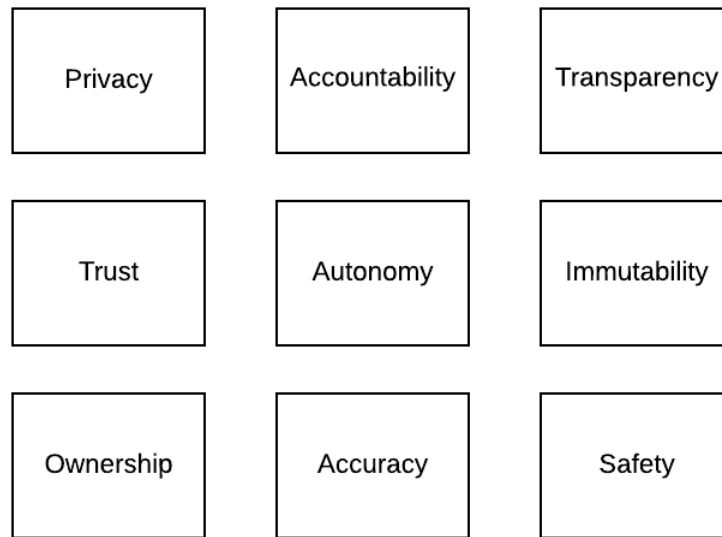


Figure 4 Value Set for Respondents

The interview was conducted in two phases. The first phase was done with the respondents slated in the table below to get a brief idea on what values are important while designing a blockchain application for education. For the second phase of interview an interview guide(questionnaire) was used based on Sekaran et al. [71]. The questionnaire for the second round is listed in the appendix section. The technique of *purposive sampling* was used. A purposive sampling is a technique where the researcher uses their reasoning to interview the right participants for use case [71]. The method is used to derive questions suited to the respective respondent's interest with the purpose of extracting the maximum detail. The second round was conducted to further push the barriers of blockchain in a educational context. This was done with the same respondents but with the focus on the technical domain to understand the specific parts of technology in relation to the educational context. The following stakeholders were interviewed for this research. The table categorizes their organization and their field of expertise, pseudo names have been used for anonymity.

Table 1 Repspondents Interviewed

| Expert | Organization | Field of Expertise |
|--------------|-------------------|---|
| Respondent A | DUO | Enterprise architect and design |
| Respondent B | TU Delft | Document Management and Archive |
| Respondent C | Blockchain Lab | Blockchain applications |
| Respondent D | Studielink | Enterprise architect |
| Respondent E | Sogeti | DLT policy and complexity |
| Respondent F | Hogeschool Leiden | Recruiter/ Domain architect |
| Respondent G | MIT Media Lab | Learning Innovation and blockchain technologies |
| Respondent H | TU Delft | ICT application and e-tech |

Analysis:

Both phases of interview were transcribed from audio recordings to text. The transcribed interviews were manually checked to draw out inferences with a *narrative analysis*. A narrative analysis involves making sense of the respondents' individual viewpoint and highlighting aspects of the narration that resonates best with the research. In the empirical study a few quotes from the respondents have been used to highlight crucial points and connecting it to other areas of research to give depth to the analysis [87].

Thematic Content analysis was performed to weed out the biases and establish an overarching impression on the data. Rather than approaching the data with a predetermined framework, common themes are identified across the data set.

Method of Analysis:

Initially a list of values sheet (Figure 3) was presented to the respondents along with the context of research and few opened ended questions and help in answering the research questions of this research to give more knowledge and background on the research. Three most important values that achieved the highest value count were selected, this was done to limit the scope of the thesis due to time constraints. The research points out that other values can impact the design phase and should not be neglected when designing such an application in the future [84].

It was then followed by *annotation* of the transcripts. Annotation is a process of labelling words, phrases, or sections of data into patterns or common themes. Labels can be about actions, opinions processes or concepts. Annotation of data helps organize it better for dissemination [87].

Based on the patterns that were identified, the data was divided into categories or sub-categories. This is done to establish link between data sets in a cohesive way. This was done with a help of a spreadsheet. The categories of data were first divided upon important stakeholders and the views they express was matched to the respective category. Based on the literature research on the technical implementation of the values that is present in (table 2) these categories were then matched to the subcategories of values. A reflection of this can be seen in the empirical investigation (Chapter 4).

Finally, the categories of data which inform the research on the stakeholder concerns is segmented based on the benefits the technology adds and the challenges it incurs and is presented in (table 3).

Conceptual Investigation:

Based on the findings of empirical study the values unpacked are studied on a closer detail with the architecture of blockchain that corresponds to the respective values. A literature study [76] is used to do the above. Research websites like Scopus, Google Scholar, Research Gate and Science Direct were the major source for retrieving intellectual papers on blockchain and concepts of values sensitive design. Since blockchain is a relatively new technology, there were challenges in finding insightful research papers. Backtracking and scanning references of certain papers was done to find other interesting papers. There has also been useful research by organizations on the impact of blockchain technologies in various domains. These researches were particularly useful to understand the different concepts that blockchain entails and to link these concepts to the philosophical definitions of the values. Figure 4 explains the orderly process of the research that was carried out and A search strategy, a tag-based approach for the word's "*privacy*", "*transparency*", "*trust*", "*blockchain*", "*education*" was searched across different education repositories such as Google Scholar and Scopus.

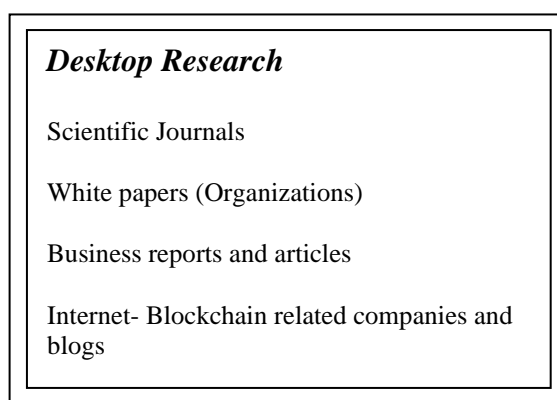


Figure 5 Data Collection for Conceptual Investigation

The goal of this investigation was to link the conceptual understanding of ethical values with the technical architecture of blockchain, its constructive and perverse features with respect to certification management. The findings of this is presented in Conceptual Investigation (Chapter 5).

Design Principles:

Designing in essential is a human endeavour, a social activity. It is important to understand that designers need to bear in mind that the products of design influence a society. More so in this case when designing a certificate management for education, an institution which is very fundamental to society, it is essential to accept responsibility while creating designs. The very rationale to look at Value Sensitive Design as a methodology to conduct this research is this.

Every design problem has two main components, the client or stakeholder who wants the product or design to be built and the user who uses the product. The need of the design must be to achieve objectives while satisfying the conditions of constraints.

Dym, Little and Orwin have a formal definition of generating design principles, “*engineering design is a thoughtful process for generating plans or schemes for devices, systems, or processes that attain given objectives while adhering to specified constraints.*” [83, pp.7].

During the design phase two facets of designing principles are to be kept in mind. Designing is *ill structured* as their statements are means to convey what the design should have/do. It shouldn't be something that can be reciprocated in a mathematical formula, it should rather address the subjective needs of the stakeholders.

Designing is *open-ended* meaning there is no unique solution but various acceptable solutions to it. Moving on to engineering terms, design principles are consideration that forms the basis of a good product, system, or process. Design principles should help stakeholders in decision making.

Technical Investigation:

The strengths and weakness of blockchain to address the relevant values of privacy, transparency and trust through its architectural changes. The strengths and limitations of blockchain with respect to its potency to imbibe or impede these values are presented in the Technical Investigation (Chapter 7). An approach of literature study [76] to map the applicable characteristics of blockchain to the findings of the conceptual investigation. This is done to unearth new design specifications that could promote blockchain as the tool for certification management in the future. The interviews were also used as a feedback mechanism to assess the technical architecture of the design based on which recommendations of further research.

Chapter 4- Empirical Investigation

In this chapter the focus was on understanding *key stakeholder values* and recognizing *benefits and challenges* for each stakeholder group. To comprehend stakeholder viewpoints semi structured interviews were conducted. Semi structured interviews offer a way to understand stakeholder's viewpoint and values. It makes it possible to dig deeper into stakeholder sentiments and their opinions with open ended questions. Stakeholders were selected from on the basis of their understanding of the technology and play a major role in education sphere such as education application developer, researcher, or recruiter. 8 respondents were contacted for the data collection and questions during the process.

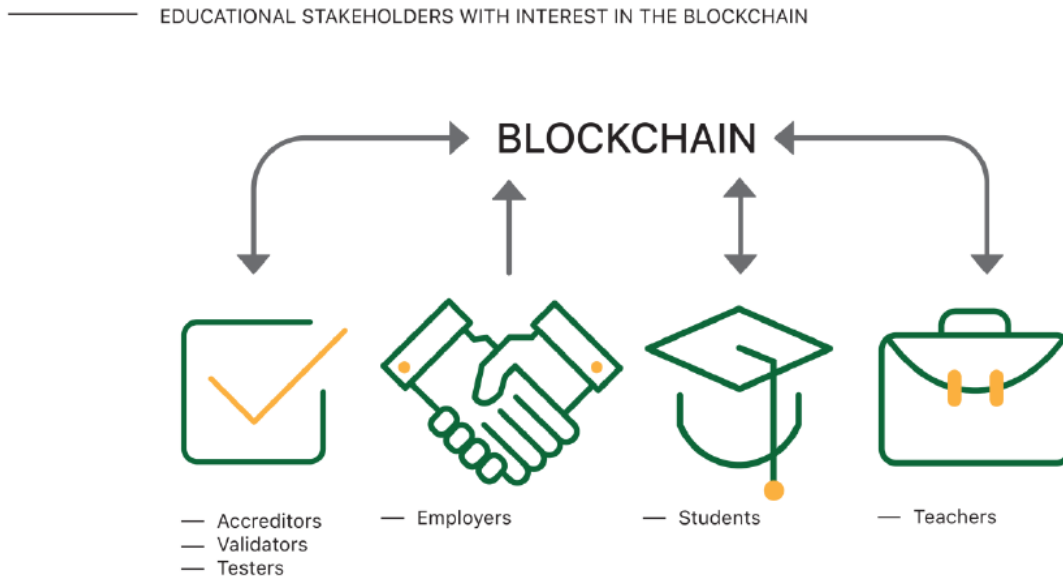


Figure 6 Stakeholders Adapted from [60]

4.1 Stakeholder Analysis

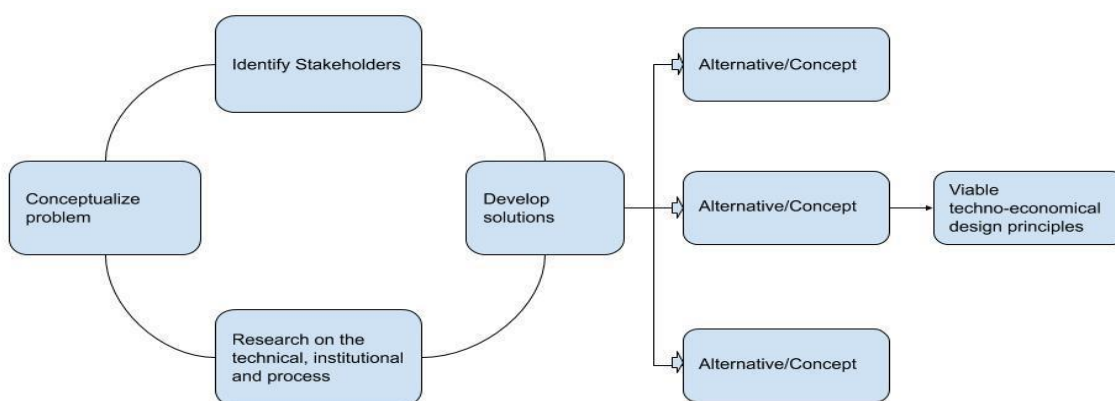


Figure 7 Stakeholder Analysis

The stakeholder analysis is structured based on above mentioned model. The goal of the research is to obtain viable design principles for the development of blockchain applications in educational credential management. In order to realise design principles, the first step was to conceptualise the problem (Chapter 1). The next was to evaluate the technical, institutional and process managerial benefits and challenges credential management in blockchain.

4.2 Data Analysis of Values

As mentioned in the methodology section a value sheet with a list of values was presented to the respondents at the time of interview. Three values that had the highest count were selected for analysis. The three intended design values are presented in the table below with their respective design features and the implementation in the context of blockchain. The design sheet was also presented to the stakeholders to explain the relevance of blockchain in the value context. Other important values like accountability, autonomy would also impact the design process and are values of significance for the design of this system, however due to time constraints the above-mentioned values are not studied in detail.

Table 2 Values in blockchain

| Value | Design Feature | Implementation |
|--------------|--------------------------|--|
| Transparency | Decentralization | Blockchain possess a publicly available and open transaction log. A user/system can confirm the transactions made. |
| | Immutability | Blockchain is immutable in nature and hence tamper-proof. |
| Privacy | Pseudo- anonymity | Parties have limited access to information about other parties involved. |
| | Public- Private key pair | Blockchain pairs public and private keys to securely verify identity of a transaction |
| Trust | Cryptographic proof | Validations are made in the form of cryptographic proof secured by an algorithm |
| | Protocol Identity | Blockchain ensures that all nodes in the network trade under the exact same conditions without the need of a central authority |
| | Time- stamp server | The system confirms each block which inhibits the user from manipulating the transactions. |

Feedback from interviews are summarized on the table. The respondents also assumed different roles such as an end user, academic and recruiter. This was done mainly to understand different viewpoints other than their technical backgrounds. This was also used as a medium for ideation as it helped in scoping the extent of the research. The table also includes technical characteristics that will be explained in detail in the technical investigation chapter(chapter 7)

Feedback from University perspective

Here the challenges of credential management from the viewpoint is observed and argued.

Respondent F highlighted that universities encounter problems where students falsify information and in some cases even pay a bribe for an illegitimate seal of authenticity from central authorities and there are not direct organization of registrar that can verify these identities. This poses two issues, one the transparency of the process on the trust of the entire system.

Respondent B points out that the new system should include methods of decision making and must be transparent and universally accepted by all stakeholders of the system.

There is a lack of communication between stakeholders “In Netherlands there is an organization called Emrex that act as a contact point between universities and client. They bridge the authentication gap between university and a client which could be a company or the student. However, such a solution is not possible internationally now and that is where blockchain could fit the gap”. The goal of the system is also a means to promote communication between universities through algorithms that help them verify credentials in a seamless way. Respondent E also highlighted on the above-mentioned statement, “the value of trust between universities or a lack off is a pending issue that needs a work around”. At this moment universities and recruiters rely on third party vendors to verify credentials. This is an expensive process and also time consuming. Blockchain as a technology offers technical principles and can act as a trust medium between universities. This is explained further in the technical investigation (chapter 7)

Respondent D , Respondent G and Respondent E univocally mentioned that single point of failure is a major problem when it comes to centralized databases meaning, if the registry that holds all the diploma's fail then the certificates themselves hold no inherent value. This can specifically be observed in the Syrian refugee crisis that has been mentioned before, people were forced to migrate to different countries and took sub-par jobs as they were not able to prove their qualifications.

Respondent A from DUO an organization that implements educational laws and reforms in education in the Netherlands mentioned that there is little consensus on which services should be used on the blockchain and which services should not. Therefor the challenge becomes to fit blockchain in the areas that would benefit from such a service and not as an overall encompassing technology that would fit all application and services.

All the respondents agreed on the fact that digital registries are susceptible to big scale data leaks. Hence privacy of information is compromised and in many cases, there have been attacks and leaks of sensitive student data [62].

Feedback from system engineers and designers:

Respondent H argues that current blockchain initiative has an over complicated application layer. With the recent regulation of GDPR in place, data cannot be directly stored on blockchain as they are immutable. Hence there is a reliance on centralized data controllers to store data. Respondent B who works closely with blockchain applications adds that “Blockchain will always levy other technologies to store data and process data, as blockchain becomes computationally intensive as the data on the chain increases. The rationale for using the technology that stores and communicates in a transparent manner should be chosen”

Respondent G believes that “Binding network rules or the rules of engagement between stakeholders from an algorithm's standpoint needs to ensure that system is trusted by all parties, this would be one of the main concerns for stakeholders to opt in or out of this system”

Feedback from end users:

Respondent F a recruiter says that “Companies find it difficult to validate credentials done through online platforms. The dynamic growth of these online platforms are a resultant that knowledge transfer can happen anywhere. Current systems do not allow transparency of qualifications resulting from these online mediums. In the future, student can choose not to get on board with the a current three to four years of standard

university education for a number of factors ranging from opportunity costs and having a variety of skill certification at different fields of study". Added to this blockchain can also help reducing costs of the hiring process, through an efficient credential management system where the trust between parties and trust between users and parties are established through a consensus mechanism.

Respondent F emphasises on the perception of end users to blockchain. The system needs to be secure and adequate protection must be enforced to prevent data leaks, this point is also reflected on the feedback from the university perspective meaning all respondents share a common consensus on the security of the system.

Respondent F shares that from a third party using the system, mechanisms for verifying user's identity and the education provider's identity is a vital cog. The respondent believes that this would generate a positive externality for the third parties (recruiters) to use the system.

Stakeholder Perceptions of Values:

The value of transparency with respect to the how the universities convene and take decisions is vital for the application on certification management. Decision making factors on techniques for identity verification so that the students and education providers cannot falsify information. The current system lacks ease of sharing and visibility. Stakeholders believe that one of the important features the blockchain offers is information on the origin of each record and its ownership. Another entity that the system needs to adhere to is access, the system must be easily accessible to the user and education providers. Grounded rules on conditions of access between third parties (recruiters), education providers and users must be present.

The value of trust is important. The application needs to execute the mechanisms for assurance meaning that each of the parties' act in good faith and relevant standards are in place with the requirements of the system. It is necessary to show the methodology on how trust is reciprocated in the system, how the certificates are released and how is trust shared between unknown parties in the system. Hence the application needs to possess a value network that needs to operate without the intervention of a defined central authority.

The value of privacy, the system to be designed has relevant security features that prevents data leaks, promote ownership of assets and back up data sources in the mishap of system due to technical or human errors. The system should also adhere to the privacy laws and regulations. Ownership of assets is a value proposition that blockchain offers which the current certificate management systems lack.

Conclusion:

Stemming from stakeholder viewpoints the benefits and challenges of using blockchain are given in the table below. This is done to understand blockchain's intended value and the stakeholders' envisioned values. It is essential to categorize these to further understand the value needs that needs to be satisfied by the system design. The numbers on the table indicate the number of respondents that stated the benefit and challenges.

According to stakeholders, blockchain preserves privacy as it entails anonymity of transactions meaning the transactions cannot be traced back to the user, in giving control back to the users they can share parts of their credentials to the recruiters. This is done by creating multiple identities and each identity can be mapped to a list of credentials the user wants to store. For example, if a user wants to store credentials relating to arts he/she can create an identity A and map these credentials related to that, similarly identity B can be created to store engineering credentials. Another feature that blockchain offers is ownership of assets however in case of a loss of public key, a centralized ledger needs to be used to store and verify public keys, the same issue of a single point failure presents itself.

Blockchain allows transparency of information sharing however the challenge for interoperability remains to be questioned. As seen in Chapter 2 documents in blockchain are difficult to forge, blockchain allows access to all education providers through its open source algorithms which are essentially called as public blockchains, a distributed ledgers stores all the activities of the blockchain locally and hence promotes

visibility of information sharing, the algorithm present verifies and validates new nodes in the system and hence the lack of communication regarding the authenticity of the process that the stakeholders prescribed in the current process can be solved.

The trust in the network is enhanced by using algorithms as a proof of verification but scalability issues arise as block size increases and hence higher computation power would be required, this would in turn increase the costs. The robustness of the system under data mismanagement and data leaks is one of the challenges the system has. The rules of engagement between the stakeholders is another challenge that restricts trust in the system.

Table 3 Benefits and challenges of values of blockchain in certification management

| Values | Definition | Benefits | Challenges |
|---------------------|--|---|---|
| Privacy | “An individual’s claim, entitlement, or right to determine what personal information is communicated to others” [44, pp.124] | Anonymity of transactions (2), selective information sharing (8), ownership of asset (6) | Right to be forgotten, untraceable transactions, loss of private keys, public key infrastructure has single point of failure. |
| Transparency | disclosure of information | Difficult to forge (4), open source algorithms (3), visibility of information sharing (5), enables communication between stakeholders (6) | regulatory frameworks for interoperability |
| Trust | “The predictability of the system’s performance: security, reliability, safety, and survivability” [44, pp. 152] | Distributed ledger (8), protocol identity(7), eliminates the threat of data leaks (2) | High storage costs, Binding network rules, robustness of the system |

Now that the empirical investigation has been discussed and different values that vital to the system has been unearthed the next chapter focuses on the conceptual understanding of these values and the value tensions and might arise as the resultant of this.

Chapter 5- Conceptual Investigation

5.1 Conceptualization of Values

The conceptual investigation gives insights on the value taken into account and the relevance of the value with the technology. In this chapter three of the most important values stemming from the stakeholder analysis are analysed.

Values by themselves need additional values to support existing values. That is privacy leads to autonomy, trust leads to transparency. Therefore, it is important to study the values at hand. In this research we focus on three values, transparency, trust and privacy. The conclusion to scope in on these values alone is mainly due to the importance of these values that have been put forth in the empirical research from interviews, literature review and also due to lack of time to analyse other important values that may affect the design of technology to be analysed.

5.1.1 Transparency

Transparency has several meanings ranging over a wide range of contexts such as science, engineering, humanities and other social contexts. Disciplinary foundation and ideological nature are probably going to influence the poise of transparency with the other values. Thus, the beneficial nature of transparency is contingent upon the control and heterogeneity of transparency that occur on the environment with which they are associated.

Transparency in philosophy is linked to individual's cognitive state depending on the context. For example, pain can be attributed to being strong transparent as when someone is in pain, he reacts immediately to it [46]. Transparency in business ethics is likened with information disclosure, it is defined as "degree of completeness of information, provided by each company to the market, concerning its business activities". Transparency in software engineering can be defined in relationship with understandability and relevance. According to Sharples et al. [16] businesses fell blockchain lacks clarity in defining relevant boundary conditions, the possibility that organizations would want to adopt business processes that would suit blockchain however the understanding of which business process would need blockchain remains to be answered. Educational institutions find it difficult to decipher which service should be a part of the blockchain and which do not. A possible solution which is later discussed in technical investigation (chapter 6) would be to allow blockchain to handle a certain business process coupled with an interface design that would handle other applications through the means of an application interface, the viability of this solution will be analysed in greater detail.

Across different literatures it is commonly seen as the ability to retrieve the desired information successfully, the information acquired can be comprehended with prior knowledge, the information obtained by stakeholders answers their question [46]. Data unavailability or intractability of data could be one of issues that arise from this standpoint. Giving control to users to handle their own data comes with a risk of loss of data. If the user loses his/her data due to mismanagement, then the onus of who is responsible for retrieving the data arises. Should the responsibility be in the hands of universities, users, or the developer of the blockchain application. Hence a trade-off between privacy and transparency could occur in this case.

For the scope of this thesis transparency would be addressed with the definition pertaining to information disclosure. The implications for disclosing information is a significant challenge. Implications could stem from legal regulations, business motives or from an ethical standpoint.

Transparency is always important, but especially in situations where individuals have a choice about whether they wish to enter into a relationship with a business. If individuals know at the outset what you will the business uses their information for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship. This can be supplemented with an example; financial companies see fit to use customer's funds and loan bundle it into prime and subprime categories in not the most effective and honest manner and resell it to stakeholders. In

the entire process the customers were not acquainted on the strategies and background information. The financial crisis of 2008 being the epitome of this very issue [46].

However disclosed information does not necessarily imply ethical consequences like the above example. Information can be ethically neutral [47]. Regular software updates that is prompted by the operating system disclosing information of underlying process does not qualify as an ethical choice but more of a design choice. Americans on an average need 201 hours to read their privacy policies and majority of them accept the conditions without reading them [22]. In the case above the principle of outcome is information, however in blockchain the principle of outcome is a real value and hence such policies when they are formed have to be concise and readable for an average user to understand and make a decision.

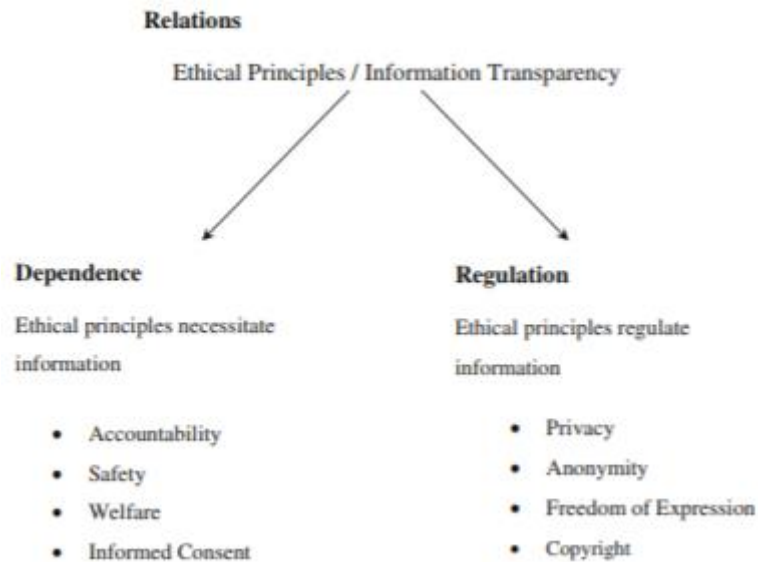


Figure 8 Relation of transparency (Source: [47])

The figure above categorises transparency in relationship with ethical principles that can either enable or impair informational transparency. Dependence has to do with some amount of information required to validate the ethical principles and regulation is the constraint on the amount of necessary information in its usage, storage and access. The recall of 2.5 million Samsung Note 7s globally after reports of overheating and in some cases property damage [50] shows the importance of welfare and safety enablement may depend on the disclosure of information.

Facilitation access to medical record to scientific research may result in life saving studies however the private information of patients may also be misused and thus expose the patient's history. So here privacy impairs informational disclosure. Hence information disclosed must be carefully studied on a case by case basis to understand its ethical consequences.

Legal systems categorise transparency as a principle of freedom or access to information. Hence one of the values that manifest from transparency is the value of access. Access can be defined as open and equal opportunities to use the system. In the legal front blockchain offers legacy problems [4]. The general data protection regulations that prescribe new storage laws giving users the right to have their data deleted at their will has a philosophical problem with the immutable architecture of blockchain. Educational institutions would find it challenging to accommodate the right to be forgotten aspect of blockchain or even correct wrong student data once it is appended to the blockchain.

Educational organizations promote access by providing licenses to operate in the form of accreditation. Organizations such as ISO, European Quality Assurance Register (EQAR) are a few accreditation agencies. These accreditation agencies recognize educational programmes that allow specific The issue in this as the stakeholders pointed out are that these accreditation do not appeal to internationally and do not account for various educational organization that provide mediums of education. Blockchain in its core

value is a desire to democratize entry barriers by enabling equal access across through peer to peer transactions. Blockchain allows users with information on the source of each transaction and how its ownership has changed over time. The questions on how to engage stakeholders through algorithmic proofs that enable communication through a transparent consensus mechanism is studied in the technical investigation.

5.1.2 Privacy

A single definition of privacy is equivocal. One of the early perceptions of privacy was viewed as principle that endorses a concept of non-interference or a boundary that separates public and private spheres from unnecessary human interventions. However, over the years the definition has grown more convoluted with technological leap and social interactions promoted through these technological advances. “An invasion is an attack in which information, whether intended to be public or not, is captured in a way that insults the personal dignity and right to private space of the person whose data is taken” meaning privacy is needed to keep one from harm [48]. Going back to the example of medical history as it contains various facets that holds complexities across different levels. Let us consider a leaked medical record of a data subject. It could further warrant an insurance company declining to provide service to this data subject because of his existing ailment which in another case would have been granted. Another argument is to correlate privacy with the value of security. Cultures and species need security of some class. In a computerised culture where gaining information is through a touch of a button, privacy develops as the declaration of a basic necessity, security. Blockchain’s nature of a peer to peer topology has reduced the privacy risks in education field. Using cryptographic techniques, blockchain was to validate learning traces and verify the reliability of transactions, where each block was data related to a learning activity [21]. Thus, innate nature of blockchain facilitates users to verify and secure their academic credentials using blockchain’s cryptographic hash signatures [2].

The value that manifests from privacy is self-sovereignty. Self-sovereignty is when a data subject or a user who uses the system own or control the data they provide to the system. In the case of the blockchain for credential management, users. The control theory of privacy fits well with self-sovereignty, privacy is an access control about the information of oneself. It also encompasses many features of the definitions of privacy. To elucidate further, Charles Fried, writes “privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves” Pragmatically this is difficult to achieve, personal information about us seamlessly slide through computer systems across the globe. Therefore, to control our information, it is vital to give access only to relevant information to the right people for the right amount of time. The relevancy of information and the timeframe of accessing the information depends on the type of service that people sign up for.

Since achieving complete control of privacy is not practically possible Tavani’s interpretation of privacy which is “one has privacy when access to information about oneself is limited or restricted in certain context” holds good in essence that privacy is achieved when there is a restricted access to one’s information. However, as Tavani points out the control theory has a few shortcomings. One being the amount of control that a user has on his/her data is not well construed. A solution to this problem is considering the RALC (restricted access or limited control) theory. According to RALC, an individual has privacy “in a situation with regard to others [if] in that situation the individual . . . is protected from intrusion, interference, and information access by others”. The emphasis on privacy regulations depends on the normative zones being laws, regulation rather than looking at privacy from a descriptive sense. Situations could be any such as signing up for applications in Facebook, allowing websites to track cookies or giving access to personal medical records to insurance companies. It is the situation or the zone that is used in determining whether the information is normatively protected, not the information itself [49].

Control on the other hand is essential aspect in the management of privacy. Control is managed through three important principles in RALC which is choice, consent and correction. Consent is attributed to the granting access of personal data to third parties in exchange for their service. Choice is attributed to level of abstraction of the data shared to these third parties and correction is attributed to giving individuals access

to amend their information if necessary [49]. An example of the above, is presented in a permissioned blockchain where restricted access to only institutions that were certified was provided. The institutions were allowed entry under certain rules to modify and access the data. This, however, is possible but not practical in a public blockchain system where to modify data, consensus of 51% of the nodes is needed. An issue that blockchain can inherit through such a model is that if a malicious node or actor takes access to 51% of the network, then they can manipulate information. Hence the system while design needs to account for such incidents and provide mechanisms to prevent the same.

Blockchain plants itself in between anonymity and traceability tensions. Each transaction in a blockchain includes a cryptographic proof however they do not provide full anonymity [64]. Anonymity works on the principle of masking information without revealing the actual details of the transaction. However, this isn't the same as hiding information. For example, if there is a mask that covers half of a person's X face leaving the other half exposed. A person Y who doesn't know person X would not recognise X immediately, however a person Z with much more information on person X can still identify X after sufficient observation. Hence masking parts of your identity or pseudo anonymization doesn't give complete anonymization.

Another problem with anonymization is the issue of legacy. Since the architecture of the chain cannot be changed new cryptographic techniques can break these older anonymization practices used in the chain before.

Blockchains are also immutable hence storing user keys on the blockchain can lead to more harms in the future with the advent of decryption technologies and quantum computing. The question on how to leverage the good characteristics of blockchain without impeding user privacy is to be studied in the technical investigation chapter.

5.1.3 Trust

Trust is a manifestation of attitude between two parties where trustworthiness is a grounded property of that attitude. The nature of trust can be ascribed to relying on other parties to be obliging to the trust through performing actions which we want them to do and relying that they will complete the set action. Hence trust is a correlation to reliance. This reliance on an another party is not a mere to part relation. A trust B to do C, hence in this way, trust can also account for an action that is performed. A does not need to trust B always but trust B in achieving C [78]. Blockchain bridges trust through its consensus mechanism. A trusts algorithm P, B trusts algorithm P and together A trusts B with algorithm P in achieving C.

For the scope of this research trust can be non-motive or normative based. The trust in stance means more than willingness to do the action C but expectation that they will do the set action. Two excerpts from Hawley attribute of normative trust is discussed here [78, pp. 4].

- *“can be implicit or explicit, weighty or trivial, conferred by roles and external circumstances, default or acquired, welcome or unwelcome.”*
- *“be trustworthy, in some specific respect, it is enough to behave in accordance with one's commitment, regardless of motive.”*

Trust entails forming and nurturing relations between stakeholders of a system. Stakeholders trust when they have confidence that the other stakeholder will not hurt even if they can [44]. A factor that enables or impedes trust in the system are open source algorithms, efficient communication between stakeholders, binding network rules, robustness of the system and investment costs to attract stakeholders to use the system. Scalability an attribute of robustness, is an issue that plagues blockchain development in any application context. As the number of actors in the system grow, blockchain requires more computational power to run the system. Therefore, the costs go to process the system increases. Thus, the benefit blockchain had in terms of reduced storage and application costs is lost in this bargain. Also, as the size of the blocks increase the transaction speed is reduced. Study on the bitcoin application of blockchain technology shows this. As educational institutions process huge quantity of data, this issue might hinder the development of blockchain technology in education. Trust is the primary factor in our system. The research has identified two forms of trust.

Ramchurn et al. has conceptualized trust in a multi-agent system in two folds.

- system level trust or meta trust whereby the stakeholders are enforced to be *trustworthy* with the protocols(rules) that are present which regulate the system.
- Local trust is the projected amount of trust of you in other nodes and is not based on the trust in the system (blockchain). [67]

We categorise the trust models to be reputation based and learning based trust.

Learning Based Trust is the *direct interaction* that a node (University/ recruiter/ student) has with respect to other nodes. Thus, this trust is an emergent property of the system. This above statement holds good to the definition that “*Trust as a social phenomenon that is inherently based on multiple interactions between two parties*” [65, pp. 67] This means to say that trust between two nodes is a dynamic property. It is a function of the ties that the nodes develop over a period of time due to their respective interactions. If there is a deflection or a mistrust between two nodes, then trust utility between the two nodes are subjected to change. Alternatively, if we take an example of nodes that trust each other, the net payoff for the system is higher.

System level trust or meta-trust is the trust on the entire system. Blockchain offers a decentralized architecture that offers reliability against attacks and reduces the need for regulation. This manifests the value of self-governance. Researchers have recognised the difficulty in handling globally distributed skilled workers in a dynamic code developments environment such as Bitcoin. In such an environment, a group of designers executes challenging tasks through consensus, collaboration, and dialogue. Self-government applies to the autonomous facets of the blockchain ecosystem, which enable the different components of the network (e.g. mining, application creation, management of nodes) to function without interference across widely understood structures and dynamics. The various functions of the framework are performed in the blockchain environment by a consensus process. A factor that would hinder this would be subcultural influences and self-regulations. Upon observation of open source implementation of Bitcoin, Mozilla foundation, self-regulated communities with a shared consensus on decision making on code algorithms is seen as an important value to be successful.

5.1.4 Usability

Usability according to ISO guidelines is defined as “*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*” [84, pp.14] Design trade-offs can impact values with the matter of usability. Usability is an important aspect that is critical to design in order to reduce errors as well as improve user experience. Higher usability design considerations can have an impact on ethical values. An example to illustrate this would be when websites provide easy access to personal information unintentionally provides easy access to third parties as well. This diminishes the values of privacy.

While addressing the values of privacy, trust and transparency with respect to certification management and blockchain technology, technical bottleneck arises. A famous saying that fits perfectly to privacy is that “The more secure you make something, the less usable it becomes” from the empirical investigation one of the key concerns of the stakeholders was on the security of personal information. Public- private encryption techniques definitely make the system more secure however losing a private key means that you also lose access to the system. A fix to this would be implementing a master key with a key hierarchy and giving the master key user rights to revoke and change it's child keys. This however provides a safety net but brings an unintended effect on transparency of the system. The user with the master key then can control the system and the system it not distributed anymore which ultimately challenges the core principle of blockchain being a decentralized technology. Also, an inclusion of a master key shifts the sensitivity to it and losing a master key would mean compromising the entire system. Every additional measure would move the problem around without creating a solution.

It is important to point out that “some architecture decisions may unknowingly limit the ability to implement usability requirements” [85, pp.469]. As the system grows, the size of the blocks increases. This would

mean more computational power is required by the algorithm to calculate the next block. Hence scalability comes at an increased cost, reports suggest that the bitcoin blockchain consumes more energy than the entirety of Switzerland [86].

Decentralized architectures raise issues of usability with respect to entity authorization, policies for revoking rights, validating credentials and distinguishing channels of trust [86]. These issues have been reflected in this research, what are the means to authorize new education providers, what are the means to validate documents, what are the means to encourage and thus also quantify trust between stakeholders and what are the means to revoke access to the system in case of malpractice. These issues add additional layers in terms of what the system should produce. Johnson et al. [86] points out that users would use even the least user-friendly systems if policies are in place that inform the need of these processes which would stimulate security or transparency over the ease of use. This however would not be true in every case but cases where data security is very integral and fundamental. An argument can be made that certification management is a fundamental system where compromises on usability can be made at benefit of having a system that promotes data integrity, transparency and trust.

Conclusion:

The conceptual investigation examines the relations between usability and human values. Based on the conceptual analysis, the three most important values from stakeholder's perspective is analysed and the resultant values that the system design should account for is shown in the figure below. Figure 8 summarizes the value support and tension for certification management using blockchain technology. The three intended values along with its manifested values. The three intended values are privacy, transparency and trust and the three manifested values are access, self-sovereignty and self-governance. Indeed, it can be said that from a conceptual viewpoint the values would support each other. However, this conceptual investigation does not compare mere values but also technical bottlenecks that arise. These values don't usually have this relationship, this is more on a case to case basis. Self-governance wouldn't always impede usability, however in this case the algorithm developed may not be efficient in scaling because of blockchain's inherent architecture and hence would prove to also impede usability.

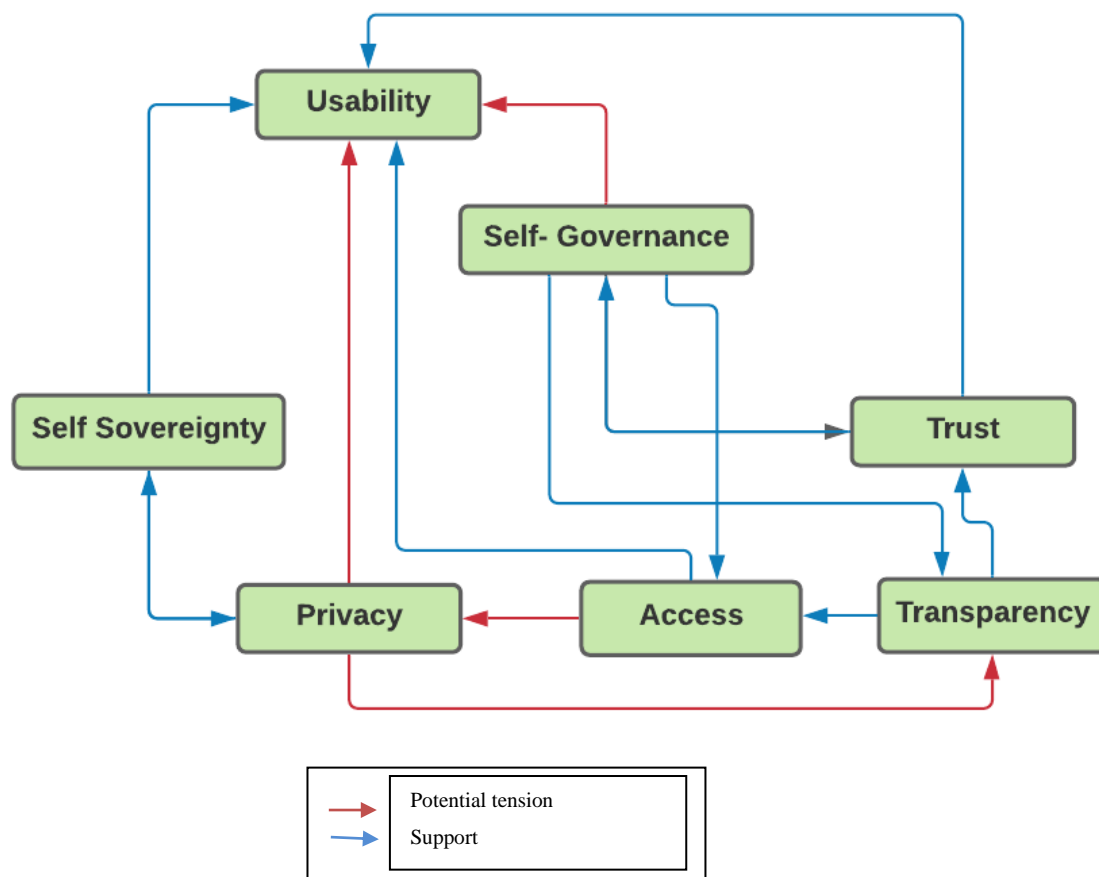


Figure 8 Conceptual interaction between values

Self-sovereignty supports privacy as the user would have control of their own data however impedes traceability. The transactions in the blockchain are anonymous and hence it is difficult to trace back to the origin of transactions. Similarly, for certification management, personal data cannot be stored on the chain due to blockchain's immutability and there are negative consequence of privacy. Since transparency promotes access, also placing strong importance on communication of stakeholders through proof of algorithms. As nodes would add new nodes through the consensus mechanism, the design needs to inform the stakeholders on how the process is conducted. Hence the medium of communication on whether a node is added or not at a certain timeframe is the proof of the consensus mechanism. Likewise, trust and self-governance support each other. The trust of the stakeholders of this education system. The system can be trusted if mechanisms place are able to verify and validate new education providers to the system. The blockchain infrastructure is intended to be open to all parties that provide education. Using the network infrastructure malicious nodes can enter the system and take control of it by capturing 51% of the system. Hence the overall privacy and security of the system is compromised.

These value relations can be used to ponder design strategies in certification management. By linking intended and manifested values, distinction on which values support or hinder the design can be understood. Values can also be singled out or taken in pairs to understand value conflicts. Based on these table 4 informs us research themes for designing principles.

The research theme is used as a goal and sets criteria on what to achieve in the technical investigation. Promoting access would mean setting up infrastructure that would enable easy access for users and stakeholders to use the system. Promoting transparency means the right information is disclosed to its users. Reconciling needs of privacy and security is important as during the conceptual investigation a value trade-off has arisen between immutability and privacy, hence new methods are studied which would still enable self-sovereignty and also ensure privacy is preserved by the system. Self-governance is important if trust needs to be prevalent in the system. In earlier system trust was provided by the third parties however, in the blockchain system algorithms would deliver trust. Hence these algorithms deliver the control that in turn promotes trust in the system. An algorithmic proof is derived that could add trusted parties through a proof of stake algorithm, this is studied in detail in the next chapter.

Table 4 Research themes for design

| Research Themes | Value Categories |
|---|------------------------|
| Promoting access | Access |
| Promoting transparency | Transparency |
| Reconciling needs of privacy and security | Privacy |
| Promoting trust in the blockchain | Trust, self-governance |
| Promoting data identity | Self- sovereignty |

Chapter 6- Design Principles

Design principles inform the designer on different objectives the system needs to adhere to. The research themes were derived from the value relations from the conceptual investigation. The objectives that were derived from the empirical and conceptual investigations are listed as challenges that the design needs to overcome. The design goals give a direction of analysis. The research themes form the basis for the design principles and are open ended however the design goal is based on what the technical characteristics that the system needs to possess. The design goals were based on literature review and empirical research. The feedback got from the interview was used to fine tune the design goals.

Most of the possible implementations of blockchain revolve around its potential to permit trusted transfers of credentials, credits or other properties between stakeholders in the network. A crucial foundation of any blockchain strategy should include initiatives to empower these systems and to utilize the full potential of blockchain to improve and facilitate the transfer of such assets. The value centric framework captures the important points of stakeholder perspectives and concerns combined with the philosophical bearing of these values. This helps shape the design of the blockchain enhanced certification management to achieve its full operational potential.

I use the word system or application interchangeably. The word system refers to the application of blockchain enhanced certification management. Based on our conceptual understanding of values we now know that blockchain cannot be a singular application that satisfies the objectives of certification management, however it can form an integral part of the application with the support of other technologies. The application that is set to be achieved is blockchain enhanced certification management.

Table 5 Design Goals

| Research Themes | Challenges | Design Goals- "The design must be/have" |
|---|--|--|
| Promoting access | Conflict of different services on the blockchain | relevant boundary conditions |
| | Open for all | open public architectural design |
| | Demarcation of rights of different stakeholders | permission rules of rights of access |
| Promoting transparency | Right to be Forgotten (GDPR) | non personal data to be stored on blockchain |
| | Data Mismanagement | off chain storage |
| Promoting needs of privacy and security | 51% node takeover by malicious parties | relevant trust architectures |
| | Legacy of anonymization techniques | encryption and preventing personal data on the chain |
| Promoting data identity | Self- sovereignty | appropriate application design |
| Promoting trust | High number of participants | able to be scalable |
| | Trust between participants | able to provide consensus on decision making |
| | Trust on the system | able to prevent data leaks |

Based on our analysis there are five design principles that the system should have

The system must promote access to the application

This principle addresses the access to the application. As stated in the empirical and conceptual investigation, the system must be easily accessible by all parties using the system. The design principle protects the value of access. The decentralized access of public blockchain facilitates high transparency and equal distribution of rights among all users but impedes usability as seen in the conceptual investigation. Even though as a value access promotes usability, the technical complication of blockchain doesn't allow a central authority to govern and hence if functions and accesses when not clearly demarcated would lead to an inefficient system. As seen in Chapter 2 certification management entails different services such as issuing certificates, verifying them and distributing them to different parties involved. To attain full capability, it is important to assign access rights with permission rules to relevant stakeholders.

An aim of a design principle is to unravel the full potential of the system. Looking at the research spectrum from the system designer's point of view, the empirical investigation state that educational organizations are uncertain about the services that should be placed on the chain and conceptual investigation highlights on blockchain's multi agent complexity leads to institutional uncertainty. Hence relevant boundary conditions can help designers with understanding which services should be placed on the blockchain and which shouldn't.

Only fully open implementations can reach the design goals set by the system. The goal that the system should be open for all type of educational bodies such as online mediums as well as reputed institutions. Hence it should have a public blockchain architecture in place that promotes this.

The system must promote transparency of information

Based on the argued definition of transparency and data mismanagement is identified as relevant to stakeholder values, it is important to protect and restore data in the event of a data loss or the user losing his/her public or private key, there has to be off chain storage of data to protect from such incidents having a major impact to the functionality of the system

The value of transparency adheres to normative terms such as regulation as explained in the conceptual investigation. The design principle safeguards the value adhering to normative regulations. The legal regulations in place inform systems to delete the data whichever the user informs the data controller. Due to blockchain's immutability deletion of personal user sensitive data is not possible if it's placed on the chain. Any personal information stored on the blockchain must be done with consent and must be informed to the relevant parties. To avoid this technical limitation and future problems from arising, it's recommended that the data stored on the blockchain should not be personally identifiable information.

The system must promote data identity

Even though self-sovereignty is a manifested value of privacy, blockchain's immutability does not allow for storing personal information on the chain, hence it categorized as a separate design principle that the system must comply to. One of blockchain's unique selling property is that it promotes self-sovereignty. This also resultant on the choice, consent and correction that is attributed to the data subject, the user needs to be given propriety ownership of their learning assets. However, it is noted due to other legal and privacy constraints mentioned in the conceptual investigation personal data cannot be stored on the chain. Hence relevant application design/interface needs to be in place that promotes the system to entail data identity.

The system must promote the needs of privacy and security

This principle aims to address the problem of compromising the integrity of the system by providing the right control measures. Since blockchain works on consensus mechanism, a malicious node or a party can control the chain and its data if it has access to 51 % of the chain. Hence relevant trust architectures need to be in place to prevent nodes from gaining unfair access of the system

Public and private keys are classified under pseudo anonymization under legal regulations. They become legacy entities when there are better decryption techniques that are developed with higher computational

power. Hence there has to be a clear recognition of the data which is put on the chain and the level of encryption that it entails.

The system needs to promote trust

Fundamental problem of a distributed system is to achieve system integrity and reliability in the existence of faulty parties. This is one of the most important design principles that the system has to have is trust. Consensus mechanism forms the core of any blockchain system, mediating conflicts and defining the rules that make sure that a newly added transaction is legitimate. Due to the trade off between system's openness and systems performance different trust architectures can be used. Thus, the consensus mechanism as algorithms safeguards the value of trust

It is seen that dependability of a system is restricted to how they prevent attacks and data leaks. Since the educational institution garner a lot of sensitive information, it is very important to have a secure protocol to protect the system.

Additionally, one of the goals of the system is to have an international participation, it would mean that there would be high number of actors and stakeholders. This however increases the overall system complexity and hence the system should be scalable. To forge trust between participants is essential. Blockchain's consensus mechanism has to trustworthy so that the nodes agree with each other on the addition of new nodes and other decisions.

Conclusion:

This chapter forms the foundation on the implementation of the technical architecture in chapter 7. The five design principles developed based on the argued values in the conceptual investigation provide a base to implement these design guidelines through the architecture of the technical application. As stated before, there are more necessary design principles with the addition of new values.

Chapter 7- Technical Investigation

This section focuses on the design of blockchain application for education. The technical investigation sets to fulfil the design developed in the conceptual investigation. This chapter mainly reflects as an example to achieve the set design principles which is derived in the previous chapter. The design of blockchain has to possess three layers. An application layer, a database layer and a blockchain layer. The application layer facilitates signing of documents between end users and educational organizations. The database layer stores acts as a layer of communication between end user and educational organizations. The blockchain layer acts as the trust layer between educational organizations.

7.1 Application Layer

The system must promote data identity:

Blockchain enables information on change in ownership however this is only possible when it is linked to a document. Storing documents on the chain can reduce the performance and also computationally inefficient with the large amounts of data. Another issue that arises with this is the problem of immutability. Even though immutability disallows tampering of the system, it also makes it impossible to remove a record after it is placed on the blockchain. The design principle also gives the rights of choice, consent and correction to the user. Hence the ownership of data should be maintained by the user and should adhere to the above principle. Hence personally identified information such as certificates have to be stored locally, the blockchain only acts as a tool to authenticate and verify the transaction. This solves two issues, privacy and ownership of the certificates is handed over to user of the system and also removes the dependency to remove personally identified information from the chain since all the personally identifiable information is stored on the local device of the user.

The application layer needs to be able to execute the following functions:

The user should be able to:

- Store certificates which only they have access to
- Send the hash of the data (certificate) to the database layer where it is stored in a central registry
- Share the certificate with relevant third parties

7.2 Database Layer

The system must promote access to the application:

The system is open for all parties. Hence it should allow all parties to access the system. The database layer provides the base for accessing the system. The database layer is connected to the blockchain however not all services happens on the blockchain. The blockchain is only used as to provide access to the relevant parties.

The access append information to this database is provided only to parties that are part of the blockchain. Hence the blockchain only has information on relations between different nodes. Overloading the blockchain with too many services can add to the scalability problem. The database layer is only used by education providers, the user mainly send and receives hashes that they can share to the third- party. This defines the design principle for promoting access to the relevant parties.

The system must promote transparency of information:

The transparency of information needs to account for data mismanagement. Hence the database is stored in the centralized registry set up with the DHT protocol to facilitate retrieval of data. Since pseudo anonymized data can also be categorized as private data by legal regulation, it is not advisable to store in

blockchain. The database layer is set up in the following way. It uses a DHT protocol. DHT means Distributed Hash Table. It is essentially a database and allows parties to store hashed certificates on the database. A distributed hash table is a look up service that enables peer to peer sharing [65]. It enables protocol identity. Protocol identity ensures that all devices on the network trade under exactly the same conditions without the need for a central authority to verify that the rules are observed.

Interaction between application and database layer:

Below are the steps that the application and the database layer need to use to complete the process

1. The end user requests for an educational organization for a certificate using the application interface.
2. The educational organization decides whether the student has completed the course by verifying this with the university database.
3. The university send the signed copy back to user and the user can save it locally in their device.
4. The university encrypts the certificate and stores the hash of the certificate on the DHT and send the hash to the user.

The encryption technique is a resultant of the design principle protecting privacy, it is done so that sensitive data can be shielded from malware and attacks.

Components of a digital signature include a SHA-256 hash, a public key, a private key and a timestamp of when the digital record was created.

A document is signed by combining a hash of the document with a person's private key to create a unique code.

The resulting sign is then combined with the certificate and the timestamp.

Note that the unsigned document and the signed document have different hash values meaning that any changes to the document would result in a completely different hash value.

This would mean that the application would be tamper proof.

7.3 Blockchain Layer

The system needs to promote trust:

The system needs to have a consensus mechanism to check addition of new nodes and to propagate trust to all parties in the system.. The design principle states promoting trust entails satisfying the objective of knowing the trust between participants. This is done by setting up a trust chain. The process is explained below.

7.3.1 Trust chain

A trust chain is a set of relations between different nodes of the chain. The links are formed based on the trust the nodes have on each other. If there is no trust, then there is no link formed between them.

The links between nodes are trust connections. When there is no link between nodes no trust exists.

To determine the importance of a new block, and since a block is a list of transactions, we take the sum of the importance of all new transactions in the block. The importance of each transaction is determined on how much value this transaction adds to the network. To calculate this, we can add the *trust values* of the two nodes that this transaction connects [89].

The trust value of a node is how much this node is connected to the rest of the network, in other words the inverse of the average distance to other nodes. The trust link is generated based on a trust value which is a mathematical calculation based on the graph distance between nodes.

$$t_p = k^{g_p}$$

Where tp is the local trust value in peer p , k is a constant describing how much trust is conveyed in one link (e.g. if node A adds a peer, how much trust would it have on this peer, ranging from 0 to 1)
 g_p is the degree of separation between a node to an existing node and peer p , this means the shortest path connecting me to peer p , in the graph where every link is in the form of “A trusts B”.
 The quantity for distrust is 0 when the k factor is 0 the nodes do not form links with each other and there will be no path through them.

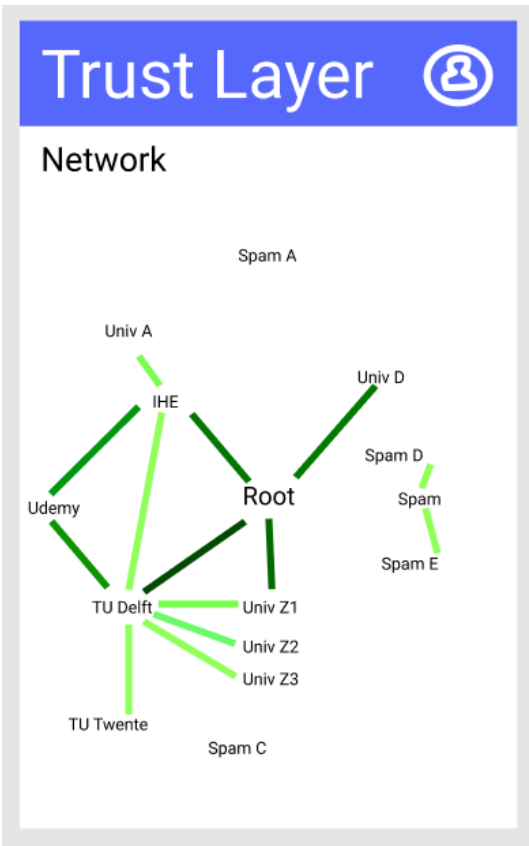




Figure 9 Trust Chain

Legend:

| | |
|---|-------------------------------|
|  | Initial nodes in the network |
|  | Nodes added in the next cycle |

Blockchain:

The blockchain acts as the trust layer or the trusted intermediary in the system. The blockchain is made up of blocks. Each block is a list of records, where each record contains the following, chapter 2 has a detailed explanation of this:

1. Trusted party- Nodes that are already in the chain
2. Trusting party- Nodes that to be added to the chain
3. Timestamp

These blocks are created each fifteen minutes. The timeline of the blockchain is given below:

| 0 minutes | 15 minutes ago | 30 minutes ago | 24 hours |
|--------------------------|--|--|--|
| Transactions are created | Peers create blocks and distribute proposals | Peers add the block with the highest stake to their blockchain | The blockchain is finalized. Whenever a conflict occurs, rewrite blockchain. |

Block formation

The block formation happens in three stages:

1. Nodes create new links in the trust chain, the application spreads them to a subset of other peers.
2. Nodes create block proposals with the best links and broadcast them.
3. Nodes receive other block proposals and select the best one
4. Retention period: if better blocks are received but not in time (because of network errors for example), the node should be able to rewrite their local blockchain using the better blocks. If he had any links that he included in the falsified blocks, the application should re-broadcast them to be included in a new block.

In stage 1, nodes need to keep a cache of the best new trust links that they know of, and periodically send and receive these links to their peers. The aim is that new trust links to reach everybody, especially the most important nodes.

Block selection

Nodes trade under the same access conditions as stated in the design principle. Every node should follow the same protocol for selecting the next best block. The protocol looks like this:

1. **Transaction distribution** – Nodes create new signed trust transactions and distribute them to other nodes
2. **Block creation** – Nodes create blocks with aforementioned transactions and distribute their created blocks
3. **Block selection** – Nodes verify other blocks and select the best block to be added to their local blockchain

7.3.2 Proof of Stake

To allow peers to reach a consensus over which block to add next in the blockchain, all peers need to follow the same transparent protocol, and furthermore need to be able to provide proof that they are the ones that should be able to append the next block which the peers can then verify [88].

Each block should increase “value” of the network by adding to the total trust while expanding the amount of trusted peers. Furthermore, the system should not let the root node being able to dominate all additions to the network. The following formula for calculating block relevance is proposed

$$b = \frac{||\{C...\}||}{\sum_i |dist(R,C) - m|} , B_i = (C, D)$$

where

- b is the block relevance
- B is a list of all trust relations in the block
- C is the trusting party of entry i in list B
- D is the trusted party of entry i in list B
- $||\{C...\}||$ is the amount of different trusting parties in the block
- *dist* is the graph distance function

- R is the root node
- m is the average graph distance to the root node of the current blockchain

Each block consists of a list of relations $C \rightarrow D$, where C is a party that is already in the blockchain that trusts a party D to be added.

Proof:

Because all nodes will put the block with highest relevance next in their blockchain, nodes that propose a block will need to provide proof of their relevance, which is the function of the distance function to the root of the network: nodes will only be needed to provide a list of (trusting party, trusted party)-relations to the rest of the network in order to verify that their block is the 'best' block. The value m is the same for every node because all the blockchains at th time before the next block will be added will all be the same, and changes only once per the addition of a new block. In the figure below a new block is not added because it has not trusted relations to the existing blockchain.

The system must promote the needs of privacy and security:

The system needs to control malicious nodes from taking control of the entire system. A few theoretical attacks on the system are provided below to show that this would not be possible

1. The root node tries to keep control of the whole network by filling blocks with relations (root \rightarrow A, root \rightarrow B, ...). Because we subtract the divisor by m, once the network grows, the root node will not be able to make relevant blocks anymore.
2. A malicious party is added to the network, and before it is revoked, tries to add many more malicious nodes to the network. Because it can only sign new relationships with itself as a trusting party, it can only add one to the dividend. Hence it doesn't matter how many relations a new party has, the number of trusted relations within the blockchain takes precedence.

The research has demonstrated how the blockchain can be used to send and receive academic credentials. A major insight is that blockchain alone cannot be used to perform the design principles based on the value criteria set up the from the empirical and conceptual investigation. It needs to be ably supported with other technologies such as an API interface, a database layer and TCP/IP network layer explained below. Blockchain acts a intermediary that enables trust in the system through it's distributed architecture.

Use of the TCP Layer:

The network layer is used to distribute all protocol messages, ranging from the spreading of new trust transactions, block proposals, and document exchange. We have the possibility of using TCP or UDP. While TCP guarantees an ordered stream of data and is connection-oriented, UDP does not provide this guarantee.

TCP is supported on every network. Peer-to-peer communication is only possible when nodes open their ports, or using some form of hole-punching. With hole-punching, a node A that wants to connect to a node B sends this request to a "hole punching server", which *punches hole* in the NAT-systems where A and B are connecting from.

Since we want to encrypt all communication with nodes, we are gonna use SSL. This is a protocol that can run on top of the TCP layer. Over this encrypted connection we can then send all data in the form of packages. This packages take the form of the tuple (package type, content). A new trust link can be sent as (NEW_TRUST_LINK, node A, node B, timestamp, signature).

Application Functions:

The application should be able to handle the following

- Blockchain: appending blocks, verifying trust connections
- Block selection: proposing new blocks, verifying other block proposals

- DHT: spreading and storing documents
- Trust chain: calculate trust for nodes
- User interface: creating documents, adding or removing trust links

The control of application is spread into layers: the application layer handle all user inputs and outputs, as well as the blockchain logic and trust calculations. The database layer translates user requests into the proper queries; the network layer handles the sharing of documents and creating blocks.

Scalability Concerns:

This formula determines the trust of node A by taking the inverse of [summing the distances to all other nodes B, divided by n, the total amount of nodes in the network]. This results in the inverse of the average node distance to A which we can call *connectedness* of node A.

When we use this trust value to prioritise trust transactions, every node needs to make the same calculation to verify that a trust transaction is indeed important. However, the formula as it stands can quickly grow unwieldy without optimisations: if we have a thousand nodes, we need to calculate a thousand trust values. And for each trust value at node A, we have to traverse all other nodes and calculate the distance to them. This process has a runtime complexity of $O(n^2 * m)$, where n is the amount of nodes in the network, and m is the amount of links. Furthermore, this process has to run again after each new block.

This formula does not have the disadvantage of giving the root node all power or giving the node that is on “average” distance to the root all power. It also does not allow malicious nodes to quickly generate local communities with very high trust, because the *connectedness* of such nodes (and their malicious peers) to the rest of the network will be small.

Scalability will quickly become an issue with this approach, as every party has to calculate the trust for every other party. There also arises the issue of a *split-brain scenario*: when two groups of people trust each other but there are no trust links between the groups, the *connectedness* of the whole graph goes down.

Conclusion:

This chapter illustrates how the design principles can be achieved through the technical architecture of blockchain. Scalability is an issue that needs to be addressed. Added to this blockchain brings in a lot more complexity rather than traditional databases. In solving one problem, it creates two more. In an ideal world the proof of stake algorithm developed in this research would face issues on the linearity of branches, meaning on two distinct branches where the nodes to be added satisfy the same condition, it could result in a blockchain where both the nodes could be added and such cases would lead to hard forks resulting in two blockchains. Another scenario is an issue of split-brain scenario, where two groups of nodes trust each other but there is no trust link between them, in such cases the *connectedness* of the whole graph would reduce.

Chapter 8- Conclusion

The chapter answers the research questions that were formulated in Chapter 1. The research focused on educational administration of credentials. The objective of this research was to understand and facilitate design principles for the adoption of blockchain in credential management

What is the current known potential of blockchain in education?

In this research credential or certificate management has been studied closely and design principles for building such applications has been given. However, blockchain can traverse other domains of education such as learning outcomes management where blockchain is used to evaluate the students' performance where each transaction describes an activity and a sum of all activities performed is coded into a block. contributed to a prompt and meaningful learning environment for students to encourage critical thinking and collaboration.

Blockchain can be used as an effective tool to check and approve transfer of credits without relying on third party or an intermediary. Blockchain could bring substantial advantages to educational applications through its distributed architecture providing management of access (self- sovereignty being one of its benefits), immutability leading to transparency of transactions, cryptographic security and low cost by cutting out intermediaries. As seen above it also provide efficiency of handling student records, improving interactions between students and supporting life-long learning and in-turn also enhances learners career decision.

Blockchain ensures privacy of transactions between peers or trusted parties through its consensus or trust algorithm. Dependability of transactions is ensured through its cryptographic hashes. The educational field could value from blockchain such as cutting out third parties, reduced use of cloud service and an overall reduced cost of system transaction using a permissioned blockchain. However, on a public blockchain controlling assess and data is difficult and the responsibility of scalability for which not many viable solutions with reduced costs are prevalent. Added to this correcting wrong data which is close to impossible with blockchain's immutability presents an additional limitation.

The domain of education and its potential is huge. There are different administrative features ranging from certificate management to improving learning outcomes that blockchain could fit in. The true value of blockchain stems from its public architecture, cryptographic security and its open consensus mechanisms. But the technology it's still its infancy. There are structural issues with respect to legal regulations, user's perception towards using blockchain, technical uncertainty with pseudo anonymity, scalability and general network binding rules. There isn't a clear cut picture at the moment of the value of responsibility, as to who takes the blame if something goes wrong, in the case of a data leak or in the case of an extended downtime of the system or in the case of a distrust between important stakeholders.

A recommendation of this research would be to let blockchain grow from grassroots. Reflecting on past technologies such as internet, its origin was that of an intranet with a few nodes between trusted universities built for the purpose of sharing host to host messages. Later, technical know-how on interoperability and reliability was ensured through an extended research in the creation of the TCP/IP layer. There were also a few organizations such as SUN and XEROX to name a few that needs to be credited for systematically applying and testing algorithms on a permissioned level to understand and efficiently grow the technology. After about 20 years, it later became the behemoth that we know of today. The same principle has to be applied to blockchain as well. There is a misguided perception that *blockchain is a solution that is searching for a problem* and this argument can be observed across certain literature and business articles alike. This argument is however skewed because in certain applications the limitation of blockchain outweigh its benefits.

What are the values needed to be incorporated into the design of blockchain application for educational administration?

The scope of this thesis is certification management. Certificates are documents that provide evidence of achievement, in educational field certificates relate to achievement of learning results. Certificates could be

provided by institutions, online mediums or any accreditation body permitted to give certificates [3]. The traditional methods of issuing certificates are archaic and inhibit new pathways to learning and access education.

The findings of the interview clearly indicated that values such as privacy, transparency and trust are the most important values to be realised in the actual design. Blockchain technology allows for users to be able to automatically verify the validity of certificates without the need for the organization that originally issued them. Certificates by itself involve a set of process. A organization in which the learning has taken place *issues* a certificate, the certificate is then recorded in centralized register owned by the organization. The next process of *validation* is to check the legitimacy of a certificate which involves third party vendors to verify the claims. The last process of *sharing* is when the certificate is shared to other parties for various reasons such as securing a job or to an educational institute for studying purposes or for student grants, loans, etc.

In this entire process the trust is delegated to third party organizations. The identity of the issuer and the holder of the certificate has to be verified. Verifying identity is often a complex process and the third party would require additional data and methods to validate it. Security features in these certificates as described in Chapter 2 can be forged and in some cases as pointed out in the empirical investigation (chapter 4), the third party organization can turn out to be fraudulent or at times do not perform an adequate job due to lack of resources. Hence the concept of trust in the third party is flawed. This was identified and new forms of trust implementation has been discussed in the technical investigation. This research has provided an algorithm to calculate trust. The parties that are in the system do not need to rely on third parties to validate certificates but can do that themselves. Hence the value of *trust* has been incorporated on the design of the application.

In this research several instances of data leaks arising out of single point of failures have been discussed. In the empirical study as well, these issues were raised. All stakeholders unequivocally raise the importance of privacy. Added to this during the conceptual analysis links between privacy and self-sovereignty was identified. Self-sovereignty was also a trait of blockchain architecture; however it has a trade-off with respect to the immutability of blockchain. This was accounted for in the technical architecture and a viable solution was presented in chapter 6. Since self-sovereignty is an important finding of conceptual analysis and also mentioned as a value proposition the application needs to process, this research used an application interface that could let users share the data that is important instead of providing entire transcripts of academic records. The data is verified by the distributed ledger and the network layer provides the overall trust mechanism to the blockchain.

Transparency with respect to information disclosure was also an important value that stems out of this search. Often at times there is lack of communication between the third party and the institutions/students. Mismanagement of data by third parties is an additional worry stakeholder are cautious of. The blockchain ecosystem provides a tamper proof and open source architecture where activities and information can be cross checked across the domain and this would give much needed reliability which is lacking in the current system. The values were mapped based on their conceptual and a value network was created in chapter 5. Based on the value network five important design principles were developed for the implantation of blockchain enhanced certification management.

How can blockchain be used as an ethical or value sensitive application of certification management?

The notion that blockchain is a standalone technology by itself is wrong. Blockchain is a combination of a set of technologies that facilitates infrastructure for reshaping interactions of users and organization. There is certainly a positive reason to use blockchain applications. It enables micro accreditation, promotes trust, provides security and privacy of transactions and enable transparent interactions between stakeholders and end users.

The research finds that blockchain technology could reduce educational institutions costs when coupled with databases creating structures of increased ownership and control over their data for its users provided the issue of scalability is fixed.

Blockchain thrives in multi actor complexity. It's open and public architecture can combine multiple theories and practises into its algorithms. Proof of stake algorithms provide a basis for trust. However, its computationally intensive architecture and its immutable functionality does not allow for personal information to be put on the chain. Hence third-party applications have to be looked at. Blockchain is a supporting technology that can attribute trust and transparency to the entire process, it cannot bring about all functionalities that an educational credential management needs.

What are design principles for blockchain for administrative educational purposes that help to meet relevant values?

The main design principles (table 6) needed to meet the relevant value criteria is explained in chapter 6. The findings of the interview clearly indicated that values such as privacy, transparency and trust are the most important values to be realised in the actual design. By narrowing the design goals down, a preliminary assessment of how the design can be addressed and analysed is given in chapter 7. There could be other explanations that could offer better solutions. It is seen that the proof of stake algorithm offers a mathematical proof that is robust and reliable however does not satisfy all the challenges that the empirical analysis in chapter 4 had prescribed, the most important challenge being scalability. The proof of stake uses the relations built by the trust chain to construct and expand the blockchain. Issues of hard forks and split-brain are seen as challenges to this public blockchain. Private blockchain can deal with these issues however private blockchain inhibit access which is one of the main goals of the design needs to accomplish.

Table 6 Design Principles

| Design Principles |
|--|
| The system must promote access to the application |
| The system must promote transparency of information |
| The system must promote data identity |
| The system must promote the needs of privacy and security |
| The system needs to promote trust |

Blockchain has a high complexity of technologies that does not provide solutions to all the challenges specified by the stakeholders. Hence different applications have to be used in consortium with blockchain to achieve the objectives presented. The database layer uses a distributed hash table which is built on centralized databases to leverage data mismanagement. This again poses a single point of failure resulting in further challenges.

My reflection will be that blockchain is indeed in its infancy, utilizing existing technology with blockchain brings back the issues that blockchain addresses in the first place and thus a conundrum. Legal regulations on privacy also pose problems on the decentralized nature of blockchain. As stated before, blockchain has a lot to offer in terms of its versatility of functions however at the moment public blockchain do not offer a great extent of value and also restricts usability. Private blockchain can be an immediate solution. A blockchain consortium of universities could be set up and new nodes can be added, to what extent would institutions trust and add other education providers such as online mediums remain to be questioned and studied.

There will also be reliability on third party dependencies. For example, a digital wallet to allow you to hold assets, a trading platform such as a DHT layer to allow the exchange of assets on the blockchain, tool providers that create interfaces to communicate with the blockchain and providers of storage solutions to offer ways to off-chain data storage. While blockchain eliminates the ability of any one party to manipulate the ledger the fact is there is significant technological, knowledge and resource barriers to entry at this point.

Private blockchains also however face scalability issues as the block size increases the costs to host and run the blockchain would eventually increase. But the ideas and theories of data integrity, open access, trust without the need of third parties, ownership of assets are all properties that are supported by

blockchain. With more research and a better technical design blockchain could well be the solution to issue of certification management.

Generalizability

Blockchain in this research is tailored for certification management but can be applied to other layers of education administration after studying the requirements and objectives of the use case in detail however, blockchain's technical characteristics analysed in this research can give necessary insights about its complexity and the domains in which blockchain is efficient. The role of educational administration would shift to a different process if blockchain technology continues to develop and in contrast educational administration process should evolve to capture the potential benefits of blockchain. The task of intermediary in educational institutions is positioned at the validating stage, which will change with the impact of technology where the people who maintain and develop the blockchain might act as supervisors and the technology in itself acting as a validator. The thesis also highlights the social value proposition of certification management as a fundamental process which needs to be open and accessible, the Syrian refugee crisis explains why this is the case. This thesis does not merely investigate the potential of blockchain but also how it can be implemented. This is an important facet as during the implantation process new challenges arise and thus could refine the initial objectives better. As the application grows positive externalities can be come into effect with the application including other functionalities which sequentially would improve the benefits of the system to its stakeholders.

The design principles are basic and can be adopted to other technologies that would certain solutions for certification management as well. Insights of this research can be used to get an empirical understanding of the issues of certification management and form objectives with a wider research spectrum with it.

Scientific relevance

The research adds new knowledge to understanding of blockchain and values in the context of education. One of the pivotal aspects of this research is that the identification of values is mainly based on the findings of the literature review and the interviews with respondents involved clearly understand the values influencing blockchain in certification management. The research contributes to academic literature in various aspects and is aimed to fulfil the knowledge gaps mentioned in chapter 1.5 based on the in detailed study on the subject.

Current literature does not focus on the values needed in the context of certification management. Other studies in related field focus on the values and value proposition of blockchain but does not focus on the values stemming from certification management. This research investigate the pitfalls and benefits of these values of blockchain and certification management together but also devoid of each other. Despite growing research in blockchain there has not been adequate design principles proposed for such an application. This thesis is aimed to bridge that gap. The multi actor complexity of blockchain has been referred in a lot of literature but there has not been a method to analyse this complexity. In this research a proof of stake algorithm is prescribed and can be steppingstone for public blockchains that use such an algorithm.

Another contribution to scientific research is knowing the actual actors involved in the development of blockchain in education. The study has initiated by identifying probable actors involved in the development of such application and contributes to knowledge gap in the empirical stance of different stakeholders in education and blockchain as a technology. It won't be appropriate to conclude that the research has identified all the actors involved as the scope of the application is large and with more complicated functionalities the number of actors involved with rise further.

To improve the understanding of the values, this study follows a systematic and a detailed methodology of value sensitive design which breakdowns the research into value centric investigations and accounts for values throughout the design process. These values can also be used for policy considerations and regulation changes for using certificates in decentralized manner in contrast to the current centralized handling of certificates. With majority of application and research focussed on fintech this study achieves to promote attention to education by discussing implications and application of the technology on certification management.

Other research institutes could improve the validity of the design principles with additional search and this study provides a base for future scientific research as the importance of blockchain in education is expected to grow in the coming years. The values that stem from this research are focused on certification management and can be applied to another technology as well. These values can be used as a reference and new and important values can manifest out of these. The design principles are directed to policy makers and educational institutions with a lot of credibility. Such institutions could stimulate the need for certification management and the social value that it adds.

Societal relevance

The importance of preserving data identity and self-sovereignty has been increasingly talked about from policy makers and adjudicators. On one hand the individuals rely on educational qualifications and without it they might not have access to certain jobs, income and future. On the other hand, society needs to make sure that the right people are doing specialized jobs otherwise it would result in a negative outcome for the society in general. This research gives guidelines on how to build an encompassing system in blockchain that gives control of data back to its users. At the time when privacy hacks and data leaks are a norm having a system where data security and self-sovereignty is preserved can lead to better prospects for different context of applications as well. As stated, before in due of natural calamities or social issues such as war leads to displacement of people. Rather than living unhappy lives with subpar jobs, such a system could offer them the work that they deserve. It could also offer a way of integrating them to the society.

In this study, it is mentioned and showcased that blockchain can disrupt key technologies and current system of decision making in businesses. However, it is important to show case that blockchain has significant use cases beyond crypto currencies and financial markets. With research on the field of education, the research explains that value proposition blockchain has to offer in education.

The study has made a clear projection on the design principles towards blockchain in certification management. This would certainly help developers of the technology, a base to build on and ideally improve on it when the application is used by the society. Regulatory bodies can use this study to understand the values that blockchain as to offer and create regulatory policies that are aimed at decentralized technologies such as blockchain. The network of important values serves as a foundation to understand supporting and conflicting relations of these values that are of primary importance to educational certifications. This research has shown ethical values with respect to blockchain and certification management in the design of the technology as well as in their process of deployment. With the social proposition blockchain has to offer, benefits such as removal of key ledgers from the control of single authorities can bring out changes to the current status quo of educational administration.

Limitations and further research

The research focuses on three main values of privacy, transparency and trust. Other values such as accountability, autonomy can also impact the design values and needs to be taken in consideration while designing such systems. Also, the number of respondents interviewed in this research is not substantial enough. More stakeholders from different domains in educational administration can result in a better value centric blockchain application in education. Certification management is the need of the hour and if immediate solutions cannot be approved by blockchain then other solutions have to be studied upon. Legal regulations are discussed on a lighter vein in this thesis. Studying the fit of blockchain with these centralized regulations can unlock further objectives to policy makers. A few approaches to satisfy the design principles in this thesis are analysed, but for example proof of work as a mechanism to build trust should also be studied upon. Research on the reduction of blockchain size could boost scalability of such an application and is an important area of blockchain that needs further research. Insights on trade-offs between more values can lead an increased complexity and a better design, current research focusses on trade-offs but a higher insights would lead to a better performance of the system.

Fit between CoSEM and this research

The CoSEM programme deals with designing in multi actor complexities with a complex socio-technical environment. The technology studied in this research deals with multi actor and multi system complexities. The focus on value sensitive design is used to understand these complexities in detail and appreciate a design implementation of the blockchain technology in the context of certification management. Various perspectives and theories used in this research such as graph theory, system architecture, ethics, designing objectives are the forefront of this CoSEM program. The research deals with creativity, theoretical understanding, recognizing stakeholder perspectives and a system perspective to understand technology and interactions. These courses and techniques form the basis of the CoSEM program.

8- Bibliography

- [1] Trustchain. (n.d.). Retrieved October 16, 2019, from TU Delft website: <https://www.tudelft.nl/en/technology-transfer/development-innovation/research-exhibition-projects/trustchain/>
- [2] Han, M.; Li, Z.; He, J.S.; Wu, D.; Xie, Y.; Baba, A. A Novel Blockchain-based Education Records Verification Solution. In Proceedings of the 19th Annual SIG Conference on Information Technology Education, Fort Lauderdale, FL, USA, 3–6 October 2018; pp. 178–183.
- [3] Grech, A. and Camilleri, A. F. (2017) Blockchain in Education. Inamorato dos Santos, A. (ed.) EUR 28778 EN; doi:10.2760/60649
- [4] I. G. Publishing, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. IT Governance Limited, 2016.
- [5] “Watson Personality Insights,” 28-Nov-2016. [Online]. Available: <https://www.ibm.com/watson/services/personality-insights/>. [Accessed: 20-Sep-2018].
- [6] S. Ray, “How Blockchains Will Enable Privacy,” *Towards Data Science*, 03-Mar-2018. [Online]. Available: <https://towardsdatascience.com/how-blockchains-will-enable-privacy-1522a846bf65>. [Accessed: 01-Sept-2018]. -18
- [7] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,”
- [8] “Blockchain, IP and the fashion industry | Managing Intellectual Property.” [Online]. Available: <http://www.managingip.com/Article/3667444/Blockchain-IP-and-the-fashion-industry.html>.
- [9] “Unlocking the Value of Personal Data: From Collection to Usage,” *World Economic Forum*. [Online]. Available: <https://www.weforum.org/reports/unlocking-value-personal-data-collection-usage>.
- [10] S. Baller, S. Dutta, and B. Lanvin, “The global information technology report 2016,” in *World Economic Forum, Geneva*, 2016, pp. 1–307.
- [11] T. McConaghy, “How Blockchains could transform Artificial Intelligence,” *Dataconomy*.
- [12] T. Lewin, “Economic Reasons Found for College Dropouts,” *The New York Times*, 09-Dec-2009.
- [13] Tarragó F.R., Wilson A.E. (2010) Educational Management Challenges for the 21st Century. In: Reynolds N., Turcsányi-Szabó M. (eds) Key Competencies in the Knowledge Society. KCKS 2010. IFIP Advances in Information and Communication Technology, vol 324. Springer, Berlin, Heidelberg.
- [14] A. Forrest, “Refugees will have the right to work - why not employ them?” *The Guardian*, 11-Sep-2015.
- [15] “3 Biggest Education Innovation Questions For 2018.” [Online]. Available: <https://www.forbes.com/sites/schoolboard/2018/01/08/3-biggest-education-innovation-questions-for-2018/#7efb55b44b13>. [Accessed: 01-Oct-2018].
- [16] M. Sharples and J. Domingue, “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward,” in *Adaptive and Adaptable Learning*, 2016, pp. 490–496.
- [17] 2019 EdTech Funding Breakthrough—Great Investment or Not? (2019, June 25). Retrieved December 3, 2019, from Nix United – Custom Software Development Company website: <https://nix-united.com/blog/2019-edtech-funding-breakthrough-great-investment-or-not/>

- [18] S. Hanafin, "Review of literature on the Delphi Technique," *Dublin Natl. Child. Off.*, 2004.
- [19] J. Yli-Huomo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology? A Systematic Review," *PloS One*, vol. 11, no. 10, p. e0163477, 2016.
- [20] B. VAN ALSENOY, "REGULATING DATA PROTECTION," 2016.
- [21] Farah, J.C.; Vozniuk, A.; Rodríguez-Triana, M.J.; Gillet, D. A Blueprint for a Blockchain-Based Architecture to Power a Distributed Network of Tamper-Evident Learning Trace Repositories. In Proceedings of the 2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT), Mumbai, India, 9–13 July 2018; pp. 218–222.
- [22] McDonald, A.M. and L.F. Cranor.(2008) "The cost of reading privacy policies." *ISJLP* 4 : 543
- [23] P. De Hert, "Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer," *Eur. Data Prot. Law Rev.*, vol. 3, no. 1, pp. 20–35, 2017.
- [24] "The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services," *World Economic Forum*, 2016. [Online]. Available: <https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services>.
- [25] "The Single Market Strategy - Growth - European Commission," *Growth*. [Online]. Available: [/growth/single-market/strategy_en](http://growth/single-market/strategy_en).
- [26] H. Gjermundrød, I. Dionysiou, and K. Costa, "privacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls," in *International Conference on Web Engineering*, 2016, pp. 3–15.
- [27] "The Missing Links In The Chains? Mutual Distributed Ledger (aka blockchain) Standards." Long Finance, 2016.
- [28] E. Sixt, *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie*. Springer-Verlag, 2016.
- [29] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System Bitcoin: A Peer-to-Peer Electronic Cash System."
- [30] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a Decentralized Currency?," *IEEE Secur. Priv.*, vol. 12, no. 3, pp. 54–60, May 2014.
- [31] N. Koblitz and A. J. Menezes, "Cryptocash, cryptocurrencies, and cryptocontracts," *Des. Codes Cryptogr.*, vol. 78, no. 1, pp. 87–102, Jan. 2016.
- [32] K. Chaudhary, A. Fehnker, J. van de Pol, and M. Stoelinga, "Modeling and Verification of the Bitcoin Protocol," *Electron. Proc. Theor. Comput. Sci.*, vol. 196, pp. 46–60, Nov. 2015.
- [33] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Security and Privacy (SP), 2016 IEEE Symposium on*, 2016, pp. 839–858.
- [34] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Proj. Yellow Pap.*, vol. 151, 2014.
- [35] T. McConaghy *et al.*, "BigchainDB: A Scalable Blockchain Database," 2016.
- [36] J. de Kruijff and H. Weigand, "Towards a Blockchain Ontology," 2016.

- [37] M. Simantov, *p2p-index: A collection of peer-to-peer decentralized projects*. 2017.
- [38] S. Díaz-Santiago, L. M. Rodriguez-Henriquez, and D. Chakraborty (2014). "A cryptographic study of tokenization systems," *11th International Conference on Security and Cryptography (SECRYPT)*, 2014, pp. 1–6.
- [39] "Finra: Distributed Ledger Technology: Implications of Blockchain for the Securities Industry." 2017.
- [40] "Bitcoin and Cryptocurrency Technologies," *Goodreads*. [Online]. Available: <https://www.goodreads.com/book/show/29452533-bitcoin-and-cryptocurrency-technologies>.
- [41] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 2084–2123, 2016.
- [42] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 2, pp. 397–413, Mar. 2016.
- [43] Villard, S. J., Flanagan, M. B., Albanese, G. M., & Stoffregen, T. A. (2008). Postural Instability and Motion Sickness in a Virtual Moving Room. *Human Factors*, 50(2), 332–345. <https://doi.org/10.1518/001872008X250728>
- [44] Friedman, B., Kahn, P. H., & Borning, A. (2008). *Value Sensitive Design and Information Systems*. 27.
- [45] van de Poel, I. (2013). Translating Values into Design Requirements. In D. P. Michelfelder, N. McCarthy, & D. E. Goldberg (Eds.), *Philosophy and Engineering: Reflections on Practice, Principles and Process* (Vol. 15, pp. 253–266). Springer Netherlands. https://doi.org/10.1007/978-94-007-7762-0_20
- [46] Tu, Y.-C. (2014). *Transparency in Software Engineering* [Thesis, ResearchSpace@Auckland]. <https://researchspace.auckland.ac.nz/handle/2292/22092>
- [47] Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, 11(2), 105–112. <https://doi.org/10.1007/s10676-009-9187-9>
- [48] Chapman, Gretchen B., and Eric J. Johnson. (1999). "Anchoring, Activation, and the Construction of Values," *Organizational Behavior & Human Decision Processes*, 79(2), 115–153
- [49] Tavani, H. T. (2007). Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. *Metaphilosophy*, 38(1), 1–22. <https://doi.org/10.1111/j.1467-9973.2006.00474.x>
- [50] Greengart, A., & Analysis, devices analyst at C. (n.d.). *In Samsung's Messy Phone Recall, Lack Of Transparency Takes Center Stage*. NPR.Org. Retrieved July 10, 2020, from <https://www.npr.org/sections/alltechconsidered/2016/10/18/497949435/in-samsung-s-messy-phone-recall-lack-of-transparency-takes-center-stage>
- [51] Curran, D. (2018, March 30). Are you ready? This is all the data Facebook and Google have on you | Dylan Curran. *The Guardian*. <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>
- [52] "Samsonite CEO Ramesh Tainwala Is Out After Being Accused of Padding His Resume," *Fortune*. [Online]. Available: <http://fortune.com/2018/06/01/samsonite-ceo-ramesh-tainwala-resigns/>. [Accessed: 02-Nov-2018].
- [53] "Credentialing, certification, and competence: Issues for new and seasoned nurse practitioners - Smolenski - 2005 - Journal of the American Academy of Nurse Practitioners - Wiley Online Library." [Online]. Available: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1041-2972.2005.00033.x>. [Accessed: 10-Nov-2018].

- [54] M. M. Lab, "What we learned from designing an academic certificates system on the blockchain," *Medium*, 02-Jun-2016.
- [55] Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction*, 31(3), 498–501. <https://doi.org/10.1093/humrep/dev334>
- [56] Using blockchain to improve data management in the public sector | McKinsey. (n.d.). Retrieved July 18, 2020 from <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector>
- [57] *What Is the Use of Big Data in Education?* (2019, May 15). Colocation America. <https://www.colocationamerica.com/blog/big-data-and-education>
- [58] Genus, A., & Stirling, A. (2018). Collingridge and the dilemma of control: Towards responsible and accountable innovation. *Research Policy*, 47(1), 61–69. <https://doi.org/10.1016/j.respol.2017.09.012>
- [59] Czeskis, A., Dermendjieva, I., Yapit, H., Borning, A., Friedman, B., Gill, B., & Kohno, T. (2010). Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety. *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 1–15. <https://doi.org/10.1145/1837110.1837130>
- [60] The Global Agenda Council on the Future of Software and Society, . "Deep Shift: Technology Tipping Points and Societal Impact" *World Economic Forum* (September 2015)
- [61] Meijer, D. (2017). *Consequences of the implementation of blockchain technology* (SEPM Master Thesis), Delft University of Technology, Delft.
- [62] *Are schools doing enough to protect student data?* (2019, September 3). Study International. <https://www.studyinternational.com/news/are-schools-doing-enough-to-protect-student-data/>
- [63] Hovell, Devika (2009) *The deliberative deficit: transparency, access to information and UN sanctions*. In: Farrall, Jeremy, (ed.) *Sanctions, Accountability and Governance in a Globalised World*. Connecting international law with public law. Cambridge University Press, Cambridge, UK, pp. 92-122. ISBN 9780521114929
- [64] Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *Proceedings on APWG eCrime Researchers Summit* (pp. 1-14).
- [65] Dasgupta, P. 1998 Trust as a commodity. In Gambetta, D. (ed.), *Trust: Making and Breaking Cooperative Relations*. Blackwell, pp. 49–72.
- [66] Liz, Crowcroft; et al. (2005). "A survey and comparison of peer-to-peer overlay network schemes" . *IEEE Communications Surveys & Tutorials*. 7 (2): 72–93 doi:10.1109/COMST.2005.1610546
- [67] Ramchurn, Sarvapali & Huynh, Trung Dong & Jennings, Nicholas. (2004). Trust in Multi-Agent Systems. *The Knowledge Engineering Review*. 19. 10.1017/S0269888904000116.
- [68] Fried, C. (1968). Privacy. *The Yale Law Journal*, 77(3), 475-493. doi:10.2307/794941
- [69] Byrne, M., Valentine, W., & Carter, S. (2004). The Value of Certification—A Research Journey. *AORN Journal*, 79(4), 825–835. [https://doi.org/10.1016/S0001-2092\(06\)60823-5](https://doi.org/10.1016/S0001-2092(06)60823-5)
- [70] Roeser, S. (2012). Emotional Engineers: Toward Morally Responsible Design. *Science and Engineering Ethics*, 18(1), 103-115. doi:10.1007/s11948-010-9236-0
- [71] Sekaran, U., & Bougie, R. (2016). *Research Methods for Business*. John Wiley & Sons Ltd.

- [72] Adams, W.C. (2015). Conducting Semi-Structured Interviews. In Handbook of Practical Program Evaluation (eds K.E. Newcomer, H.P. Hatry and J.S. Wholey). doi:[10.1002/9781119171386.ch19](https://doi.org/10.1002/9781119171386.ch19)
- [73] Alammery, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: A Systematic Review. *Applied Sciences*, 9(12), 2400. <https://doi.org/10.3390/app9122400>
- [74] Creswell, J. W. (2009) *Research design : qualitative, quantitative, and mixed methods approaches* (3rd ed.) London: Sage Publications
- [75] Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1), 1. <https://doi.org/10.1186/s40561-017-0050-X>
- [76] Software Engineering Group: Guidelines for Performing Systematic Literature Reviews in Software Engineering (2007)
- [77] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in *IEEE Access*, vol. 6, pp. 5112-5127, 2018, doi: 10.1109/ACCESS.2018.2789929
- [78] McLeod, C. (2020). Trust. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2020). Metaphysics Research Lab, Stanford University. <https://plato.stanford.edu/archives/fall2020/entriesrust/>
- [79] Hölbl, M.; Kamisalić, A.; Turkanović, M.; Kompara, M.; Podgorelec, B.; Heričko (2018). M. EduCTX: An Ecosystem for Managing Digital Micro-Credentials. In Proceedings of the 2018 28th EAEEIE Annual Conference (EAEEIE), Hafnarfjörður, Iceland, 26–28 September 2018; pp. 1–9.
- [80] Gilda, S.; Mehrotra, M. Blockchain for Student Data Privacy and Consent (2018). International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 4–6 January 2018; pp. 1–5.
- [81] Sychoy, S.; Chirtsov (2018). A. Towards Developing the Unified Bank of Learning Objects for Electronic Educational Environment and Its Protection. Workshop on PhD Software Engineering Education: Challenges, Trends, and Programs, St. Petersburg, Russia; pp. 1–6.
- [82] Brief History of the Internet. (2020). *Internet Society*. Retrieved September 2, 2020, from <https://www.internetsociety.org/internet/history-internet/brief-history-internet/>
- [83] Dym, C. L., Little, P., & Orwin, E. J. (2014). *Engineering design: A project-based introduction*.
- [84] ISO/IEC. 9241-14 (1998) . Ergonomic requirements for office work with visual display terminals (VDT)s
- [85] Hoffman, D., Grivel, E., & Battle, L. (2005). Designing software architectures to facilitate accessible web applications. *IBM Systems Journal*, 44(3), 467e483.
- [86] Vincent, J. (2019, July 4). *Bitcoin consumes more energy than Switzerland, according to new estimate*. The Verge. <https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison>
- [87] Creswell, J. W. (2009) *Research design : qualitative, quantitative, and mixed methods approaches* (3rd ed.) London: Sage Publications
- [88] Foundation, E. (2014). *Slasher Ghost, and Other Developments in Proof of Stake*. Retrieved September 10, 2020, from <https://blog.ethereum.org/2014/10/03/slasher-ghost-developments-proof-stake/>

[89] David, E., & Jon, K. (2010). *Networks, Crowds, and Markets: Reasoning About a Highly Connected World*. Cambridge University Press.

Appendix A: Questionnaire empirical research

Personal

1. What is your role in the organization?
2. Do you have experience with large IT innovation projects?
3. Who would you consider as an intermediary or brokers in this field?
4. Are you familiar with the concept of blockchain? If yes, how did you get to know about this?

Blockchain in Education

1. An obvious educational use is to store records of achievement and credit, such as degree certificates. The certificate data would be added to the blockchain by the awarding institution which the student can access, share with employers, or link from an online CV. How do you view blockchain as a distributed digital record?
2. What is your perception of digital certificates for education?
3. Are there any current interests within your organization to implement such initiatives?
4. What do you think would be the major challenge in standardising to achieve a widespread adaptation of such a system?
5. With a blockchain application such as this you could share which details you want with which organization, but you can never delete information once it's on the chain. This is the philosophical problem with blockchain but how far do you think this will have an impact on implementation of such systems, also what do you think are other problems that would complicate the use of blockchain?
6. In the value sheet provided to you, could you mark the list of values that you think is important in certification management?
7. Other than challenges of standardisation what other challenges do you think impacts the use of blockchain in education?
8. What are your thoughts on the current process of certification management? What are the challenges according in it?
9. Does the current educational administration taken into account micro accreditation?
10. What are factors of trust that stakeholders look at? How do they resolve a conflict or communicate changes to the status quo of the application?

Impact on Technical Architecture

Since we are dealing with values of certification management, the questions are more focussed on the values, certification management and blockchain architecture. Based on the values you ranked in blockchain, technical implementation of these values in blockchain is presented to you.

1. What are the factors according to you would blockchain add in certification management?
2. In the area you specified, do you feel the consideration of these values to be relevant when developing blockchain technology? Elaborate shortly.
3. When developing blockchain in education, what factors contribute towards privacy, trust and transparency?
4. Now consider the development of blockchain technology dealing with personal data. How would you store this type of personal data on a public blockchain?
5. What should the design of the application look like, what are the different constraints and objectives that this application should have?
6. According to you, if the control of data is handed over to the user, who takes responsibility if there is a loss of data?
7. What is your perception of blockchain technology in this chosen area? Do you think it adds value or not?
8. From your own perspective and outside the scope of the chosen area. What relationship between blockchain and education would you wish for in the future?