Ossi Huttunen
Joel Leskinen
Anu Tamminen
Jesperi Vuorinen

BLOCKCHAIN IN PLATFORM OF TRUST

Group Assignment
TLO-35307 Emerging Technology Adoption and Use
April 2021

ABSTRACT

Anu Tamminen, Ossi Huttunen, Joel Leskinen & Jesperi Vuorinen:
Blockchain in Platform of Trust

Technology: Blockchain
Context: Data Product Trust
Lens: Upcoming, prescriptive

Data are employed in almost all the activities of organizations and formulate the basis of decision-making on operational and strategic levels. With the current competitive business environment, data are regarded as a critical asset and it is sold to business partners in the eco-system of the data-driven business models. Blockchain technology has given rise to a new platform which enables accountability and security without a centralized regulator. With its traits, blockchain can be used to guarantee trust in data and companies can focus on their data-driven business model without being overly worried about properly securing.

This research aims at prescribing how blockchain technology can be utilized in data product trust context in upcoming. This research is conducted in collaboration with Platform of Trust, Finnish SME founded in 2019. Platform of Trust's business is based on high-quality productization of data and the company is developing an index for data trust that is Data Trust Index (DTI). DTI includes seven different data product trust factors which can determine the DTI value for each data product. The trust factors of a data products are identity, reliability, rights, flow quality, content quality, compatibility, and security.

Blockchain's opportunities for trust are transparency, decentralization, immutability, anonymity and efficiency which support the best possible value of the factors. Some of the challenges of blockchain technology also affects to data trust factors. Three blockchain implementation options are also covered in the study, which are Blockchain as a Service (BaaS), Infrastructure as a Service (IaaS) and monetizing access to a platform. BaaS model was chosen as the approach for implementation. In BaaS, Platform of Trust develops and provides a blockchain application to customer enterprise based on customers' needs. Ultimately, the concept is Data Trust Ledger (DTL) where data trust factors and DTI are combined with BaaS model by Platform of Trust. DTL's high-level architecture is supported by the BaaS model since Platform of Trust has the role of platform provider.

Keywords: blockchain, data product, trust, Data Trust Index, Platform of Trust

The originality of this thesis has been checked using the Turnitin Originality Check service.

TABLE OF CONTENTS

.

1. INTRODUCTION

As outlining the new digital reality for organizations, data is one of the main elements of the organizations in supporting various functions to reach organizational goals. Organizations use the data they collected to personalize services, optimize decision-making and forecast trends and more. (DalleMule & Davenport, 2017) With current competitive business environment, companies that adopt a data-driven business model to transform their business, e.g., providing additional data-based services, can become sustainable (Rath, Codenie & Hristoskova, 2020). Businesses are gaining huge amounts of data about consumer behavior. Personal data will be a growing competitive advantage – but the same time gaining the trust of the individual will be the key. (Morey, Forbath & Schoop, 2015) In recent years, blockchain technology has given rise to a new platform which enables accountability and security without a centralized regulator (Zyskind et al. 2015). Blockchain creates a new basis of trust where users are aware of the data collected about them and companies can focus on their data-driven business model without being overly worried about properly securing.

Redman (2015) highlights that in order to gain consumers' trust, transparent data practices are required. Data are regarded as a critical asset and it is sold to business partners in the eco-system of the data-driven business models. A data provider company must convince that the collected data are real, accurate and not manipulated. Hence, building trust in data and ensuring transparency are the significant ways to convince the eco-system partners. (Rath, Codenie & Hristoskova, 2020) New data combined with existing data and analytical features creates a concept called data product. More specifically, data product is an output of using analytical features and data assets providing potentially game-changing insights to an organization. (Davenport & Kudyba 2016)

How to indicate whether the data product, new information, can be trusted? Platform of Trust is Finnish SME founded in 2019, whose business is based on high-quality productization of data. Platform of Trust is developing an index for data trust that is Data Trust Index (DTI). DTI includes seven different data product trust factors which can determine the DTI value for each data product. DTI's aim is to provide a clear number on data trust in order to inform the user of the data product about the value of the factors. The trust factors of a data products are identity, reliability, rights, flow quality, content quality, compatibility, and security. More on, data trust and the factors can be categorized as reputation- and policy-based groups. (Rath, Codenie & Hristoskova, 2020).

Blockchain has demonstrated in the financial space how it can serve functions requiring in trusted computing and auditability. Zyskind et al. (2015) have created a decentralized blockchain platform which enables users to own and control their data without compromising security or limiting companies' ability to offer personalized services. Blockchain is a certain type of database which could be regarded as a public ledger and all committed transactions are stored in a list of blocks. The blocks are chained together, and the chain increases as new blocks are appended to it continuously. The blockchain technology generally has typical features of decentralization, persistency, anonymity and auditability. (Zheng *et al.*, 2017) Blockchain is a natural remedy for a platform which can achieve data transparency, design an adequate transaction order under the condition of trust, and provide high-level data security protection (Wang & Guo 2020). With these traits, blockchain can be used to guarantee data trust factors.

This group assignment has done for Tampere University's Emerging Technology Adoption and Use course in spring 2021. The purpose of this assignment is to study blockchain technology in data product trust context with prescribe research lens. We follow the ETAU framework guided by the course. We instruct how to use blockchain in data product trust in the upcoming. Our group has previously collaborated with Platform of Trust from which the assignment was developed. We have studied the trust factors and parameters in DTI before, and now we add the prescriptions how to manage and measure data trust with the blockchain technology.

2. RESEARCH METHODOLOGY AND LENS

For this work, an upcoming, prescriptive research lens was used. The lens was chosen using the ETAU-framework (Emerging Technology Adoption and Use -framework) (Pirkkalainen, 2021), in which the choice of lens is primarily based on the desired objective and outcomes of the research. This document is that outcome, a prescriptive work, that will cover the *why* and *in which way* blockchain can be utilized in the context of choice, namely data products and trust, and in particular the Data Trust Index developed by Platform of Trust.

The upside of the chosen research lens is the ability to produce practical outcomes that are ready to be utilized (Pirkkalainen, 2021). Additionally, the upcoming perspective provides additional value, by focusing on the future possibilities & capabilities and thus, provides insights on sources of future competitive advantage.

The downside of the lens is the deep understanding of both the technology (blockchain) and the business context (DTI, Platform of Trust) needed to undertake this form of research. However, this downside is partially mitigated by the previous experience of the business context, possessed by majority of the research team; And while the utilization of this previously acquired knowledge requires care to be taken in averting possible cognitive biases, this does not pose a significant obstacle, due to the previously acquired knowledge being acquired relatively recently, within the last six months, and having been proven accurate with the success of previous projects (Vuorinen et al., 2020; Vuorinen, 2021).

Because of these circumstances, the focus in this work will be on understanding the technology aspects, such as the utility and features of blockchain, as well as the existing and possible technical solutions. This will be achieved with a mono-method, abductive research approach (Saunders et al., 2019), centered around reviewing existing literature of blockchain technology and its applications.

3. DATA PRODUCT & DATA TRUST

This chapter will introduce the concept of data product and trust in data. Data product development create a market for new technology and value creation is continuous. Trust is divided in policy-based and reputation-based groups. Data Trust Index (DTI) developed by Platform of Trust is discussed and the data trust factors in DTI are explained. It is elaborated how every data trust factor creates value for DTI.

3.1 Data Products

The current information revolution changes society, academia and business. Driven by networked communication systems and Internet, the present revolution has created a surplus of a valuable new material – data – and has converted us all into both data consumers and producers. More and more, data impacts every aspect of human life, from the food eaten to social interactions. (Morey, Forbath & Schoop, 2015; Bengfort & Kim 2016) Products and services which are highly personalized and led by data-driven design are developed to create a market for new technology – data product.

Data product is an application of using analytical features and data assets providing potentially game-changing insights to an organization. The objective of data product is to help organizations improve their processes, services, customer experience and so on. It creates value by processing new and existing data collected from different sources. (Davenport & Kudyba 2016) Bengfort and Kim (2016) emphasize that data product is not just an application with data; it is a data application acquiring its value from data itself and generates more data consequently. Hence, a data product is an economic engine since it derives value from data, cultivates more data, and more value perpetually. It might lead to the creation of other data products. (Bengfort & Kim, 2016) Eventually, more data products convey more data, which leads even more data products, and so forth.

Data product development does not differ much from ordinary product development, including user groups identification, actual product development, impact assessment and iteration. However, adding the data component to product brings new challenges for companies with the involvement of various stakeholders. (Sands Glassberg, 2018) Data products are designed with data science workflows through the application of models to a domain-specific dataset (Bengfort & Kim, 2016). It can receive data e.g., from an Internet of Things (IoT) device of one stakeholder, which in turn collect data from another stakeholder. When collaborating, the stakeholders have different roles in managing data, and thus data trust plays a key role in data product operations.

3.2 Data Trust

Data trust is an approach to data management and decision-making in the same way that trust has been used earlier to manage and make decision about the asset management. Data trust is defined as trust in who manages, maintains and controls the usage and sharing of data – who has the access to the data and under what conditions. (Redman 2015) Thus, in data trust, one party empowers the other to make decisions about the data on their behalf, in which stakeholder benefit. Data trust cover factors to measure the trust of the data product.

3.3 Policy- and reputation-based groups

When trust is viewed in the way described previously, it can be thought of as the forfeiture of control (Gambetta 1988; Vuorinen et al., 2020; Vuorinen, 2021). In everyday life, we can think of this as the trust we have that a friend will return something we borrow to them or we trust a business partner to keep their word on small, routine scale tasks without proof of an agreement, or we can trust that some technology that we utilize daily still works as it has done previously. In all these cases, control of future events is given up in order to gain both convenience and opportunities. Because of this loss of control is in itself a clearly negative thing in business context, it must justify this loss in some way (Gambetta 1988; Vuorinen et al., 2020).

The sources of this justification can be roughly divided into two categories: those based on policy and those based on reputation (Gambetta 1988; Vuorinen et al., 2020; Vuorinen, 2021). The latter of these, reputation-based trust, is the more convenient, everyday form of trust seen in the examples above. It allows for the outsourcing of the verification of the trustworthiness by connecting it to the trust given to the identities behind the object of trust, such as someone's character, with that someone often being synonymous with that to which give the control to.

While in an ideal world, this hard work of verification and justification could always be outsourced, sometimes the risks of associated with this outsourcing cannot be justified. This is especially true in contexts, where there is a lack of reliable, and importantly impartial identities to connect trust to in order to justify it. Therefore, it is important counterbalance reputation-based trust with the independently verifiable policy-based trust (Vuorinen, 2021). Policy-based trust depends on the exchange of hard evidence e.g., contracts and proxies, and therefore does not require for other parties or identities in order for establishment of trust (Gambetta, 1988; Vuorinen et al., 2020). This balancing act between convenience and speed of reputation, and verifiability of policy is at a heart of many problems, both practical and theoretical, related to trust, and subsequently also related to data commodification and trading of data products.

3.4 The Trust Factors in DTI

To help with the need for convenience and speed verifiability in data products, we have previously been working on a tool to be used as a way of expressing the factors which contribute to the trustworthiness of data and data products. This **Data Trust Index** combines several indicators of seven policy- and reputation-based trust factors in an easy to understand, yet adaptable tool, which is meant to be used by both providers and consumers of data. These factors are: Identity, Reliability, Rights, Flow quality, Content Quality, Compatibility and Security. A summary of these factors can be seen in table 1.

Table 1: Data trust factors in the DTI

Data Trust Factor	Explanation	Value for DTI
Identity	Trust in the identities of the people in the data product	Data products become diversified, business thrives, and new identities are established
Reliability	Trust in organization’s reputation, brand, identity, ethical and legal functions	Data provider supplies legally and ethically reliable secure data.
Rights	Trust in data ownership and data ownership policies	Data ownership and access rights to the data content are permitted.
Flow quality	Trust in the continuity and speed of data flow	No errors are detected in the further processing of data.
Content quality	Trust in data’s ability to meet the data quality requirements	High quality data are often crucial to organization’s operations.
Compatibility	Trust in data is built to be interoperable according to the requirements	Data from multiple different sources are enabled to be combined.
Security	Trust in data source and the implementation of information security.	Security formulates the basis of the other trust factors.

Data identity views data as representative, providing empirical evidence which can detached from theoretical assumptions. On the other hand, data is used as evidence in which data identity is determined on the basis of queries and identity changes with the context. (Leonelli 2016) In the DTI context identity refers to the trust in the identities of the people in the data product, i.e., organizations. Thus, there is a mutual dependency; the higher organizational-level identity, the higher the DTI value. The value of identities is expected to be highly industry- and user-specific. The primary role for identities in the DTI is grown as data products become diversified, the organization takes its business further and new identities are established.

Data reliability covers the reputation of the data publisher. It can be observed through an organization's reputation, brand, and identity, as well as its ethical and legal functions. The evaluation of data reliability comes from the brand and reputation management. (Kuoppakangas et al. 2019) In the DTI, the reliability of the organization determines the data reliability value to a large extent. If the data provider's reliability is low, the data product's reliability cannot be estimated to be high. The value from reliability as a trust factor derives from confidence that reliable data provider supplies legally and ethically reliable secure data.

Data rights refer to trust in how the rights of data owner are treated and handled. Data ownership and data ownership policy are critical to data rights as trust factor. Data ownership includes the rights to use, store, share data and to restrict access to the data. (Thouvenin et al. 2017, p. 111) Whereas the allocation of data decision-making rights is involved in the data ownership policy. (Storey et al. 2010) The rights as parameter in the DTI give the user an idea of the data rights level in a data product. Data rights primarily create value by allowing data ownership, and thus access rights to the content. Therefore, data access rights should be built by sharing data ownership clearly, in which way trust in data can be assessed from a data rights perspective.

Data flow quality refers to sources that produces data e.g., different kind of IoT sensors which produces unlimited and continuous data. Data flows generally moves very rapidly and can consist of structured or unstructured raw data. (Geisler et al. 2016). In the context of DTI, data flow quality means that the data will flow reliably. High-quality data flows are essential part of the data quality as unreliable data flow can cause errors in the further processing of data. Data flow quality generate value to an organization, as high-quality data flows can be used to ensure the continuity and speed of data flow.

Data content quality is often defined as 'fitness for use' and its ability to satisfy its usage requirements (Khatri & Brown 2010). In the DTI, data content quality refers to data's ability to meet the data quality requirements. Data quality can be measured in many different ways. Platform of Trust has selected the following data characteristics as elements of the DTI: timeliness, margin of error, accuracy and integrity. Data content quality influences greatly organization's operations. Poor quality data have significantly negative effects on the efficiency of organization, while high quality data are often crucial to company's success. (Haug et al. 2011)

Data compatibility refers to the ability to combine data with another data. It includes both data integration and exchange. (Pagano 2013) In the DTI context, compatibility means that the data is built to be interoperable according to some requirements. Data compatibility creates value primarily by enabling data from multiple different sources to be combined. This makes it possible to generate more multidimensional data and information. Compatibility as a parameter in the DTI gives the user an idea of data compatibility level in a data product.

Lastly, **data security** indicates how trustworthy the data source is. In the DTI, data security is essentially related to information security and when the data source is secure, it provides good conditions for the implementation of information security. (von Solms & van Niekerk 2013). It is important that data source is reliable because unreliable data source might have direct negative impact for other data trust factors and for overall DTI value. Data security is considered as basis for the other trust factors in the DTI.

4. BLOCKCHAIN TECHNOLOGY

This chapter will discuss the theoretical benefits and downfalls, or in other words the *ifs* of blockchain technology for the chosen business context; *If* this technology is chosen, what opportunities does it provide? What *if* there are challenges with the technology or *if* we lack existing know how on this matter, is it possible to still aspire for such goals?

4.1 Basics of blockchain technology

Blockchain is a decentralized database of records, or public ledger of all transactions, or digital events that have been executed and shared among participating parties. Each transaction in blockchain is verified by consensus of the participant of the system and when the information is entered to chain it can never erase from there. (Crosby et al. 2016) The blocks of blockchain can contain any kind of data, for example text, files, media, or code. Blockchain considered a way of share, produce, or maintain decentralized databases with different parties without knowing each other or even trust each other's. The hypothesis in blockchain is that it establishes as system of creating digital consensus in the online world (Crosby et al. 2016; Li & Wang 2017). Blockchain systems can be divided to three main categories which are: public blockchain, private blockchain, and consortium blockchain (Zheng et al. 2018). Each category has their own positive and negative side. For example, public blockchain is open to all data miners but its efficiency is lower than private blockchain which is open only for one organization (Zheng et al. 2018).

The data of blockchain is entire and reliable due to hash function. The hash function is made by the data of block and former block's hash. So very block has a pointer to its parent, which made blocks linked and creating the chain of blocks called blockchain (Atlam et al. 2018). Through the hash functions is possible to confirm the validity of data. The data of blockchain is reliable simplified, because of the hash function every party participated at the chain can identify the changes of data in blockchain immediately. In next picture (Figure 1.) is presented simplified principle of blockchain.

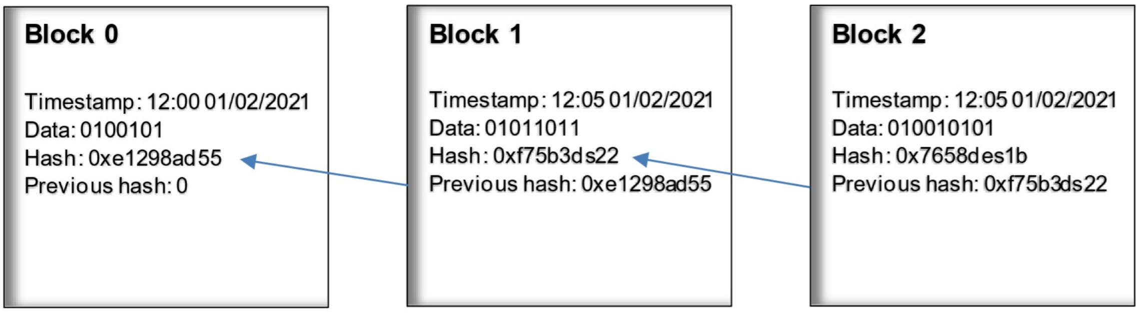
Block 0
Timestamp: 12:00 01/02/2021
Data: 0100101
Hash: 0xe1298ad55
Previous hash: 0
Block 1
Timestamp: 12:05 01/02/2021
Data: 01011011
Hash: 0xf75b3ds22
Previous hash: 0xe1298ad55
Block 2
Timestamp: 12:05 01/02/2021
Data: 010010101
Hash: 0x7658des1b
Previous hash: 0xf75b3ds22

Figure 1: Simplified blockchain

With blockchain technology is possible to evade use of third-party database in maintain or share of data, because the blockchain works as distributed database in network of computers with included parties without administrator (Crosby et al. 2016). Distributed database made possible to avoid excessive costs and dependency on third parties to maintain database. The distributed database functioning based on validation of data on peer-to-peer (P2P) network. Transaction validation is performed by running predefined checks on structure and the actions of the transaction (Atlam. et al. 2018). When the majority of network has validated the transaction, the transactions become new block of blockchain.

One of general solution by blockchain is smart contracts. Simplified smart contract is a script that is anchored on a blockchain or some else distributed infrastructure. (Ante, 2021) As soon as the conditions of smart contract are fulfilled the blockchain will trigger its transaction and validate through its network. Conditions of smart contract are transparently stored on the blockchain intended by all stakeholders, which reduce trust issues between those parties. (Ante, 2021) That is only a one example how blockchain can be used to increase trust between parties and in next section we look on those opportunities in trust.

4.2 Contemporary uses of blockchain

Most of us signify blockchain as a cryptocurrency, like bitcoin and that is probably the first widely known blockchain based service. Other widespread solution for blockchain is supply chain management systems. There are lot of operators on supply chain and as much as possible problems in data transfer to another operator, and that is planned to solve with blockchain solution. Also, there are many other industries, which would benefit blockchain solutions like real estate industry, construction industry and media. (Kilroy 2019)

The thing in common in those industries, which desire to use blockchain is that the trust issues or data missing between stakeholders. It is easy to make conclusion that there are room for blockchain solutions in data platforms, especially in industries where you must share trusted data between stakeholders. Also, the cloud service enterprises have recognized that possibility, and for example the world leading cloud service companies Amazon, Microsoft, IBM Google have their blockchain solution for data sharing (Lu et Al. 2019).

4.3 Opportunities of blockchain for trust

Blockchain can be divided to six different opportunities which create value for trust. These six factors are transparency, decentralization, efficiency, immutability and anonymity.

Transparency of blockchain comes from the user's ability to view every transaction and block of blockchain because every user has their own ledger. However, users are not able to modify these transactions without unique key to transaction. (Atlam et al. 2018) Blockchain technology improves the traceability and transparency of data (Zheng et al. 2018). Transparency features add value for trust.

Decentralization means that most of the users of blockchain must verify transactions of blockchain for transaction to be approved into the distributed ledger. Also no one can make the approval of transaction by themselves. (Atlam et al. 2018) Traditional centralized system would need central trusted agency like central bank for each transaction verification (Zheng et al. 2018). These both features create trust for data. However, there are differences between different blockchain system types. Public blockchain is fully decentralised, consortium blockchain is only partially centralised, and private blockchain is centralised to certain organization (Zheng et al. 2018)

Immutability is one of the features of blockchain. Immutability comes from the immutable distributed ledger of blockchain which registers each transaction and change of ledger. (Atlam et al. 2018) Every change must be approved in the way that is described in the decentralization section. Immutability adds increased security and privacy (Atlam et al. 2018). This increased security will add value for trust.

Blockchain keeps the buyer and the seller **anonymous** through the whole process of transaction by using unique anonymous addresses (Atlman et al. 2018). This means that the privacy of the buyer and the seller is protected which will give value for trust.

Blockchain's **efficiency** comes from the distributed transaction feature. This feature makes transaction faster because each transaction is distributed to different users across the blockchain network. (Atlam et al. 2018) There are some differences between different types of blockchain systems. The most efficient blockchain systems are private and consortium blockchains because they usually have less validators and they are not as strict as public blockchain in network safety (Zheng et al. 2018).

4.4 Challenges with blockchain

Blockchain is not a perfect technology, and it has multiple major challenges. (Atlam et al. 2018) recognizes challenges such as the need of processing power and time, possible future legal problems with blockchain, and the incompetence with blockchain. Achieving encryption in blockchain needs a lot of processing power and therefore time. Possible legal problems in the future are linked to the lack of laws and other legal aspects which might cause problems. (Atlam et al. 2018) It might be a major problem if the regulation changes radically in the future. Blockchain is relatively new technology and there is still a lack of expertise about blockchain and not too many people have the needed skills and knowledge of blockchain (Atlam et al. 2018). Blockchain is a new technology with limited tooling and documentation, so the developers need a lot of training and that would be time consuming (Lu et al. 2019). This means that it might be a big problem especially in context of data trust because it requires knowledge and skills in both data trust and blockchain.

Another challenge is scalability. Scalability issues are is caused by the increasing amount of transaction that leads to heavy blockchain meaning that it requires a lot of storage. This is due poor scalability of blockchain technology. (Zheng et al. 2018; Atlam et al. 2018) These problems with scalability might lead to centralization (Atlam et al. 2018). These scalability issues could be removed by optimizing storage of blockchain and by better designing of blockchain (Zheng et al. 2018). Blockchain is by design immutable data store, so updating of deployed can be hard (Lu et al. 2019). This makes it difficult to made bug fixes or changes on service by releasing new version of solution or smart contract. Also, this make a huge threshold on serve in blockchain when you have to have almost perfect service before release, because updates after release would be very hard and expensive.

5. HOW TO IMPLEMENT BLOCKCHAIN

With the theoretical challenges and opportunities of blockchain technology providing answers to the “if” of blockchain based solution implementation, it is important to not forget their practical counterparts in the business context when deciding the “when” of this implementation. For DTI and Platform of Trust, the entire business concept revolves around value creation from through practical connection, harmonization, and utilization of industrial data, and as such these practical concerns will prove imperative in deciding when the right time to implement a blockchain based solution arrives.

5.1 Blockchain implementation options for data products

Three blockchain implementations for data products are distinguished: Blockchain as a Service (BaaS), Infrastructure as a Service (IaaS) and monetizing access to a platform. All the implementation options are elaborated in this chapter 5.1. Further, we will discuss pros and cons of every blockchain implementation options.

5.1.1 Blockchain as a Service to data producers

The first option is for implementation is that the Platform of Trust could offer blockchain as a product or more specifically as a service (Blockchain as a service, BaaS). BaaS can be created in many different service business models (Singh 2018). One common approach to create BaaS is application-oriented approach which is resembles Software as a Service (SaaS). This approach means that the BaaS provider develops and deliver a customized blockchain application to client enterprise based on clients’ needs. (Singh 2018) In our case application provider would be Platform of Trust. This blockchain application could be for example a blockchain based DTI application.

Another approach to create BaaS is much like Platform as a Service (PaaS), where client enterprise selects which components of blockchain infrastructure they need and then customize, integrate, and use these components according to their needs. This means that the client enterprise is able to customize technical specifics of blockchain like ledger or access details. (Singh 2018)

Application-oriented approach to BaaS would be good for more general BaaS business model which would have multiple client enterprises that wouldn’t need much customization. On the other hand, the PaaS like approach BaaS would be better for more client enterprises which would need more control over blockchain application and its technical specifics. The downside of either BaaS option is that they need a lot of knowledge in data productization (Vuorinen et al. 2020). Other downside is that it needs good knowledge and skill in blockchain technology.

5.1.2 Blockchain as a feature of a data product marketplace and platform

The second option is to implement blockchain as part of the Platform of Trust's data product. The data trust platform is a blockchain-based solution able to ensure data trust. The architecture of blockchain-based platform would consist of three main parts: data collection, data procession and data storage and access.

Data can be derived from e.g., device acquisition, transaction processing and personal information input. In the blockchain, data is summarized, transactions are extracted, and information is recorded. Various industry data are integrated and classified by the rules. After processing, the data can generate industry value. Acquired industry information are stored through the blockchain API interface. After verifying the identity and permissions, a visitor access to the platform and can send a data request and find the data location in the blockchain. The timestamp of the tag verifies authenticity of the original data. (Wang & Guo 2020).

Blockchain can be also approached as a traditional Infrastructure as a Service (IaaS) offering. Then, Platform of Trust could rent out a specific blockchain-tailored infrastructure such as nodes and devices. IaaS can be used to run particular nodes or even an entire blockchain network, cloud storage services to host ledgers and identity management services to permit access control. (Singh 2018) Additionally, this solution could provide a level of centralization for the solution, that could overcome one of the major disadvantages of blockchain by increasing transaction speeds.

If implementing blockchain as part the Platform of Trust's data product, more general cloud services as blockchain ledger infrastructure can be optional. The pure blockchain-based platform can help to achieve high-level DTI values, even if the system is planned to operate in an untrusted ecosystem.

5.1.3 Dataproducts as distributed blockchain solutions

The third option is to utilize blockchain as the basis of the data product in its common form, as a distributed ledger, while monetizing the access to the data product (Schmarzo, 2021). This would keep the essence of both blockchain and the data product intact, while being possible with existing technology.

Within this context, the role of Platform of Trust would be in the discovery of data sources (in partnership with data producers) and subsequently creating a blockchain based data product from the discovered source. From there, the data product/blockchain would be published in a form that would be accessible via a monetized method. In practice, access to these products could be gained via a purchase of a private key or other common and existing means of granting access to the product (Medium. 2021).

While most sources talk about monetization of user data (Horwitz, 2021; Medium. 2021; Schmarzo, 2021), utilizing the same principles for industrial and business data that is common for Platform of Trust to work with (Vuorinen et al., 2020), should provide a straightforward implementation process, while being achievable with current technology. This solution would provide benefits to "accuracy, reliability and transparency of the data itself" (Horwitz, 2021), which are intimately connected to many of the trust factors of the DTI.

The challenge with this solution is the slow transactions speeds of distributed blockchain solutions (Horwitz, 2021; Schmarzo, 2021). However, this distributed solution would also provide future possibilities. With the distributed nature of blockchain, the data products could be published in separate batches, in which case they would not be reliant on the existence and/or upkeep by the platform provider, or as a continuously updating whole, consisting all the previous versions. In either case, as the published solution would be independent of the company and would instead be accessible to anyone with the correct credentials after the original publication, these solutions would create an extra sense of security in clients, knowing that their access to the data is guaranteed after the publication by the distributed nature of the solution.

5.1.4 Pros and cons of blockchain implementation options

Each of the three previously mentioned options are compared to each other with their pros and cons in the table 2.

Table 2: Pros and cons of different options of implementing blockchain.

Option	Pros	Cons
BaaS/PaaS	The most established option of implementing blockchain to business. Offers business opportunities for both highly customized (PaaS like approach) and standardized blockchain products (application-oriented approach).	It would need a lot of knowledge and skill in both data productization and blockchain to create either of the BaaS approach-oriented product.
IaaS	IaaS would improve the accuracy and trustworthiness of current DTI. This would allow achieving higher leveled values in untrusted ecosystems. Could allow for faster transactions speeds in case of a level of centralization is included in the solution	Fairly new approach of implementing blockchain to business which means it might take much more resources and skill to create. Also maintaining the infrastructure would require commitment of resources on an ongoing basis.
Data products as distributed blockchain solutions	Distributed nature of the solution would prove advantageous to trust factors such as Identity, reliability and rights. The solution is comparably simple and straightforward to complete with current technology.	Slow nature of transactions in a distributed solution could prove a major disadvantage to some customers, detrimental to data flow quality trust factor and the overall scalability of the solution. Simultaneously, speeding up transactions is an unsolved problem in blockchain research.

Each of the options has their good and bad sides but the most promising blockchain implementation option is BaaS. It is the most flexible option for business because it offers business opportunities for both the highly customized and more standardized product to sell to the data producers. BaaS would probably also require the least number of resources and modifications of current business of these three options. BaaS product could be offered alongside with current DTI.

Other options would be great for future to improve current DTI business but currently they aren’t as worth investing as BaaS because they would need either a lot of resources or even redesigning the current DTI tool.

5.2 Blockchain implementation for DTI and trust factors

In this chapter blockchain's opportunities and challenges are linked to Data Trust Factors in the DTI. Blockchain's opportunities are transparency, decentralization, immutability, anonymity, and efficiency. In turn, the challenges with data trust context are scalability, legal problems, decentralization and need for processing power and time. Table 3 summarizes these opportunities and challenges.

Table 3: Linking Data Trust Factors to blockchain opportunities and challenges.

Data Trust Factor	Opportunities	Challenges
Identity	Decentralization, Transparency, Anonymity, Efficiency,	
Reliability	Decentralization, Transparency, Anonymity, Efficiency	Scalability, Legal problems
Rights	Decentralization, Transparency, Efficiency	Scalability
Flow quality	Decentralization, Efficiency, Immutability, Efficiency	Scalability, Need for processing power and time
Content quality	Immutability	
Compatibility	Decentralization	Scalability
Security	Immutability, Anonymity	Need for processing power and time, Decentralization

5.2.1 Linking blockchain opportunities with Data Trust Factors

Blockchain technology establishes policy-based trust in data and guaranteeing transparency in data, instead of using the history of interactions as a means to measure trust. Generally, data trust management approaches address establishing trust among interacting parties in distributed and decentralized systems. Blockchain has a potential to provide a platform which enables auditable architecture, enhanced privacy and controlled data access, sharing and processing. As implementing a blockchain part of Platform of Trust, the trust factors determine the DTI value for each data product. Blockchain's traits (transparency, decentralization, immutability, anonymity and efficiency) support the best possible value of the factors. There is a mutual relationship between DTI factors and blockchain opportunities (Table 2).

Blockchain's transparency addresses rights, identity and reliability. Firstly, each user has transparency over what data is being collected and how they are accessed. The system supports data ownership, since the users as the owners of data are recognized. The services are identified as guests with delegated permissions. (Zyskind et al. 2015) Our architecture aims attention at ensuring that users own and control their data in order to gain data trust from data rights perspective. Optimizing transparency by data ownership policy and traceability are correlated (Franscisco & Swanson 2018). Traceability is defined as the ability to identify and verify the components of information and chronology of events in all steps of a flow chain (Skilton & Robinson 2009).

Secondly, through traceability of information, it can be ensured that nothing is unduly modified. (Franscisco & Swanson 2018) The levels of transparency and traceability that blockchain affords increase the accountability. Accountability in the blockchain and trust context involves that a party or parties experience consequences for their actions, in other words parties, are held accountable for their actions (Rizal Batubara et al. 2019). Accountability influences organizational-level identity since it impossible to hide transactions and relatively easy to track data entries. Organizational-level identity retains in turn mutual relationship with data-level identity. Thirdly, transparency, traceability and accountability keep blockchain honest and untangle the reputation of data publisher. Ultimately, reliability in the DTI is upheld since it derives from confidence on data provider.

Decentralization provides an alternative which reflects in data reliability, rights, flow quality, compatibility and security. At the start with a decentralized data management system, it is ensured that users own and control their data. Blockchain enables using a decentralized network of peers accompanied by a public ledger. (Zyskind et al. 2015). Data rights are supported since we implement a protocol which turn a blockchain into an access-control manager. Secondly, blockchain offer a way for parties who do not know or trust each other to reach consensus on a common digital history. Our protocol that does not require trust in a third party strengthens reliability since reliability could be transferred by collaborative, decentralized approach. With collaborative approach, data is sourced from communities and partners that use the data stored in a blockchain (Willoughby et al. 2018).

After second with decentralization, the peer-to-peer networks offer profound possibilities for collaboration for companies which exchange data with their partners. This data is typically stored in each company's data silos. Each time the data is transformed, it can cause data loss or incorrect data to enter the workstream. (Halaburda & Mueller-Bloch 2019) By having a decentralized data warehouse, every party has access to real-time and shared view of the data which link decentralization to data flow quality. Eventually, taking legal and regulatory decisions about collecting, storing and sharing data should be simpler with a decentralized platform. Having all this in mind, compatibility is associated with decentralization.

Blockchain technologies indeed provide transparency and decentralization, but more importantly they create an immutable and distributed aspect of the custody record (Franscisco & Swanson 2018). With immutability, blockchain will be used to guarantee that data is tamper-proof and ensure that data tampering can always be detected. Immutability enacts data content and flow quality and security in the DTI. First off, data flow management is responsible for managing the raw data. Once received the raw data is stored in the blockchain's immutable storage. The data in the immutable storage will be used to validate the data in the off chain. (Rath, Codenie and Hristoskova, 2020) With immutable storage, data flow quality can be reached in DTI.

Secondly, data auditing allows a data customer to audit the data set and check whether or not data tampering occurred. (Rath, Codenie and Hristoskova, 2020) Once a data is appended to the blockchain, it cannot be altered, turning a blockchain into an immutable record of past activity (Franscisco & Swanson 2018). As ledger remain unchanged, complete data set is not stored on the blockchain, only a hash value of it and its meta data. For these reasons, immutability can undertake the data quality issues. Our immutable ledger gives credence to the validity of record of the change or sharing of data and could be used for a peer-to-peer community-based sharing network permitting for community auditing (Willoughby et al. 2018). Altogether, our immutable ledger with its traits improves data security in the DTI.

Anonymity attempt to protect personally identifiable information. Each user can interact with the blockchain with a generated address, which does not uncover the real identity of the user. Normally the users of the platform remain anonymous, and no central party keeps users' private information (Zheng et al. 2017). At first, since user's addresses are pseudonymous in blockchain, anonymity raises data identity in the DTI. As such, participant and data provider confidentiality may be maintained (Franscisco & Swanson 2018), which directly affects data reliability. Lastly, anonymity transforms the process of obtaining a relationship with the identity irreversible (Zheng et al. 2017). Data security in the DTI context leverages that process with the ability to hide the real identity.

With all other opportunities in blockchain technology, blockchain can greatly improve the efficiency. Blockchain's efficiency removes obstacles which could slow down recording transactions between two parties. It can take a lot of time to propagate transactions and blocks as there a large number of nodes on public blockchain network. With fewer validators, consortium blockchain and private blockchain could be more efficient. (Zheng et al. 2017) As operations efficiency impacts an organization's competitiveness (Franscisco & Swanson 2018), data identity and reliability benefit blockchain ledger's efficiency in the first place, which gives value to data trust. However, efficiency namely takes place due to blockchain's distributed ledger and decentralized nature. Data flow quality in the DTI leverages the distributed ledger and the decentralization holds data rights up. In this degree, blockchain's efficiency acts on flow quality and rights.

5.2.2 Linking blockchain challenges with Data Trust Factors.

Some of the challenges of blockchain technology also affects to Data Trust Factors. Scalability has the most issues with DTI because it affects to reliability, data rights, flow quality, and compatibility. Issues with reliability, compatibility, and data rights are linked to scalability's risk with centralization which might cause problems with data ownership. Another issue with reliability is about possible legal problems with blockchain which may have negative impact on organization reputation.

Another major challenge in data trust factors is with security and the need of processing power and time. The problem is with encryption and its need for a lot of processing power and time. Encryption might not be successful if it does not get the right amount of processing power and time (Song, 2020). Energy consumption of blockchain have been hot topic in sustainability lately, so it is also possible that using blockchain will decrease the reputation-based trust. Also, blockchain is not well-known technology, so it would be hard to get people understand, how blockchain will increase data trust, and in worst case they might think that decentralized database will give easier access to data.

Decentralization can also be challenge in data-trust, especially when some private data is stored. In decentralized system there are usually more databases, which could store the data, so there are more places where some hacker could discover private data. Also, if the data is stored to places which do not have enough focus on information security, it would be easier to get that data. This could be tackled with authentication, authorization, or encryption (Reyna et Al. 2018), but those actions affect to blockchain performance and need even more processing power to maintain system.

Challenges linked to flow quality are scalability and need for processing power. These both might slow down the data flow and even stop the data flow if system is overloaded. This impaired or paused data flow could risk the continuity of data. Also, blockchain needs storage, which could be limited especially, if the system is maintained on system where are more than computers with lower data capacity (Song, 2020). Probably all of earlier challenges be associated with the reality that there are too few professionals in blockchain and that fact which is widely mentioned in the research about blockchain. Probably that is main operator to, why those challenges show up, but that also makes blockchain based technologies hard to implement.

5.3 Data Trust Ledger and high-level architecture

Our concept is called Data Trust Ledger (DTL). In our Data Trust Ledger concept, Data Trust Factors and DTI are combined with Blockchain as a Service (BaaS) model by Platform of Trust. Our solution is a blockchain-based platform for building data trust, derived from data trust factors to determine the DTI value of every data product. The proposed DTL concept is used to safeguard that the data is trusted and safe and if data trust deteriorates, it can be quickly detected by means of trusted auditing tool operating, DTI, from the platform provider system (Zyskind et al. 2015). In our BaaS model, Platform of Trust develops and provides the DTL application able to guarantee data trust for customer enterprise based on customers’ needs.

Platform of Trust is the DTL-platform provider, but there are also other entities involved in the eco-system. Other entities are e.g., data providers and clients. Platform of Trust’s partners in the eco-system are data providers and clients which conveys the raw data and utilize the platform for trusted data-driven management. Rath, Codenie and Hristoskova (2020) proposes a high-level architecture for blockchain-based solution for building data trust, which can be leveraged for our DTL platform’s architecture. The architecture is made up of three main modules: data source environment, data flow management and secure data processing (Figure 2). First, raw data is generated in the data source environment. Secondly, through secure communication data is circulated to the data flow management, which is responsible for managing the raw data. The raw data is stored in the blockchain’s immutable storage and the traditional database called off-chain. (Rath, Codenie & Hristoskova, 2020)

Thirdly, in the secure data processing and storage, blockchain systems stores a copy of received data for validation purpose. The data is deposit off-chain storage for data processing and information and knowledge extraction. The submodule, data processing, conducts processing and extracting information and knowledge from the data set. Data processing is composed of data pre-processing, data classification and knowledge extraction. Above all, the data auditing and validation allows a data entity (data provider, client, platform provider, and so on) audit the data and inspect whether or not data tampering has occurred. The auditing module carries out the operation by matching the data set stored in the off-chain and its image stored in the blockchain. If these match, no tampering has occurred. (Rath, Codenie & Hristoskova, 2020) The auditing module is hosted by Platform of Trust to ensure transparency and trust. We propose that evaluating data trust and expressing DTI value occur in DTL platform's auditing module. The high-level architecture of our DTL solution is designed in the Figure 2.

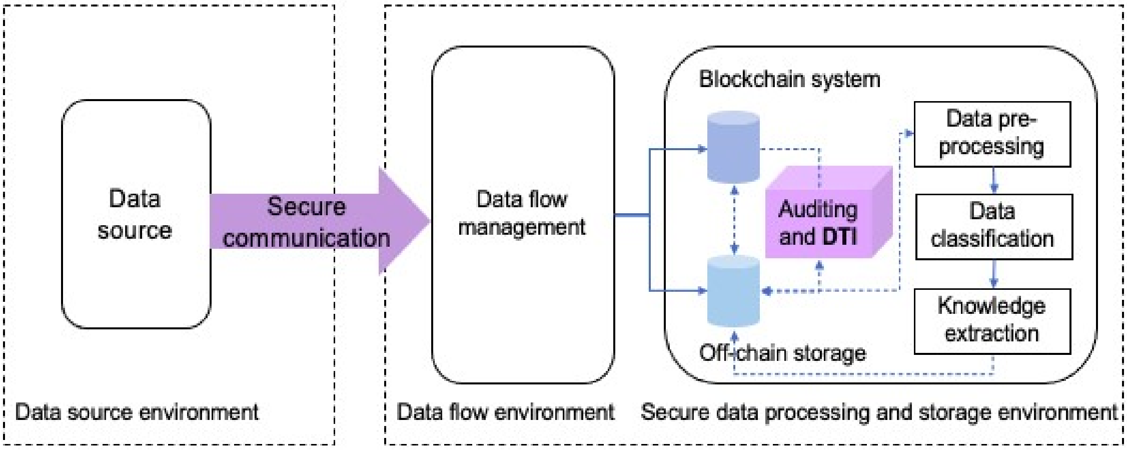

Figure 2: High-level architecture of our blockchain-based platform, Data Trust Ledger (DTL) (adapted from Rath, Codenie & Hristoskova, 2020)

Blockchain's opportunities support the highest data trust factors levels, as it is possible to audit the high DTI value of data with our platform. The evaluation of the DTI value happens in the auditing module within blockchain system, and the evaluator is Platform of Trust (Figure 2). According to BaaS model, we propose that Platform of Trust delivers blockchain-based DTL application to its customers and partners. BaaS model supports the high-level architecture we suggest since Platform of Trust has the role of platform provider. Platform of Trust's DTL platform will offer transparent and trusted environment to leverage data. Platform of Trust can lead its eco-system into unimaginable collaboration and innovation.

6. CONCLUSION

There are obvious needs for ways to equalize data trust, which is still a major source of competitive advantage for well-known companies, who are able to leverage their reputation based, while less established companies have limited means to compensate for trust that is gained over time.

Blockchain has lots of potential to even this situation, offering a solution where we can move form reputation-based trust to policy-based trust. As an additional benefit, this policy-based trust is found to be superior not just the data utilizer, but also the ecosystem, with data providers being able to compete on an even playing field (Vuorinen et al., 2020). Blockchain technology have a benefit in every data trust factor that we have identified with Platform of Trust. On the other hand, blockchain is new technology, which presents challenges such as the lack of detailed documentation on intricate solutions and their implementation, as well people who understand technology adequately to undertake such solutions.

The blockchain field is on where there is a lot of ongoing research, so the next few years are likely show us the fields and solutions for which blockchain provides the best match for. Despite the challenges, the possibilities of the technology from the point of view of trust, lack of similar solutions from existing competition, and wide scale value to the entire ecosystem, there is a large potential gap to release either data products or services based on blockchain solution.

From this premise, it is possible to see scenario where blockchain technology have become so common that it would be competitive against centralized cloud service-based solutions, but that need lot of work in documentation of technology and education in blockchain based solutions. In this work we provided three possible solutions for utilization of the blockchain in data trust, all of which answer to different possible future states of the technology:

- **Blockchain as a Service / Platform as a Service**, best fit for the current trends of the technology with opportunities for highly customized or more standardized product to sell data.
- **Infrastructure as a Service**, which could answer to the needs of a trustless ecosystem by providing a level of centralization, while also providing possibilities for faster transactions speeds.

- **Data products as distributed blockchain solutions**, optimal in the case where distributed solutions become the industry standard.

Overall, blockchain technology has advantage in systems, where two or more stakeholders should share trusted data between each other, and in future it would serve alternative option to cloud-service based solutions. All three of these blockchain solutions are beneficial especially in environments where the trust in data is important. As such, adopting one of them is one possible option to increase the general DTI values of data products provided by Platform of Trust.

REFERENCES

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. Telematics and informatics. [Online] 57.

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. (2018). Blockchain with internet of things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), 40-48.

Bengfort, B. and Kim, J. (2016). 'The Age of the Data Product', in *Data Analytics with Hadoop*. O'Reilly Media, Inc. Available at: https://www.oreilly.com/library/view/data-analytics-with/9781491913734/ch01.html (Accessed: 3 March 2021).

DalleMule, L. and Davenport, T. H. (2017). 'What's Your Data Strategy?', *Harvard Business Review*. May-June 2017, p. 15.

Davenport, T. H. & Kudyba, S. (2016). Designing and Developing Analytics-Based Data Products. MIT Sloan Management Review.5(1), pp.83-89.

Francisco, K., & Swanson, D. (2018). The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics*. 2(1), 2–13.

Gambetta, D. (1988). "Can We Trust Trust?" in Trust: Making and Breaking Cooperative Relations. Ed. Oxford: Basil Blackwell, pp. 213–237.

Geisler, S. et al. (2016). Ontology-Based Data Quality Management for Data Streams. *Journal of Data and Information Quality.* 7 (18).

Horwitz, L., (2021). *How to Monetize Customer Data with Blockchain Technology – Channel Futures*. [online] Channel Futures. Saatavilla: <https://www.channelfutures.com/security/how-to-monetize-customer-data-with-blockchain-technology> [Haettu 8 Huhtikuu 2021].

Halabura, H. & Mueller-Bloch, C. (2019). Will We Realize Blockchain's Promice of Decentralization? *Harvard Business Review*, 04 September 2019.

Haug, A., Zachariassen, F. & Liempd, D. (2011). The costs of poor data quality. *Journal of Industrial Engineering and Management*. Vol. 4 (2), pp. 168-193.

Khatri, V. & Brown, C. V. (2010). Designing Data Governance. Communications of the ACM. Vol. 53 (1), pp. 148–152

Kilroy, K. (2019). Blockchain as a Service. 1st edition. O'Reilly Media, Inc.

Kuoppakangas, P. et al. (2019) Revisiting the five problems of public sector organisations and reputation management-the perspective of higher education practitioners and ex-academics. Springer.

Leonelli, S. (2016). Data-centric biology: A philosophical study. Chicago: University of Chicago Press.

X. Li and C. A. Wang, (2017). "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," Decis. Support Syst., vol. 95, pp. 49–60, 2017.

Lu, Q. et al. (2019). uBaaS: A unified blockchain as a service platform. Future generation computer systems. [Online] 101564–575.

Medium. (2021). *Monetizing User Data on the Blockchain*. [online] Saatavilla: <https://olshansky.medium.com/monetizing-user-data-on-the-blockchain-3584351a752e> (Accessed 8 April 2021)

Morey, T., Forbath, T. 'Theo' and Schoop, A. (2015). Customer Data: Designing for Transparency and Trust. *Harvard Business Review*, 93(5), pp. 96–105.

Pagano, C. (2013). Data Interoperability. *Data Science Journal.*

Pirkkalainen, H. (2021). TLO-35307 Emerging Technology Adoption and Use (Lectures)

Rath, A., Codenie, W. and Hristoskova, A. (2020). 'Towards Building Data Trust and Transparency in Data-Driven Business Applications', in Casimiro, A. et al. (eds) *Lecture Notes in Computer Science*. Cham: Springer International Publishing.

Redman, T. C. (2015). 'Can Your Data Be Trusted?', *Harvard Business Review*, 29 October. Available at: https://hbr.org/2015/10/can-your-data-be-trusted (Accessed: 21 February 2021).

Reyna, A. et al. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems. [Online] 88173–190.

Rizal Batubara, F., Ubacht, J. & Janssen, M. (2019). Unraveling Transparency and Accountability in Blockchain. *Proceedings of the 20th Annual International Conference on Digital Government Research.* 204–213.

Sands Glassberg, E. (2018). 'How to Build Great Data Products', *Harvard Business Review*. October 2018.

Saunders, M., Lewis, P., & Thornhill, A., (2019). Research methods for business students. Eighth edition. Harlow, England: Pearson Education.

Schmarzo, W., (2021). Is Blockchain the Ultimate Enabler of Data Monetization? - KDnuggets. [online] KDnuggets. Saatavilla: <https://www.kdnuggets.com/2017/04/blockchain-ultimate-enabler-data-monetization.html> (Accessed 8 April 2021)

Skilton, P., & Robinson, J. (2009). Traceability and Normal Accident Theory: How Does Supply Network Complexity Influence the Traceability of Adverse Events? *The Journal of Supply Chain Management*. 45(3), 40–53.

Storey, V., Dewan, R. & Freimer, M. (2012). Data quality: Setting organizational policies. Decision Support Systems. Vol. 54 (1), pp. 434–442.

Singh, J., & Michels, J. (2018). Blockchain as a Service (BaaS): Providers and Trust. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 67–74. https://doi.org/10.1109/EuroSPW.2018.00015

SONG, J. et al. (2021). Research advances on blockchain-as-a-service: architectures, applications and challenges. Digital communications and networks. [Online]

Thouvenin, F., Weber, R. H. & Früh, A. (2017). Data ownership: Taking stock and mapping the issues. In: *Frontiers in Data Science.* pp. 111–145. Boca Raton: CRC Press. p. 393.

von Solms, R. & van Niekerk, N. (2013). From information security to cyber security. Computers & Security. Vol 38, pp. 97-102. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404813000801> (Accessed 1.3.2021).

Vuorinen, O.J., Ryhänen, A., Huttunen, O., Tamminen, A., Järvinen, K., Rintamäki, K., & Viertola, V. (2020). CASE PLATFORM OF TRUST: Trust in Data.

Vuorinen, O.J. (2021). Conceptualization of a Data Trust Index Based on the Role of Turst as a Forfeiture of Decision-Making Power.

Wang, L. & Guo, S. (2020). Blockchain Based Data Trust Sharing Mechanism in the Supply Chain. In *Security with Intelligent Computing and Big-data Services*. [Online]. Cham: Springer International Publishing. pp. 43–53.

Willoughby, G., Ingram, T., Byrne, T., Smith, D. & Rahman, N. (2018). Decentralization of reliability data through blockchain. Reliability Blockchain.

Zheng, Z. *et al.* (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. in *2017 IEEE International Congress on Big Data (BigData Congress)*. *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375. Available at: https://www.researchgate.net/profile/Hong-Ning-Dai/publication/328271018_Blockchain_challenges_and_opportunities_a_survey/links/5bd2706f92851c6b278f31eb/Blockchain-challenges-and-opportunities-a-survey.pdf (Accessed 14.3.2021).

Zyskind, G., Nathan, O. and Pentland, A. (2015). ‘Decentralizing Privacy: Using Blockchain to Protect Personal Data’, in *2015 IEEE Security and Privacy Workshops*. *2015 IEEE Security and Privacy Workshops*, pp. 180–184. doi: 10.1109/SPW.2015.27

APPENDIX A: CHANGELOG

This version is the final version of group work as 9.4.2021 and it has been modified and fixed after its first return which was in 19.3.2021. The list of changes is shown below.

Changes:

- Chapter 5: How to implement blockchain
    - Added general description of the chapter
- Chapter 5.1.3: Dataproducts as distributed blockchain solutions
    - Reworked chapter
- Chapter 5.1.4: Pros and cons of blockchain implementation options
    - Added table 2 for comparision of pros and cons of blockchain implementation options.
    - Added reasoning for choosing BaaS as the implementation solution.
- Chapter 5.2: Blockchain implementation for DTI and data trust factors
    - Text above table 2 was improved and the chapter contents were elaborated.
- Chapter 5.2.1: Linking blockchain opportunities with data trust factors.
    - More detailed step-by-step description was included on how blockchain opportunities connects with each data trust factors (identity, reliability, rights, flow quality, content quality, compatibility, and security)
    - More references were sought to support the argumentation and added in-text citations.
- Chapter 5.2.2
    - Explained challenges with data trust and blockchain solution.
- Chapter 5.3. DTL concept description
    - Our concept BaaS + data trust factors + PoT was elaborated, and it was named as Data Trust Ledger (DTL).
    - High-level architecture of our solution was explained.
    - Figure 2 was drawn.
- Combined "Chapter 6 Discussion" and "Chapter 7 Conclusions and contributions" to "Chapter 6 Conclusions"
- Removed "TODO: IoT and Blockchain" in p.13 because it wasn't relevant for our group work.
- Fixed several grammar errors and polished overall look of paper.