MASTER'S THESIS

INFORMATION SCIENCES

Digital Identity Management on Blockchain for Open Model Energy System

---

Author :
Sesaria Kikitamara
s4561414

Supervisors :
Prof. dr. M.C.J.D. van Eekelen
Dipl. Ing. Jan-Peter Doomernik (Enexis)

August 23, 2017

Preface

This thesis was produced for the completion of my master's course in Information Science. The presented thesis is the outcome of a case study on Enexis, a Dutch energy grid company. They provide access to energy for 33% of the Netherlands (2.7 million households). They ensure this access to energy by owning the electricity grid.

For the future, they identify several exponential technologies that, combined, could disrupt the way people are provided with energy. Enexis is focused on solutions that are caring and inclusive: caring in that they serve the citizens and the organizations of the Netherlands, and inclusive, in that energy distribution is not determined by business cases or profit formulas, but can be ensured as a right for everybody.

Enexis follows Gartner's vision concerning the ability of blockchain to lead to a programmable economy. In this programmable economy, Gartner expects new economic models to arise. In this vision, blockchain would be the fabric with which these new economic models are operated, by artificial intelligence, autonomous machines, companies, or individuals. Currently they are preparing to implement EV charging points based on blockchain applications, as one of their actions towards a programmable economy.

Furthermore, although this study case is performed for Enexis, the results can be implemented in other economic models. Therefore, the solution is presented in this report is widely applicable and may be suitable for other fields, such as finance, healthcare, government and others. However, the solution is not free of limitations. There may be problems with and challenges to some aspects and practices.

I am grateful to all the people involved in this study. In particular, I would like to thank Prof. Marko van Eekelen for supervising this master's thesis and Mr. Jan-Peter Doomernik for giving me opportunity to take part in this Enexis project, as well as for offering a lot of insight into this project.

Finally, I would like to thank my family and my friends for being helpful and supportive during my time studying in Radboud University, as well as the Indonesia Endowment Fund for Education (LPDP) for granting me a master's scholarship to study in Netherlands.

Nijmegen, August 23 2017
Sesaria Kikitamara

Abstract

Nowadays blockchain has gained the interest of both technological and business sectors. Accordingly, the energy sector is considering blockchain as the future of their infrastructure. There are two visions for energy system related to this, closed model and open model. Technically speaking, closed model related to the intranet system and open model to the internet system. Particularly, through its decentralized mechanism, blockchain could offer a decentralized energy transmission and supply system in an open model environment supported by the use of the Internet of Things and artificial intelligence. In an open model, there are interconnected devices and machine-to-machine interactions, and the transaction data is stored on the blockchain. Users and companies identifies themselves using their digital identities. Therefore, due to the implementation of blockchain, there is a need for different kinds of digital identity management. In this study, we examine three categories of digital identity—federated identity, user-centric identity, and hybrid identity—to determine which is best-suited for the open model energy system that is our case study. In order to move towards open model, we need to evaluate also the closed model implementation. Thus the basic method that we apply is a comparison of the digital identity categories based on their implementations for both closed and open model, advantages, disadvantages, and similarities with blockchain characteristics and open model characteristics. The proposed solution reveals that hybrid identity is most likely the most appropriate for an open model system. Additionally, this thesis also proposes some properties that are needed to developed the selected digital identity category.

Keywords: Blockchain, Digital Identity, IoT, Hybrid Identity

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

1.1.1 Two Visions for Future Energy System

This study began with ideas for the future of energy infrastructure. Today, energy is generated by power plants and from several renewable energy sources. This energy is distributed to companies and other customers using the energy grids. It may be the case that this system will change only incrementally in the years to come.

There is also another possibility, however, a possibility for disruptive change. Energy distribution could change through a combination of several emergent technologies. There are also many raw energy sources that could be used. For example, the sun distributes a very thick layer of raw energy over the earth. New infrastructures could be put in place using machines that transform raw energy (sunlight) into usable energy (for example the solar fluid hydrogen). At the Massachusetts Institute of Technology (MIT), researchers are exploring artificial leaves as an example of such a technology. As well as the distribution starting point, the distribution process could also be changed, such as when we use excess capacity in self-driving cars.New infrastructures in which machines communicate could manage future energy demands.

In both visions, there are many emergent technologies that will help us to connect with devices, vehicles, building, etc., including embedded sensor and network connectivity that will enable our devices to collect and exchange data. Technologies such as blockchain, autonomous assets, artificial intelligence and the internet of things (IoT) are correlated and become the buildings blocks of future infrastructure. The amount of change in the energy system will determine the future infrastructure of the energy system. One emergent technology that could impact distribution is blockchain. This could be used to change the current system incrementally or to disrupt the current system.

To have a high-level understanding of the extent to which an emergent technology can change a system, this introduction discusses a technology introduced 20 years ago and determines when the technology enabled incremental change and when it enabled disruptive change. The characteristics of both types of change are described in two scenarios and these are used as part of the analysis (the comparison analysis). The technology in question, which has brought both incremental change and disruptive change, is the internet.

In the form of the intranet, it has brought incremental change. This technology is used in a closed environment, typically, as an enterprise- or consortium-focused solution. The main focus is the optimization of the process. There is no impact on current paradigms like current economic models, solutions for the current dominant market players or the lock-in of customers in the current business model. The solution is valuable for known players who have an enhanced control over their processes, and it does not add value for new players. Basically, it made it possible to rebuild known infrastructures with perhaps one or two significant changes.

In the form of the internet, it has brought disruption. This technology is used in an open environment, typically, as an ecosystem solution. Main focus is a value-adding redesign of both mechanisms and systems. We can observe paradigm shifts like new economic models, solutions with new market players or radical shifts in business models with new forms of lock-in effects. This solution forces known players to change or to lose control over their processes and markets. A few examples are the shifts from hardcopy to downloadable media for a fraction of the price, from shopping in stores to online shopping with distribution changes like the "long tail approach" and from enterprise software solutions running on individual servers to software as a service in the cloud.

From an energy perspective, in the closed scenario, the dominant market players create platforms to exchange energy. The use of renewable energy creates the need for a different kind of exchange, a flexible exchange. This is because the grid is limited and if too many users require energy, for example, for cars charging at the end of the working day, or deliver energy, for example, when the sun shines, solar panels deliver everywhere simultaneously, customers have little choice. At this moment in time customers find it difficult to understand their energy bills and to compare products. Closed (consortium) blockchain solutions help to produce transparent markets.

The impact of the open scenario is much harder to predict, as we can see from the example of the internet. We can suppose that changes in energy generation and distribution would be beneficial for new entrants or even society as a whole. We find some guidance in publications by researchers like Gartner, who predicts a programmable economy, and the theories of Christensen about disruptive innovation [24].

In order to move towards an open scenario, we should first examine the implementation of the closed scenario. So, in this study, we use the open and closed scenarios to explore the solutions for blockchain-based digital identities. In particular, this study examines the management of digital identity in an open model system, since in the future everything

Table 1.1: The Difference of Closed Model and Open Model

Characteristics	Closed Model	Open Model
Focus	Enterprise or consortium focused	Ecosystem
Change	Optimization of the process or incremental change	Disruption
Playing field	Within current paradigms	Paradigm shift
Beneficial for	Current Dominant market players	Mainly New entrants
System architecture	Minimal change in design and market players. Changes are known beforehand and result of negotiation	Radical redesign by evolution and revolution. No control over changes
Business models	Business model of dominant market players maintain	Redesign of business models and boundary conditions

will be connected: the identity of things. Everything inside the house including heating system, fridge or a lightbulb will be connected to the internet; therefore, the evolution of digital identity will be a vital contribution to building the future of open model systems.

1.1.2 Applying Blockchain to The Vision

Blockchain is considered to be a suitable technology to achieve the visions described above. Blockchain is a distributed ledger, with which many people can write entries into a record of information, and a community of users can control how the record of information is modified and updated. Blockchain is the first step towards the future of the distributed ledger platforms that enable the *Programmable Economy* [52] predicted by Gartner Inc. vice president, David Furlonger. The programmable economy is a new economic system based on autonomic, algorithmic decisions made by robotic services, including those associated with the IoT, and this concept is opening the door to a groundbreaking range of technological innovations [81]. Additionally, following are some reasons why blockchain is the appropriate choice:

- **Secure transactions**. The database can only be extended and previous records cannot be changed. Everyone who participates can see the blocks and the transactions stored in them.
- **Interconnected machines**. Blockchain has drawn the attention of companies such as International Business Machines (IBM), which is embracing it as the next genera-

tion of inter-device transactions and using it as the technology to enable IoT devices to exchange information without the need for intermediaries [58].

- **No centralization**. Blockchain is decentralized, so there is no single authority that can turn it off.

In support of the above-mentioned vision, blockchain is used as the application layer of the internet. For example, this technology works as an instrument to authenticate and manage the metering and billing processes for electricity consumption or autonomous vehicle charging stations. In existing energy delivery mechanisms, a complex system carries multiple roles, ranging from power producers, transmission system operators, distribution system operators, and suppliers, that transact on various levels using huge databases, which are operated differently for each area. By using typical blockchain applications, such as Hyperledger[1] for the closed blockchain system, such complexity can be reduced because they offer a decentralized transaction model.

Under such mechanisms, a decentralized energy transaction and supply system [42] becomes a possibility for the future (Figure 1.1). Energy that is generated in distributed generation facilities could be transported to end users via smaller networks. The transaction could be based on a smart contract and recorded on the blockchain. One of the system components, a smart meter, would measure the amount of energy produced and consumed, while energy-trading activities and cryptocurrency payments would be controlled by smart contracts and executed through the blockchain. Additionally, other smart systems such as smart devices or homes, sensor technology, and smartphone apps could also be placed on the blockchain as system components, allowing them to communicate with each other. Particularly, in an open model energy system, there are interconnected devices. Digital identity needs to verify the identification and access permits of those devices. This research seeks to investigate the application of digital identity management on blockchain for an open model energy system.

1.2 The Assumption

This thesis begins by assuming that blockchain technology is a suitabe technology for attaining the open model system, despite there being some counter arguments on the use of blockchain in this context [2]. Thus, even though there may be some future challenges that halt the implementation of blockchain (whether the blockchain is appropriate choice or not), this is not considered as part of this research. We will not look further into those

[1]Hyperledger : an open source blockchain project hosted by The Linux Foundation

[2]On paper : *Do you need blockchain ?* by Karl Wüst and Arthur Gervais, there is a flow chart to determine whether a blockchain is the appropriate technical solution to solve a problem or not

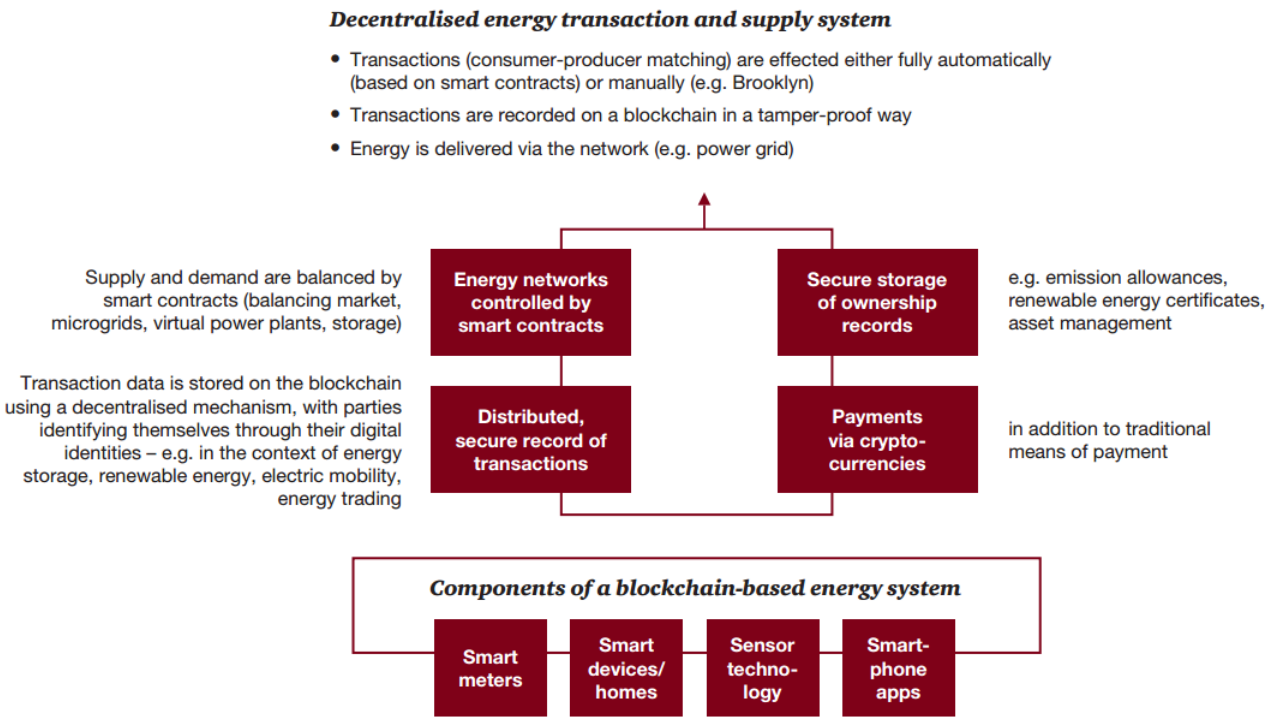

Figure 1.1: The Decentralized Energy Transaction and Supply System. Adapted from *Blockchain – an opportunity for energy producers and consumers?* by PwC Global Power Utilities. Retrieved July 7, 2017.

challenges, since our objective is to study what digital identity will look like when it is applied to blockchain for the proposed energy system.

1.3 Research Question

The main question for this research is :
What kind of digital identity management combined with blockchain is suitable for application in future open model energy systems ?
To answer this main research question, this research will address several sub-questions :

1. What is blockchain and how does it work?
2. What is digital identity and what does it looks like on blockchain ?
3. What are the roles and categories of digital identity management ?
4. Which categories of digital identity management are suitable for future open model energy systems ?

5. What properties necessary to build the chosen category of digital identity management ?

1.4 Scope of Study

Since the primary topic is the use of digital identity on blockchain, this research investigates the way it is used for organizational business within the perspective of information technology such as the components and attributes it needs, and the possible challenges it presents. Thus, this research does not go further into technical details like the cryptographic technique or the network architecture.

1.5 Methodology

Systematic literature review (SLR) is the methodological approach used to analyze the problems and find the solutions. A SLR is an essential tool for summarizing evidence accurately and reliably. There are many reasons for undertaking a SLR. The most common reasons are the following [49]:

- To summarize the existing evidence concerning a treatment or technology, e.g., to summarize the empirical evidence of the benefits and limitations of a specific agile method.

- To identify any gaps in current research in order to suggest areas for further investigation.

- To provide a framework or background in order to appropriately position new research activities.

However, SLRs can also be undertaken to examine the extent to which empirical evidence supports or contradicts theoretical hypotheses, or even to assist the generation of new hypotheses. For this research, the literature is mostly derived from relevant research conducted in three fields: digital identity, blockchain and energy systems.

The specific methodology presented on this research is a comparative analysis of each digital identity category and its practical implementations, advantages, and disadvantages to formulate the advice for the approach. For the result, this research delivers an approach for what kind of digital identity is suitable for an open model system, a use case scenario and the properties that will be needed.

1.6 Report Structure

Overall there are eight chapters, including the introduction and discussion. The main analysis is presented in Chapters 2 to 6. Chapter 2 discusses blockchain technology in order to answer the first research sub-question: *what is blockchain and how does it work?* Chapters 3 and 4 analyze the role of digital identity management and its current implementation, engaging with the second and third sub-question: *what is digital identity and what does it look like on blockchain? What are the roles and categories of digital identity management?* Chapter 5 presents an evaluation of the comparison of the digital identity categories to identify which one is best suited to an open model system, responding to the fourth sub-question: *which categories of digital identity management are suitable for future open model energy systems?* Finally, Chapter 6 explains the selected category and the properties it requires, in response to the fifth sub-question: *what properties are necessary to build the chosen category of digital identity management?*

Chapter 2

The Blockchain Technology

2.1 The General Concept of Blockchain

Blockchain technology has become popular since the introduction of bitcoin as digital currency. The bitcoin mechanism was introduced by Satoshi Nakamoto in 2008 in a paper entitled *Bitcoin: A Peer-To-Peer Electronic Cash System* [62]. This paper described a peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution [27]. Blockchain is the name of the technology behind this. The technological concept behind blockchain is similar to a database, except that interactions with them differ. A blockchain is essentially a distributed database of records, or a public ledger of all transactions or digital events that have been executed and shared among the participating parties [27] across peer-to-peer networks.

Blockchain has two fundamental features. The blockchain is *public*. Anyone can view it at any time, because it resides on the network, and not within a single institution charged with maintaining and keeping the record. Blockchain also *encrypted*, since it uses encryption involving public and private keys to guarantee its security. Figure 2.1 represents the general idea of how this technology works, referring to its application for bitcoin. The bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called blockchain. The transactions in one block are considered to have happened at the same time. These blocks are linked to eachother (like a chain) in a linear, chronological order, with every block containing the hash of the previous block.

Furthermore, as blockchain establishes the new era of the digital economy, there are seven design principles for creating software, services, business models, markets, organizations, and even governments on the blockchain [79]. These are detailed below.

1. Networked integrity
   The system lets the network reach a consensus (the acceptance and verification by

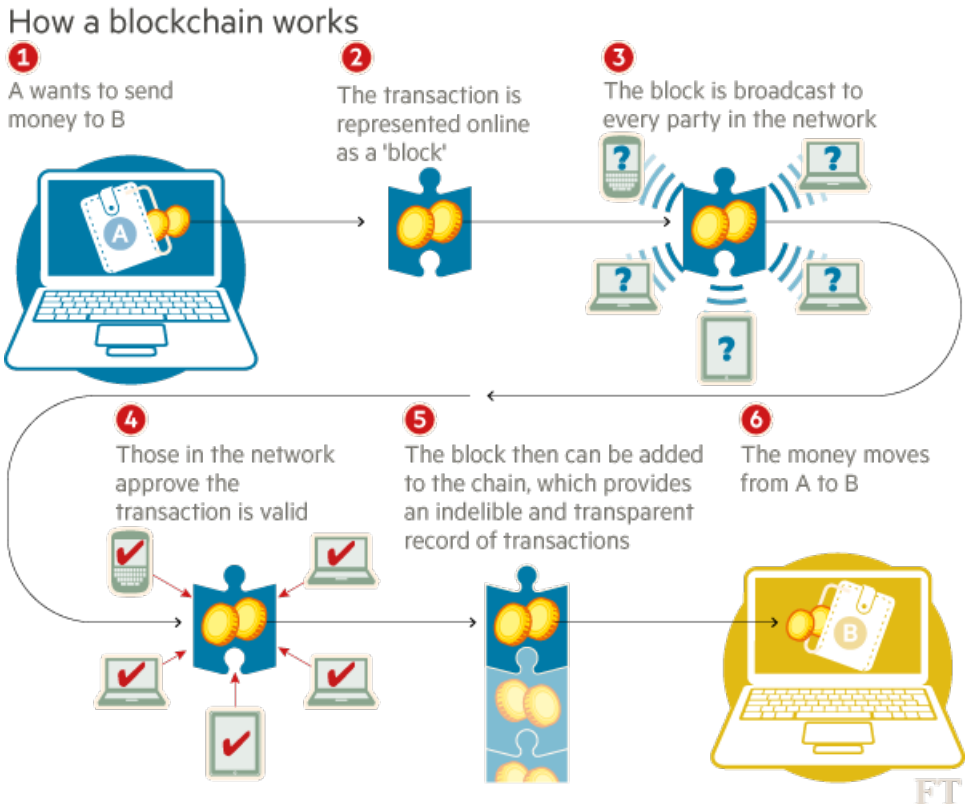

Figure 2.1: How Blockchain Works. Adapted from BlockChain Technology: Beyond Bitcoin, Retrieved May 2, 2017, From *Applied Innovation Review, Issue No.2 June 2016.*

all the users in the network) algorithmically on what happened and record it cryptographically on the blockchain. Integrity is encoded into every step of the process and distributed, not vested in any single member. Participants can exchange value directly with the expectation that the other party will act with integrity. Each block must refer to the preceding block to be valid. No one can hide a transaction, and that makes the transaction more traceable than cash.

2. Distributed power
   The system uses peer-to-peer networks to distribute power without any single point of control. No single party can shut the system down. If a central authority manages to black out or cut off an individual or group, the system will still survive. Everyone can see what is happening if some of the network attempts to overwhelm the whole.

3. Value as incentive
   The system aligns the incentives of all the stakeholders. In the case of bitcoin, there is an incentive for miners to participate in creating a block and linking it to the previous block. Imagine a peer-to-peer network of solar panels for which the home owner receives real-time compensation on the blockchain for generating sustainable

energy.

4. Security
   Anyone who wants to participate must use cryptography. In Satoshi's paper, he claimed that participants were required to use a public key infrastructure (PKI) for establishing a secure platform. The PKI is an advanced form of asymmetric cryptography, in which the user receives two keys that do not perform the same function: one is for encryption and the other for decryption.

5. Privacy
   Individuals control their own data, not a single party. On a blockchain, participants can choose to maintain any degree of personal anonymity in the sense that they do not need to attach any personal details to their identity or store those details in a central database. Additionally, the identification and verification layer are separate from the transaction layer.

6. Rights preserved
   Ownership rights are transparent and enforceable. Individual freedoms are recognized and respected. As a ledger of everything, the blockchain can serve as public registry. through a tool called Proof of Existence (PoE), a site that creates and registers cryptographic digests of deeds, titles, receipts, or licenses on the blockchain. The hash of the document is calculated on the user's machine, not on the PoE site, thus ensuring the confidentiality of the content.

7. Inclusion
   Blockchain allows for distributed capitalism, lowering the barrier for participation. This makes the economy work best for everyone. Currently most financial institutions have mobile payment apps that combine camera or QR scanner codes. As a result, fees are needed to support these kinds of intermediaries. Satoshi designed the system to work through the internet, but it can run without the internet if necessary. He imagined that the typical person would interact with the blockchain through what he called simplified payment verification. This would drastically lower the cost of transmitting funds.

2.2 Types of Blockchain

The types of blockchain are discussed from two perspectives: first, with a high level of abstraction for the technological view, and then from a business perspective, especially energy trading. Basically there are three types of blockchain: private blockchain, consortium blockchain and public blockchain. Those types then grouped again based on business perspective to belong to two categories: open blockchain for public blockchain and closed

blockchain for private or consortium blockchain. Private or consortium blockchain is linked to a limited environment such as company, group of companies or one specific value chain, while public blockchain supports a permission-less type of blockchain.

2.2.1 Types of Blockchain from a Technological Perspective

2.2.1.1 Private Blockchain

For a fully private blockchain, the write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc., internal to a single company, and so public readability may not be necessary in many cases, though in other cases public auditability is desired [16].

Hyperledger. Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by the Linux Foundation, including leaders in finance, banking, IoT, supply chain, manufacturing and technology [9].

MultiChain. MultiChain is a platform for creating and deploying private blockchains. It solves the related problems of mining, privacy, and openness via the integrated management of user permissions [40]. It is easy to configure and can work with different blockchains at the same time. The benefit for institutional users is that it enables private blockchains to be configured and deployed by system administrators rather than specialized developers. An analogy is the way in which relational database management systems such as Oracle or SQL Server allow databases to be created and used with a few SQL commands. A further benefit of supporting multiple blockchains is the opportunity for a server to create connections between the activities on different chains [40]. For instance, an institution may want the arrival of funds on one blockchain to trigger a corresponding transfer of funds on another.

2.2.1.2 Consortioum Blockchain

Consortium blockchain is partly private. The consensus process is controlled by a preselected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node, of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants [10]. A consortium platform provides many of the same benefits associated

with private blockchain—efficiency and transaction privacy, for example—without consolidating the power of only one company [80]. Consortium blockchain platforms have many of the same advantages as a private blockchain, but operate under the leadership of a group instead of a single entity. Examples of this type are Ethereum and R3.

Ethereum. Ethereum is a blockchain platform allowing anyone build and use decentralized applications that run on blockchain technology. Currently it counts more than 86 firms in the alliance. It is attempting to build technology on which all transaction-based state machine concepts may be built [84]. This refers to the technical perspective of bitcoin. In Ethereum, the state is made up of objects called "accounts", with each account having a 20-byte address and state transitions being direct transfers of value and information between accounts that contains four fields [15]:

- The nonce, a counter used to make sure each transaction can only be processed once.
- The current ether's balance
- The contract code, if present
- The storage (empty by default)

Ethereum can also be thought of as an expanded version of bitcoin since it uses a similar underlying blockchain technology, while broadening the scope of what it can do.

R3. This is a distributed database technology company which is headquartered in New York City. It is allied with many of the world's largest financial institutions, with a mission to realize the benefits of distributed ledger technology [44].

2.2.1.3 Public Blockchain

This type of blockchain maintains the principle that anyone in the world can access the data. This includes the consensus process to write the data into the public blockchain or to block it. Public blockchain is an open-source system which is secured by the concept of cryptoeconomics, a system of economic incentives and cryptographic verification backed up by consensus algorithms such as proof of work (PoW) and proof of stake (PoS). Cryptoeconomics enable developers to create systems which have certain desired properties, such as availability, in which higher fees result in faster transactions, or convergence, in which new blocks can be added to the blockchain, but blocks cannot be replaced or removed [10]. An example of a public blockchain is bitcoin.

Bitcoin. Bitcoin is the most popular example of a concept intrinsically tied to blockchain technology. Bitcoin is a digital currency and online payment system in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank [78].The bitcoin value chain is composed of several different constituents: software developers, miners, exchanges, merchant processing services, web wallet companies, and users or consumers. From an individual user's perspective, the important elements in transacting bitcoin are an address, a private key, and wallet software, a computer software to manage the bitcoin [78]. The advantages of public blockchains generally fall into two major categories [16]:

1. Public blockchains provide a way to protect the users of an application from the developers, establishing that there are certain things that even the developers of an application have no authority to do.

2. Public blockchains are open, and therefore are likely to be used by very many entities and gain some network effects, for example, cutting costs the intermediaries with a smart contract.

In addition, there is an enhanced mechanism for a public ledger developed by IOTA[1]. Regarding the necessity of cryptoeconomics, they created a system where there is no separation between the user and the miner. So that it eliminates the need for users to pay 'miners' for doing the proof of work (because they do it themselves).

Table 2.1: Generalized Features Comparison : Public vs Private/Consortium Blockchain

Characteristics	**Public**	**Private/Consortium**
Access	Open read/write access to database	Permission rean and/or write access to database
Speed	Slower	Faster
Security	PoW/PoS	Pre-approved participants
Identity	Anonymous/pseudonymous	Known identities

2.2.2 Types of Blockchain from a Business Perspective

2.2.2.1 Closed Blockchain

Private or consortium blockchains were categorized as closed blockchains due to the similar advantages that both offer an enterprise. This solution uses blockchain in a fixed

[1]IOTA is new open-source distributed ledger. They developed Tangle, a cryptocurrency developed for the Internet of Things, will allow companies to explore business-to-business models by making technological resources potential services to be traded in an open market.
source : https://www.cryptocoinsnews.com/tangle-cryptocurrency-for-the-internet-of-things/

environment or, in another words, is an enterprise-focused solution. By allowing no change in the environment, the only beneficial effect of blockchain comes from an optimization of the process. The type of innovation is incremental, using current economic models or solutions from the currently dominant market players. Typically, these types of blockchain are interesting to known players in the industry. What they do is rebuild the known infrastructure with perhaps one or two significant changes. The IBM Hyperledger, for example, focuses on this type of solution. It brings different known players together in one blockchain solution. This solution does not need a validation (trust) mechanism, such as PoW. The players already know each other, so trust is not an issue. Optimization is possible because everybody has the same data at the same time (no data errors or data delay minimizes opportunities for the mystification of the market). We can look at industries as one connected body. The synergy effects are maximized if all the players in the blockchain solution ecosystem cooperate to create one healthy solution and to regulate competition in fixed and healthy processes.

From an energy perspective, they create platforms to exchange and trade energy. The use of renewable energy creates the need for a different kind of exchange, an exchange of flexibility, because the grid is limited and too many users ask for (for instance, car charging at the end of the working day) or deliver energy (for example, solar and wind energy—when the sun shines everywhere, solar panels deliver everywhere simultaneously). Currently, customers have a hard time understanding their energy bills and comparing products. Closed blockchain solutions, particularly consortium solutions, help to produce transparent markets. The benefit to the known market players (owners of the current infrastructure) of creating a closed blockchain system is that it is a very controlled system. A lock-in effect occurs as soon as the users are part of the closed dominant system. Dominant players can decide together if new market players may enter. They can force users to buy additional updates or hardware.

A dominant solution for identity constitutes the best barrier of entry, because every transaction (that concerns the transmission of a scares value) needs an identity. Other typical functionalities of identity include data-ownership, in which the user controls his own data, and identification by attribute, in which the user is verified not by his own unique identifier (e.g.,DIGID), but by an attribute that has been verified in the blockchain, such as a house owner with an energy neutral house.

2.2.2.2 Open Blockchain

A public blockchain can bring about disruptive changes and has the potential to lead to a programmable economy. On an open blockchain anybody can build solutions that can be used by anybody else. This can create new economic models such as a zero-margin economy [8]. In this economic model, the new market players like machines who own themselves, breaking the barriers of current industry and market models. It also enables

machine-to-machine transactions. Designs for parts of machines can exist on the blockchain before they are built, thus functioning as a kind of requirement before parts are created or 3D printed. Moreover, distributed autonomous organizations (DAO) in combination with AI constitute a logical next step in evolution of open blockchain applications.

Current energy solutions are dominated by big players who own big production plants (grey energy) or have other big stakes (investments in assets). As grid operators, they own the electricity and gas infrastructure, making them a dominant (and, by law, monopolistic) player in the current energy ecosystem. Open blockchain solutions, in combination with autonomous assets and AI, could change that rapidly. For instance they create global solutions in which machines could manage to distribute and balance energy through blockchain infrastructures (e.g., IOTA).

2.3 The Architecture of Blockchain

This section describes the basic architecture of blockchain as a distributed ledger. However, the elements of the architecture may vary depending on which types of blockchain are used. For instance, the consensus mechanism can be different for bitcoin and Hyperledger.

2.3.1 Block

The blockchain facilitates a highly distributed ledger for recording transactions, attributing them to a specific node in a network, and ordering them in time. Data is permanently recorded in the network through files called blocks. A block is a record of some or all of the most recent transactions that have yet to be recorded in prior blocks. The ledger of past transactions is called the blockchain, as it is a chain of blocks [35].

A block consists of *block header* and *block body* [86]. The block header consists of three sets of block metadata. First, there is a reference to a previous block hash, which connects this block to the previous block in the blockchain. The second set of metadata, namely the difficulty, timestamp, and nonce, in the case of bitcoin, relate to the mining competition. The last piece of metadata is the Merkle tree root, a data structure used to efficiently summarize all the transactions in the block [4]. The block body includes a record of all transactions separated into input and output.

2.3.2 Digital Signature

Creating a transaction on the blockchain requires a digital signature to authenticate the transaction. A typical digital signature involves two phases: the signing phase and the

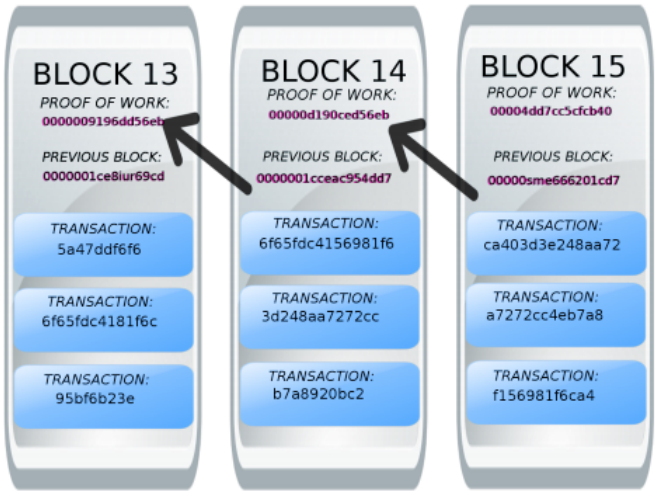

Figure 2.2: Illustration of a Blockchain. Adapted from Block Chain Technologies & The Semantic Web by Mattew English, Retrieved May 25, 2017, From *Technical report, University of Bonn, Germany*

verification phase. For example, when user "Alice" wants to sign a transaction, she first generates a hash value derived from the transaction. She then encrypts this hash value using her private key (confidential to her) and sends another user "Bob" the encrypted hash with the original data (i.e., the transaction). Bob verifies the received transaction through the comparison of the decrypted hash (using Alice's public key) and the hash value derived from the received data by the same hash function as Alice's [86].

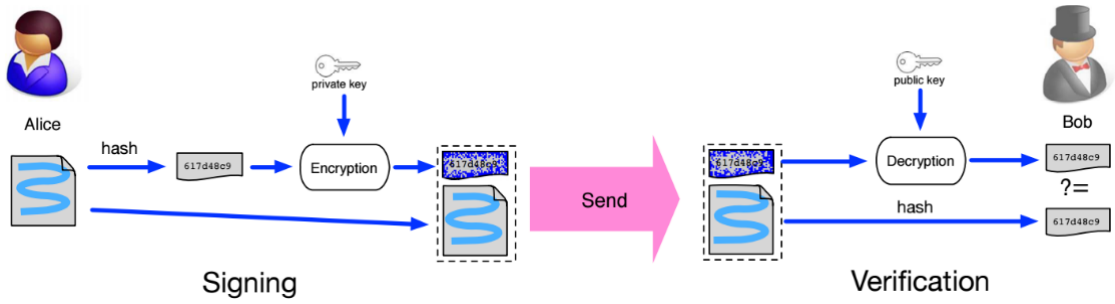

Figure 2.3: Digital Signature Used in Blockchain. Adapted from *Blockchain Challenges and Opportunities: A Survey* by Zibin Zheng et al,. Retrieved May 25, 2017.

2.3.3 Decentralized Network

The interactions among user on blockchain principally use a decentralized network in which each user represents a node at which a blockchain client is installed. When a user

performing a transaction with another user or when a node receives data from another node, it verifies the authenticity of the data. It then broadcasts the validated data to every other node connected to it [86]. Within such a mechanism, the data spreads across the whole network. The benefit of using this mechanism is the centralization of the human factor is minimized and trust shifts from the human agents of a central organization to an open source code [5].

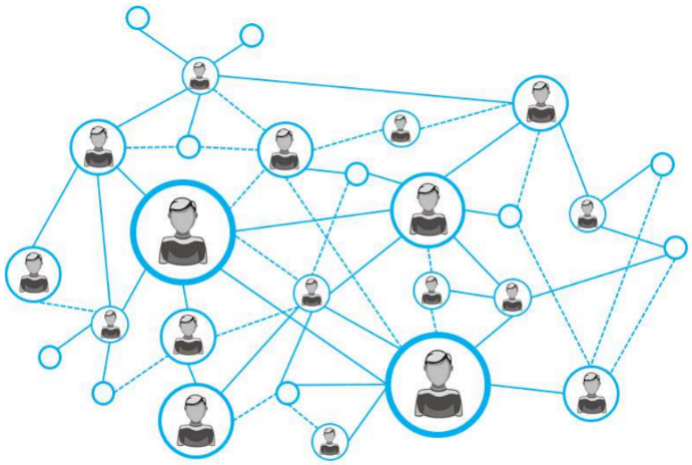

Figure 2.4: Decentralized Network. Adapted from *Blockchain Challenges and Opportunities: A Survey* by Zibin Zheng et al,. Retrieved May 25, 2017.

2.3.4 Network Consensus

Looking into how blockchain works, it requires acceptance and verification by all the users in the network, usually called a consensus. But each node has a different view of the whole network state. Thus, it needs a distributed mechanism to cope with this problem. To reach consensus in distributed mechanism is a substantial challenge for the development of blockchain. Generally, there are four consensus algorithms that can be applied [86].

1. Proof of Work (PoW)
   The PoW consensus algorithm is the most widely used algorithm in blockchain. It was introduced by bitcoin and assumes that all peers vote with their "computing power" by solving PoW instances and constructing the appropriate blocks. Bitcoin, for example, employs a hash-based PoW, which entails finding a nonce value such that when hashed with additional block parameters (e.g., a Merkle hash, the previous block hash), the value of the hash has to be smaller than the current target value. When such a nonce is found, the miner creates the block and forwards it through the network layer to its peers. Other peers in the network can verify the PoW by

computing the hash of the block and checking whether it satisfies the condition of being less than the current target value [39]. To make it simply, consensus requires that the calculated value must be equal to or less than a certain given value.

2. Proof of Stake (PoS)
   The PoS algorithm aims to replace the existing way of achieving consensus in a distributed system; instead of solving the PoW, the node that generates a block has to provide proof that it has access to a certain amount of coins before being accepted by the network [82]. This method requires people to prove ownership of an amount of currency because it is believed that people with more currency would be less likely to attack the network [86]. Therefore, only those who can provide the PoS can participate in the process of maintaining the blockchain. In terms of energy saving, PoS delivers more efficiently on energy consumption compared to PoW.

3. Practical Byzantine Fault Tolerance (PBFT)
   This consensus algorithm was developed to tolerate Byzantine faults, for instance, the arbitrary behavior of the node, joining and quitting the network at any time that usually occurs in a distributed system. This algorithm presents a state machine replication technique to cope with Byzantine faults. Theoretically, it uses a state machine replication algorithm with only one message round trip to execute read-only operations and two to execute read-write operations. Also, it uses an efficient authentication scheme based on message authentication codes during normal operation; public-key cryptography is used only when there are faults [19].

4. Delegated Proof of Stake (DPoS)
   The major difference between PoS and DPoS is that PoS is a direct democratic process, while DPoS is representatively democratic—stakeholders elect delegates to generate and validate a block. With significantly fewer nodes to validate the block, the block can be confirmed quickly, meaning the transaction can be confirmed quickly [86].

2.4 The Application of Blockchain

The implementation of blockchain is going to have a transformative effect on some use case applications. The first blockchain, bitcoin, was developed to enhance the system for financial applications, due to its transparency as a result of its decentralized principle. Later, more varied uses of blockchain were developed for financial applications, such as smart contracts, insurance and crowdfunding. Furthermore, as many people are interested in this new technology, the application of blockchain also currently being developed widely for non-financial services like voting systems for governmental affairs. In this regard, we could divide the use of blockchain into two sectors: financial and non-financial services.

2.4.1 Financial Applications

Digital Payment System. This is basically the core function of bitcoin as digital currency. The birth of bitcoin brought about an evolution in and a disruption of conventional payment systems managed by banks or another financial organizations. A digital currency scheme incorporates both a new decentralized payment system and a new currency. All the schemes exhibit a publicly visible ledger which is shared across a computing network. A key defining feature of each digital currency scheme is the process by which its users come to agree on changes to its ledger (that is, on which transactions are accepted as valid) [31].

Smart Contract. Basically, a smart contract is a computer application that can automatically execute commercial transactions and agreements. It also enforces the obligations of all parties in a contract without the added expense of an intermediary [14]. A smart contract also provides a means for owners of assets to pool their resources and create a corporation on the blockchain, where the articles of incorporation are coded into the contract, clearly spelling out and enforcing the rights of those owner. Associated agency employment contracts could define the decision rights of managers by coding what they could and could not do with corporate resources without ownership permission [79].

Insurance. Any valuable asset or property that is difficult to replicate or destroy can be registered in blockchain. It can verify ownership and trace the transaction history. Everledger is a company that creates a permanent ledger of diamond certifications. The characteristics that uniquely identify the diamond such as height, width, weight, depth, color, etc. are hashed and registered in the ledger [27].

Crowdfunding. Currently, an increase number of startups are implementing cryptocurrency tokens and blockchain protocols as a means of crowdfunding their ventures. The idea is enabling crowdfunding platforms powered by blockchain technology, removing the need for an intermediary third party like Kickstarter or Indiegogo. The startups then raising funds by creating their own digital currencies and selling "cryptographic shares" to early backers [78]. Investors in a crowdfunding campaign receive tokens that represent shares of the startups they support.

2.4.2 Non-Financial Applications

Decentralized Governance Services. Decentralized governance services. The most common use of blockchain in governance services is in the form of a *notary public*. Applying blockchain to notarization secures the privacy of the document, as well as those who seek certification. Publishing proof of publication using the cryptographic hashes of files in the

blockchain takes notary timestamping to a new level [27]. Even the Estonian government, in partnership with the world's first blockchain powered virtual country, *Bitnation*, will start offering a public notary service to their e-residents [67]. Another form of governance service that also adopted blockchain is the online voting system or e-voting. Usually, votes are recorded, managed, counted and checked by a central authority. Blockchain-enabled e-voting (BEV) empowers voters to do these tasks themselves, by allowing them to hold a copy of the voting record. The historic record could then not be changed because other voters could see that the record differs from theirs. Illegitimate votes could not be added, because other voters would be able to scrutinize whether votes were compatible with the rules, perhaps because they had already been counted, or were not associated with a valid voter record [12]. In this way, blockchain technology could encourage transparency in governmental systems.

Decentralized Storage. This concept has been implemented in the health and music industries. For health-related applications, blockchain provides a structure for storing health data or electronic medical records (EMRs) on the blockchain such that they can be analyzed but remain private, with an embedded economic layer to compensate for data contribution and use [78].Taking advantage of the pseudonymous identity coded into a digital address, and its guaranteed privacy mechanism, personal health records could be encoded as digital assets and put on the blockchain just like digital currency. On the other hand, in the music industry blockchain was applied to maintain a comprehensive and accurate distributed database of music ownership rights information in a public ledger. In addition to ownership rights information, the royalty split for each work was also held, as determined by smart contracts [27].

Decentralized IoT. The use of IoT also presents some big challenges. One of these is due to the centralized ecosystem also known as the client/server paradigm. While this model has connected generic computing devices for decades and will continue to support small-scale IoT networks as we see them today, it will not be able to respond to the growing needs of the huge IoT ecosystems of the future. Existing IoT solutions are expensive because of the high infrastructure and maintenance cost associated with centralized clouds, large server farms, and networking equipment [29]. By using a standardized peer-to-peer communication model to process the number of transactions between devices, it will significantly reduce the costs associated with installing and maintaining large centralized data centers and will distribute computation and storage needs across billions of devices that form IoT networks. In partnership with Samsung, IBM has developed ADEPT (Autonomous Decentralized Peer To Peer Telemetry), a platform that uses elements of bitcoin's underlying design to build a distributed network of devices, or decentralized IoT [27].

2.5 The Challenges

There is a lot of excitements surrounding blockchain and the opportunities it offers for both financial and non-financial services. Contrary to expectation, blockchain also has some drawbacks. A lot of work must still be done on the applications and implications of blockchain. Here several challenges that commonly arise in relation to public blockchains are described.

- **Performance**
  When a transaction is being processed, a blockchain has to perform the same tasks a regular database does, but it carries three additional burdens as well [83]:

  1. Signature verification. Every blockchain transaction must be digitally signed using a public-private cryptography scheme. The generation and verification of these signatures is computationally complex. By contrast, in centralized databases, once a connection has been established, there is no need to individually verify every request that comes in.
  2. Consensus mechanisms. In a distributed database such as a blockchain, effort must be expended on ensuring that nodes in the network reach a consensus. Depending on the consensus mechanism, this might involve significant back and forth communication and/or dealing with forks and their consequent rollbacks. While it is true that centralized databases must also contend with conflicting and aborted transactions, these are far less likely where transactions are queued and processed in a single location.
  3. Redundancy. This is not about the performance of an individual node, but the total amount of computation that a blockchain requires. Whereas centralized databases process transactions once (or twice), in a blockchain they must be processed independently by every node in the network, meaning that far more work is done to achieve the same end result.

  It can therefore be assumed that performance issues on blockchain result essentially from shifting the mechanism from being centralized to decentralized. This new mechanism introduces greater complexity in computer processing, such as signature verification, consensus mechanisms, and redundancies. As a result, the processing time can be slower than that for a conventional centralized database.

- **Scalability**
  In public blockchain, scalability is a major issue that developers are encouraged to solve or minimize. This issue is often raised in technical discussions of the bitcoin protocol. Since bitcoin is a self-regulating system that works by discovering blocks at approximate intervals, its highest transaction throughput is effectively capped

at the maximum block size divided by the block interval [26]. However, the main obstacle to blockchain scalability is a tendency toward centralization with a growing blockchain: the larger the blockchain grows, the larger the requirements become for storage, bandwidth, and computational power that must be spent by "full nodes" in the network, leading to a risk of higher centralization if the blockchain becomes so large that only a few nodes are able to process a block [46].

- **Privacy**
  Blockchain can preserve a certain amount of privacy through the public key (an address for each entity) [86]; however, it is shown that blockchain cannot guarantee transactional privacy since the values of all transactions and the balances for each (pseudonymous) public key are publicly visible [51]. Thus, the public nature of the blockchain means private data would flow through every full node fully exposed. The HD wallet has already tackled this problem; it uses an extended public key as the unique index for associating blockchain transactions by giving users the capability to generate as many public keys as they want. Then users can choose to protect their privacy by sending their payments in multiple transactions without requiring any explicit coordination between the sender and the recipient [70].

- **Energy Consumption**
  The creating PoW blocks in a public blockchain consumes a large amount of computational power and with that a large amount of electricity. The computational power is used for this process only, and the results do not have any other benefit than for the sake of the blockchain [77].

2.6 Conclusion

This chapter set out with the aim of assessing the first research sub-question on the definition of blockchain and how it works. The theory underpinning blockchain is a public ledger of all executed transactions. It uses a decentralization principle and encryption involving public and private keys. It works by placing transactions in groups called blocks and linking these blocks through what is called blockchain. From a technical perspective, are three types of blockchain: public, consortium and private. The basic elements are the blocks where the data is stored, digital signatures to authenticate transactions, a decentralized network for user interaction, and a network consensus to verify the transaction. Perhaps the use of this basic elements may very depending on which type of blockchain is used. Looking from business point of view, we could group blockchains into two categories: closed for private or consortium blockchains and open for public blockchains. Both types offer different economic advantages and can lead to different market players for example machines who own themselves that exist in an open blockchain. In the energy market,

closed blockchains helps with the transparency of the market but produce dominant and lock-in effects. On the other hand, open blockchains enable machine-to-machine transactions that could generate disruptive changes.

At first blockchain technology is commonly seen as the main technological innovation of bitcoin. Today, this technology has more advanced practical implementations than bitcoin. These range from financial application, including digital payment systems, smart contracts, insurance, and crowdfunding, to non-financial applications, such as governmental services, decentralized storage, and decentralized IoT.

Chapter 3

Digital Identity Management

3.1 The Concept and Properties of Digital Identity

The identity concept can be seen from different perspectives and is applicable in different domains, depending on the objective for which digital identity is used. In general, personal identity in philosophy refers to the answer to the question, 'Who am I?' It consists roughly of those properties that make the individual unique and different from others [65]. Precisely, identity refers to a set of qualities and characteristics that make an entity definable, distinguishable, and recognizable compared to other entities [6]. However, in the digital world, "identity" is a set of digital records that represents a user. These records are saved and managed in a standard format by entities that provide the identity information or assurances needed to complete transactions. A digital identity also accepts and integrates new records to create a rich view of the user [36]. Following are five properties which should be applied to contribute in more detailed and provisioning solution of a digital identity system.

1. **Entities**
   According to its definition, an entity is an object that exist or has its own independence existence. Entity conduct as representation from unit which bears the legal rights for the system, e.g., individuals, businesses, and affiliates. In a digital system, some types of entities require digital identities, including people, machines or devices, organizations, codes, and agents. Those entities can be specifically categorized into three types [75]. *Locally-installed identity agents* run on devices that are with the user, like smartphones and laptops. *Remote identity agents* reside on the network. They have their own private and public keys and can be run by parties that have certain user credentials, such as banks, universities, or other entities that are trusted by the user. The last type consists of *Relying parties*, which represent a party with which a user intends to interact, essentially, an online service provider; however, in

a peer-to-peer system, relying parties can be other users.

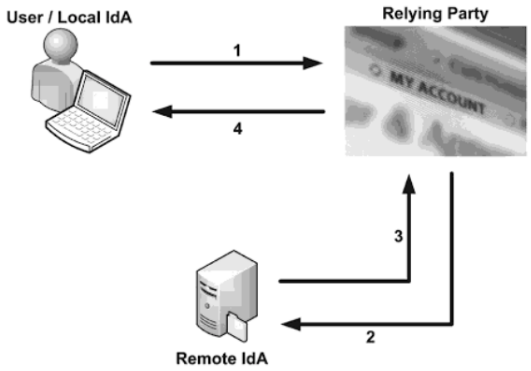

Figure 3.1: Entity Communication Sequence. Adapted from *Digital Identity and Access Management: Technologies and Frameworks* by Raj Sharman. Retrieved May 18, 2017.

2. **Attribute Type**
   The attribute type is used to identify the entity. It commonly consists of three attributes [85] ; *who you are*, *context*, and *profile*.

   Who you are. This is the attribute that uniquely identifies a single entity in a real-world context. It can include knowledge or data that is only know by that entity, unique physical characteristic of that entity, or items that the entity possesses.

   Context. This can refer to the type of transaction or organization that the entity identifies itself as, as well as the manner in which the transaction is made. Different constraints on digital identity maybe implemented depending on the context. For instance, transferring sensitive information relating to birth certificates over phone or the internet maybe prohibited. Context is also used to determine the amount and type of identity information that is needed in order to provide the appropriate level of trust. For example, in an email context, the amount of identifying information necessary is usually only two things: a username and password.

   Profile. A profile consists of the data needed to provide services to users once their identity has been verified. User profiles can include what entities can do, what they have subscribe to, what groups they are members of, their selected services, etc. A user's profile can change during the course of an interaction with the service provider.

3. **Lifecycle**
   There are three fundamental steps to creating digital identity [25]: *registration*, in-

cluding enrollment and validation; *issuance* of documents or credentials; and *authentication* for service delivery or transactions.

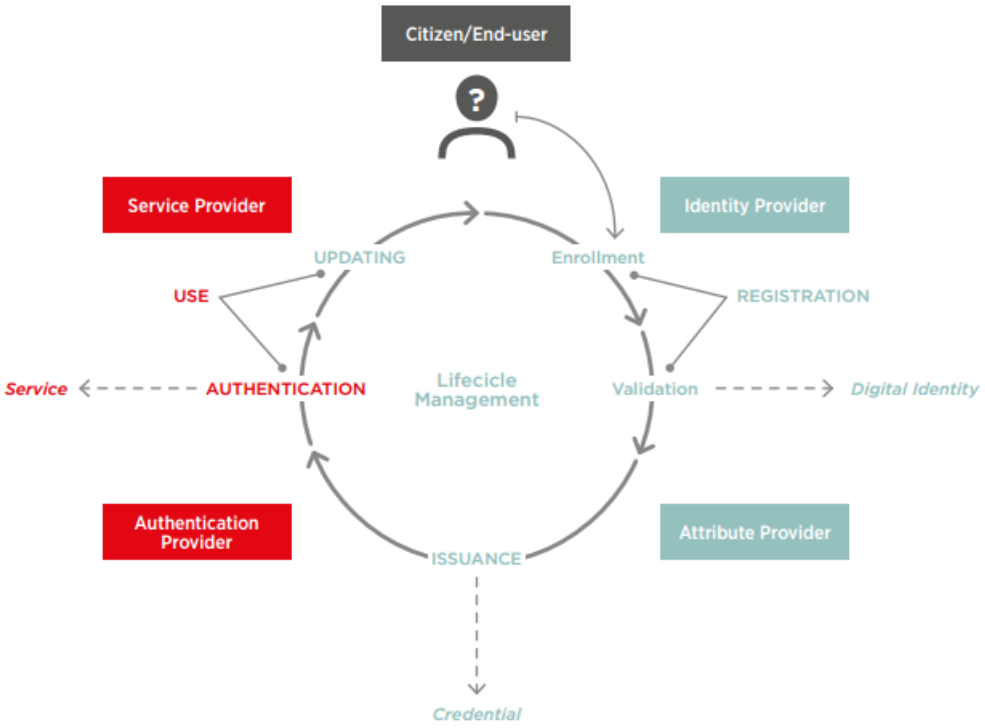

Figure 3.2: Digital Identity Life Cycle. Adapted from *Discussion Paper : Digital Identity Towards Shared Principles for Public and Private Sector Cooperation* by World Bank Group, GSMA, Secure Identity Alliance. Retrieved May 20, 2017.

Enrollment. This stage is divided into two parts: enrollment and validation. Enrollment entails registration steps: capturing and recording key identity attributes of a person who claims a certain identity. This may include biographical data (e.g., name, date of birth, gender, address, email), biometrics (e.g., fingerprints, iris scan), and the other attributes. Once a person has claimed an identity during enrollment, this identity is then validated by checking the presented attributes against existing data.

Issuance. Before it can be used by a person, a registered identity goes through an issuance or credentialing process. For an identity to be considered digital, the credentials or certificates (e.g., birth certificate, passport) issued must be electronic, in the sense that they store and communicate data electronically. Types of electronic credentials including smartcards, 2D barcode card, mobile identity, and identity in the cloud.

Authentication. After users have been registered and credentialed, they can use their digital identities to access public or private services. For instance, citizens may use their eID number to pay their taxes through an online portal, while bank customers can use smart debit cards or mobile financial services. In order to access services, the user must be authenticated using one or more factors, for example, password, pin, or fingerprint.

During the lifecycle stages, digital identity providers manage and organize the identity system, including its facilities and staff, record keeping, compliance and auditing, and updating the status and content of digital identities. For example, users may need to update various identity attributes, such as address, marital status, profession, etc. In addition, identity providers may need to revoke an identity, which involves invalidating the digital identity for either fraud or security reasons, or terminate an identity in the case of the individual's death.

4. **Policies**
   Policies are used to manage the identities. This is a set of rules, defined by the resource owner, for managing access to a resource (asset, service, or entity) and for what purposes it may be used. The level of access is conditioned not only by the identity, but is also likely constrained by a number of further security considerations, such as the company policy, the location (i.e., inside a secure corporate environment, connected via a hotspot, or an internet cafe, and others), or the time of day.

5. **Technology**
   To ensure usability, security, and privacy, digital identities must be implemented using advanced technical methods. Therefore, technology must be applied in at least three areas: authentication, security protocols, and storage improvements.

Authentication Technique. Authentication technique. The authentication techniques range from single factor to multi-factor authentication. Below is a list of common methods used in authentication systems:

- Password or personal identification number (PIN)
  Password authentication is a traditional method in which the user is provided with a username and password. However, many have shown this technique to be ineffective since the username and password are often easy to guess or steal. In order to make the authentication process more secure, an advanced form of password usage called a one-time password (OTP) is used. The user only enters the password once and must request another from the server at the next attempt to log in or make a transaction. This advanced methods involves hashing and the techniques and data are then exchanged with the server and stored [75].The PIN technique basically has the same mechanism as a password, but it consists of a

numeric term only (usually with four to six digits). A PIN-based authentication mechanism is commonly used for financial services such as ATM banking and credit card payments.

- Token
  This works using the two-factor authentication (2FA) principle. Instead of using a username and password, a level is added on to obtain time-limited token (typically a cryptographic key or password) that is used for further transactions during the session. Generally, it has a physical display, and the authenticating user simply enters the displayed number to log in. The physical device for tokens mostly does not require an internet connection because it communicates using mobile telecommunication service operator services such as voice calls, SMS, or USSD .
- Public key cryptography
  This method utilizes cryptographic mechanisms that, as their underlying theory, engage an asymmetric key pair: a public key and a private key [20]. Public-key encryption uses that key pair for encryption and decryption. The public-key is made public and is distributed widely and freely. The private-key is never distributed and must be kept secret.

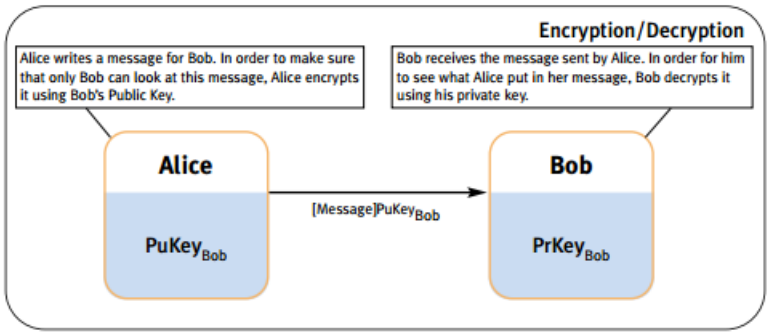

Figure 3.3: Encryption/Decryption Principle. Adapted from *Public Key Encryption And Digital Signature - How Do They Work?* by CGI Group (2014). URL : *https://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf*. Retrieved May 22, 2017.

- Biometric
  Biometric authentication requires a completely different style of authentication process. Biometric authentication, or just biometrics, is the process of making sure that people are who they claim to be. This approach is based on a person's biological uniqueness and it can be used for the biometric identification of a person [7], using, for example, fingerprint or iris recognition. A pattern-matching technique is essential for measuring the characteristic. Biometrics also require sensor devices to collect the characteristic from the user.

- Smart Card
  When used for logical access, smart card technology typically comes in two forms: a credit-card-sized plastic card or a USB device, each with an embedded computer chip [53]. Using a smart card to store password files is its simplest application.

Security Protocols. These are valued for their strong identity verification and authentication attributes. Specifically, they are designed to transfer authentication data between two entities. The widespread authentication protocols used to address security issues within open networks are Secure Sockets Layer (SSL), IP Sec, Secure Shell (SSH), and Kerberos [33].

Storage. New technologies contributing to storage improvement hold considerable implications for the creation of robust digital identity systems. There are two new technologies that may offer improved methods in database storage [36]. The first is distributed ledger technology, or blockchain combined with encryption and cloud storage, and this allows information to be held and transferred point-to-point in a dispersed, immutable network. The second consists of federated identity standards, such as SAML 2.0, which create interoperability between identity management networks and external applications, allowing federated identity systems to scale to accommodate large numbers of identity providers and relying parties.

Recently, there has been an increasing emphasis on additional functionalities such as single-sign on (SSO) authentication. This system allows users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards [28]. Those applications are transferred and managed from remote distributed systems with different characteristics and access control methods. This system serves different purposes [61]. It communicates between applications and the network, it enables communication to applications that are connected by the internet using web resources, and it integrates different domains with different sets of credentials located all over the world. The aim of using SSO is to improve the communication and security of user authentication and access permission verification and also to decrease the management costs [18]. Popular examples of SSO systems are found at Google, Microsoft, and Yahoo; they provide SSO to their users when accessing emails, groups, documents and other facilities embedded in their SSO system.

3.2 The Roles of Digital Identity Management

The illustration below indicates that digital identity is not just a straightforward technique to deliver authentication and access control, but is more like a complex flow of information within the trusted framework [68]. Furthermore, identity management is also a critical building block for information security. It forms the basis for most types of access control and for establishing accountability online. Thus, it contributes to the protection of privacy by reducing the risks of unauthorized access to personal information, data breaches, and identity theft [76].

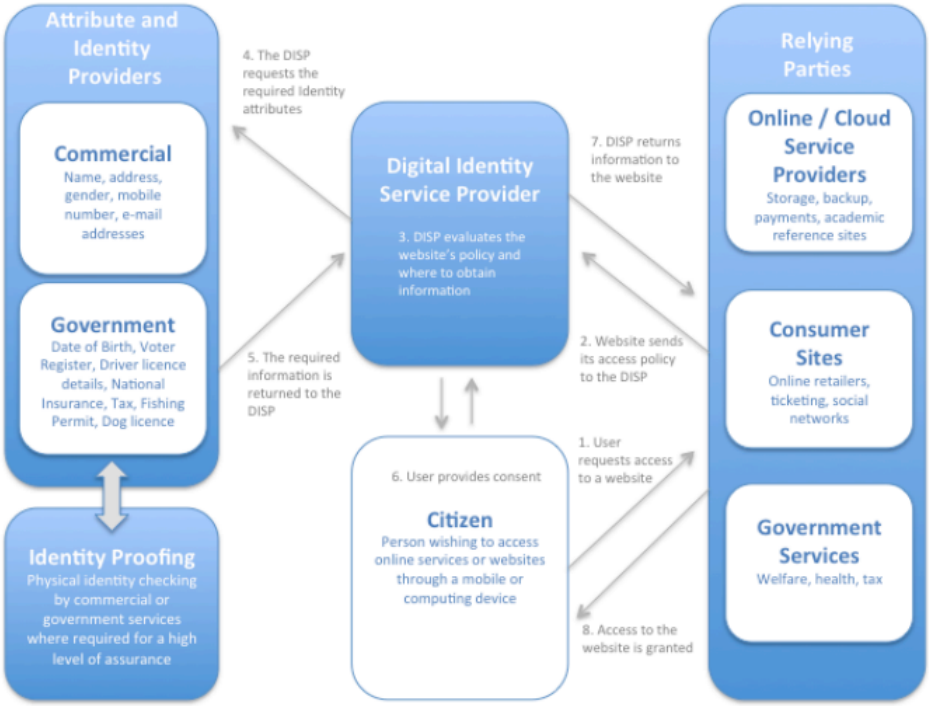

Figure 3.4: Website Access Using Digital Identity. Adapted from *Digital Identity : An Introduction* by Piran Partners, URL : *http://piranpartners.com/wp-content/uploads/2014/12/An-Introduction-to-Digital-Identity.pdf*. Retrieved May 18, 2017.

In the physical world, identity management helps address the risks associated with human interactions and increases confidence between the interacting parties. It is therefore fundamental to economic and social life. The same is true online, where the lack of a demonstrable link between a physical person and a digital identity can create additional uncertainties that do not exist offline [63].

3.3 The Categories of Digital Identity Management

There are three categories of digital identity management which are widely available [41]: *federated*, *user centric*, and *hybrid*. This section only discusses conceptual knowledge of each of these categories, while the implementations from real-world examples are presented in Chapter 5.

1. **Federated identity managament**
   Federated identity management allows users to access multiple services based on a single authentication [48]. Conceptually, it involves a group of organizations setting up a trust relationships that allows them to share assertions about user identities, in order to grant users access to their resources [21]. The user signs up once to access all of the services offered by different partners across the federated enterprise. Federated identity architecture (FIA) essentially consists of an identity provider (IdP) and a service provider (SP) [38]. The IdP manages the identity of the user and performs the authentication process in order to validate the user's identity. The SP provides one or more services to users within the federation.

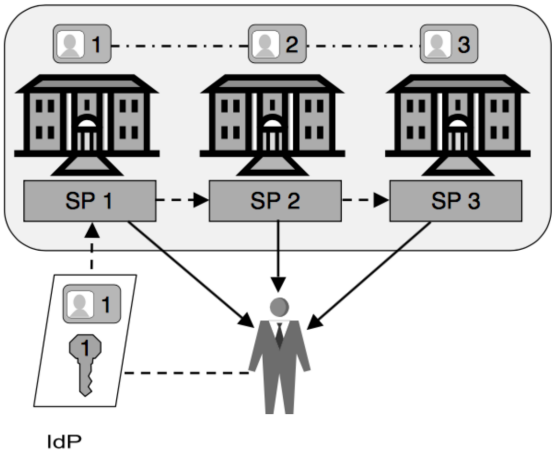

Figure 3.5: Federated Identity Model. Adapted from *User Centric Identity Management* by Audun Jøsang and Simon Pope. Retrieved May 26, 2017.

2. **User Centric Identity**
   In this system, users are able to choose which of their identities to use for each application. It allows users to store identifiers and credentials for different service providers in a single tamper-resistant hardware device, which could be a smart card or some other portable personal device [47]. This user-centric model can be distinguished from the federated model since it is more likely to focus on which users are in the context than the organizations or enterprises. A further practical advancement of this type of system is *attribute-based identity*. This approach aims to solve

security- and privacy-related problems by using an attribute-based credentials (ABC) technique. The ABC technology takes a different view of identity and authorization; it enables attributes to be issued and stored with the data subject (the individual). Moreover, only the relevant and often non-identifying subset of these attributes needs to be shown in the context of a particular verification and authorization instance. The individual cannot change his or her attribute values; this provides assurance to systems that use ABC to make access decisions [3].

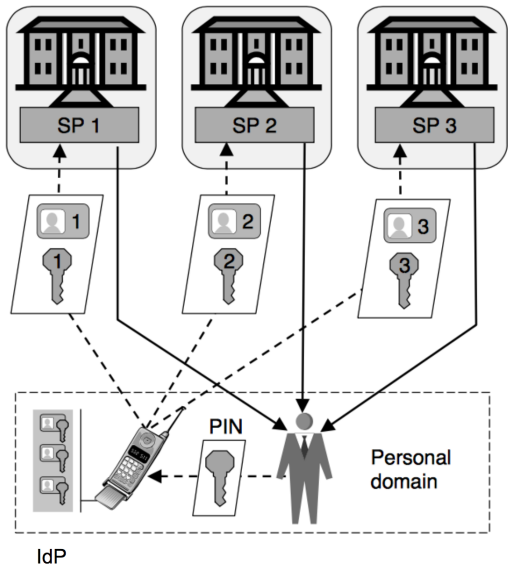

Figure 3.6: User-centric Identity Model. Adapted from *User Centric Identity Management* by Audun Jøsang and Simon Pope. Retrieved May 26, 2017.

3. **Hybrid Identity Management**
   This approach provides an alternative when both federated and user-centric approaches do not readily cope with certain circumstances. For instance, in healthcare scenarios, attribute exchange and delegation processes cannot be completely user-centric, since in cases of critical accidents, users cannot give their consent. On the other hand, federated models raise privacy concerns since medical records may be available to every entity within the circle of trust, even if there is no emergency. Hence, the proposed hybrid model allows users to configure and track access to their medical records, while the identity providers store and manage user credentials [73].

3.4 The Challenges

Talking about the challenges, most identity management technologies suffer from a set problems principally caused by the legacy architectural approach and the lack of se-

curity and privacy features in current technologies. The most severe current problems are summarized as follows [74]:

Global identifiers. Many systems use global identifiers to identify users, such as social security numbers, URLs, or e-mail addresses. Global identifiers allow different sites to correlate information about users, which usually allows sites to gain more information than was specifically allowed by the user.

Insecure workstations. The typical workstation used by a user for internet access is not a secure environment. Viruses and other malware can easily infect the workstation and gain control over all the user's activities. While the workstation is under malware control, the user's activity can easily be tracked, entered passwords can be observed, and even complex man-in-the-middle attacks can be mounted against strong authentication mechanisms. Many government digital signature schemes can also be subverted using client-side malware.

Honeypot effect. Centralizing personal information may be very convenient from a data-management perspective, but such a repository creates a very attractive target for attackers. The effect is the same whether the information is stored on governmental servers, hosted by internet identity providers, or kept on the user's workstation.

3.5 Conclusion

Digital identity management relates individuals to their respective online identities. It consists of several properties: entities, attributes, lifecycle, policies, and technologies. These properties contribute to a more detailed and provisioning solution for deploying digital identity management. The role of digital identity is a critical element of information security; it forms the basis for most types of access control and for establishing accountability online. Thus, it contributes to the protection of privacy by reducing the risks of unauthorized access to personal information, data breaches, and identity theft.

Digital identity solutions can be categorized into three types: federated, user-centric, and hybrid. Each category has different schemes and architectural options. Federated identity allows a group of organizations to establish a trust by developing a digital identity management system for their alliance; however, this category still relies on a centralized mechanism. In order to move closer to the user by letting them to choose which identities to use for different applications, user-centric identity has been proposed. This system focuses particularly on the user context rather than the organization or enterprise. The last

type is hybrid identity management. This provides flexibility due to certain circumstances on the system and ambidextrous behavior between federated and user centric identity.

Chapter 4

Digital Identity on Blockchain

Digital identity is critical in many business and social transactions. However most recent conventional identity systems are costly and hinder the innovation and greater customer experience. By using blockchain, it introduces a new way of managing the identities. This chapter examines the core characteristics that blockchain had : self-sovereign identity and handshake mechanism. These characteristics are what makes blockchain differs from another identity solutions. It also presents the current implementation of blockchain-based digital identity from some companies.

4.1 Self-Sovereign Identity

Blockchain has the potential to be adopted as a digital identity system. Instead of storing all data and transactions in a secure and open way, creating an identity on the blockchain makes it easier for people to manage their identities and to grant control over who has their personal information and how they access it. This is called self-sovereign identity (SSI). There are 10 specific principle which attempt to ensure the user control that is at the heart of SSI [2];

1. Existence
   Users must have an independent existence. Any SSI is ultimately based on the ineffable "I" that is at the heart of an identity. It can never exist in a wholly digital form. This must be the kernel of self that is upheld and supported. An SSI simply makes public and accessible some limited aspects of the “I” that already exists.

2. Control
   Users must be in control of their identities. They should always be able to refer, update, or hide them.

3. Access
   Users should have direct access to their own identities and all related data. All data must be visible and accessible without gatekeepers.

4. Transparency.
   Systems and algorithms must be transparent. The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated.

5. Persistence
   Identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity should remain. In the fast-moving world of the internet, this goal may not be entirely reasonable, so it is a minimum requirement that the identities should last until they are replaced by newer identity systems.

6. Portability
   All information about identities must be transportable. The identity must not be held by a single third party.

7. Interoperability
   Identities should be as widely usable as possible. Regimes may change, users may move to different jurisdictions, but transportable identities ensure that users remain in control of their identities regardless of this, and this can also improve an identity's persistence over time.

8. Consent
   Users must agree to the use of their identities and the sharing of all related data. Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs.

9. Minimization
   The disclosure of claims must be minimized. When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed.

10. Protection
    The rights of users must be protected; when there is conflict between the needs of the network and the rights of entities, the priority should be the latter.

Aside from SSI, according to WEF 2016, blockchain also promises some key features that hold great potential for identity systems: low transaction costs, immutability, and convenience.

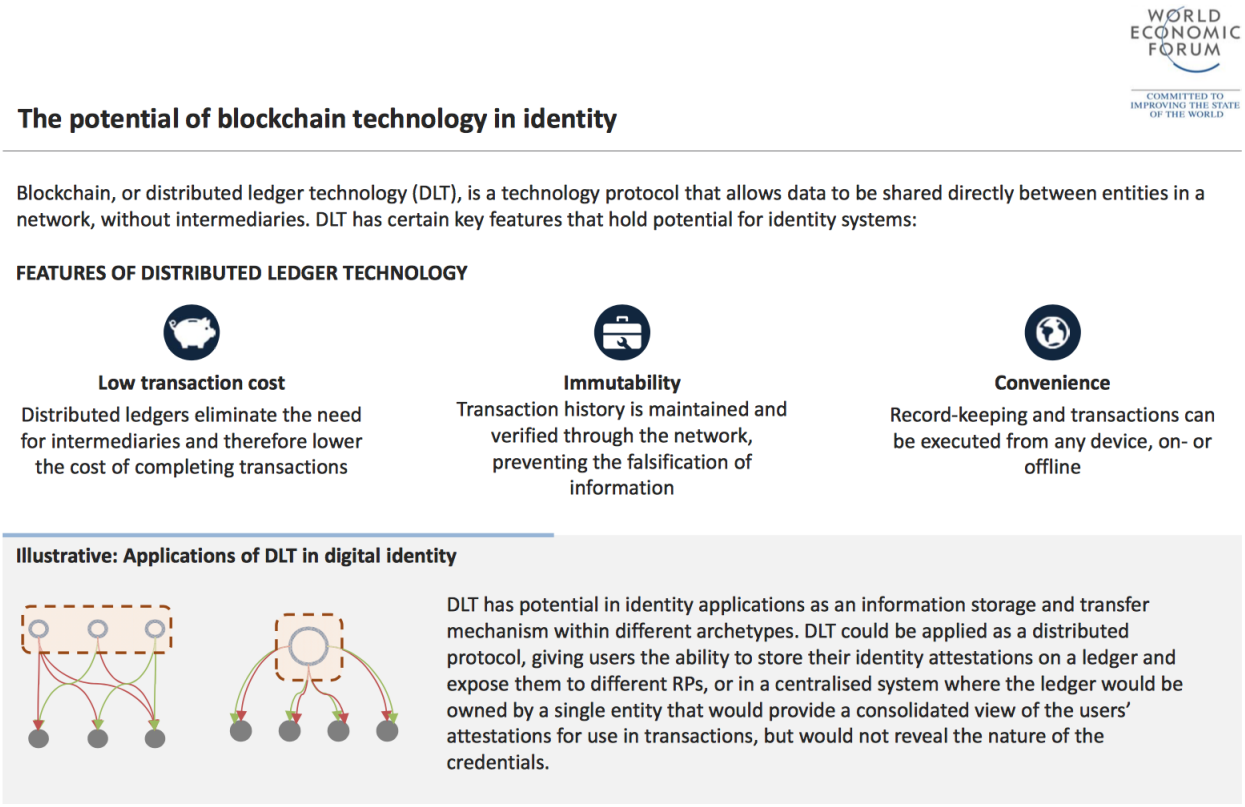

Figure 4.1: The Potential of Blockchain for Identity. Adapted from *A Blueprint for Digital Identity : The Role of Financial Institutions in Building Digital Identity* by World Economic Forum 2016. Retrieved May 26, 2017.

4.2 Handshake Mechanism

Blockchain introduces cryptography procedures that occur in the digital identity system. The critical process underlying an authentication mechanism is called a *handshake mechanism* [32]. This mechanism eliminates the need for a third party to provide authentication by constructing a direct interaction between the user and the service provider. service provider can be a protected app that requests the service. The mechanism can then be divided into three main steps:

Login. In this first step, instead of using a username and a password for login, the app uses a QR code as an authentication method, since using QR codes makes it easier to encoded the authentication request. The next step is to verify the request and create the response.

Verify Request. This step contains procedures that ensure authentication. First, the public key cryptography is completed to verify that the request data is legitimate and that the app is what the user is expecting to use. It allows the app to sign the request, which is then published, either through blockchain or a certificate authority[1]. To support a simple transition, it begins with the certificate authority system used in TLS for HTTS. Then it transitions into a full blockchain authentication by creating an app-identity on the blockchain. After that, the user clicks a "verify login" button.

Create response. The last stage is to create a response after the user clicks the "verify login" button. After this action, the app creates a response, signs it, and then sends it back to the user through a specified route on the app. This request is then verified using a PKI on the protected app and the user is then logged in.

4.3 The Implementation of Blockchain-based Digital Identity

Some companies have been pioneering the development of blockchain-based digital identity management and authentication. Below are several implementation solutions grouped by the types of blockchain used as the underlying technology for developing digital identity systems [59]:

1. Closed Blockchain (private or consortium)
   Digital identity which built in a private or consortium blockchain, will generally set up a permissioned network. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Only the entities participating in a particular transaction will have knowledge and access to it — other entities will have no access to it.

   - uPort
     This was developed by ConsenSys using Ethereum, which consists of three main components: smart contracts, developer libraries, and a mobile app. The user's

[1] A certificate authority (CA) is a trusted entity that issues electronic documents that verify a digital entity's identity on the Internet

key is saved in a mobile app. Ethereum smart contracts form the core of the identity and contain the logic that lets users recover their identities if their mobile device is lost. Finally, the developer libraries allow third-party app developers to integrate support for uPort into their apps.

- Microsoft Decentralized Identity Foundation (DIF)
  Microsoft has developed a foundation for building an open-source decentralized identity ecosystem for people, organizations, apps, and devices. It uses four pillars in a new ecosystem: decentralized identities, blockchain identity, zero trust data stores, and being universally discoverable.
- Cambridge Blockchain LLC
  This platform was developed in order to allow financial institutions to meet the strictest new data privacy rules, eliminate redundant identity compliance checks, and improve the customer experience. By combining blockchain technology with an off-chain personal data service, they created an independent source of truth through the network effects of transactions between individuals and trusted parties.
- Netki
  Netki provides open-source and open-standard based digital identity solutions that allow financial service companies to meet their compliance requirements on both public and private blockchains. Netki Wallet Name Service (WNS) translates easy-to-remember names like "wallet.myname.me" into bitcoin (and other cryptocurrency) wallet addresses.
- KYC-Chain
  This is a novel platform built with the convenience and security of DLT, allowing users to manage their digital identity securely, while businesses and financial institutions are able to manage customer data in a reliable and easy manner.
- HYPR
  HYPR provides decentralized biometric authentication to secure users across mobile, desktop, and IoT systems. It enhances the user experience by allowing users to choose from voice, face, touch, and eye recognition. By using biometric authentication, data breach fraud can be avoided.
- Guardtime's BLT
  This is a blockchain standard for digital identity, an authentication and signature protocol intended to replace RSA as the standard for digital signatures. In contrast to the RSA's reliance on quantum-vulnerable asymmetric key cryptography, BLT is based on Guardtime's quantum-secure Keyless Signature Infrastructure (KSI) technology, which uses only hash-function cryptography.
- Evernym
  Evernym is developing a sophisticated identity platform built on Sovrin, a

private-sector, international non-profit that was established to govern the world's first SSI network. These tools and products are designed by the same team that created Sovrin to significantly ease the deployment and integration of SSI infrastructure in many different industries.

2. Open Blockchain (Public)
   A public blockchain network is completely open and anyone can join and participate in the network. The digital identity in open blockchain typically has an incentivizing mechanism to encourage more participants to join the network.

   - ShoCard
     This easy-to-use digital identity built on a public blockchain data layer means that companies do not own the user data. A user's identity is encrypted, hashed, and then written to the blockchain, where it can be called up when needed. Users, in effect, give banks temporary access to the private side of this blockchain record in order to verify identity. Once that is completed, the bank creates its own record which can be consulted in the future to determine that a certain individual is who they claim to be.
   - UniquID
     This provides identity management, integrated with fingerprint and other biometrics, on personal devices. Ready to be deployed in custom hardware, servers, personal computers, smartphones, or tablets, UniquID Wallet also runs on battery- and low-powered devices, providing integrity and interoperability at the edge of one's infrastructure.
   - Bitnation
     This is a governance 2.0 platform powered by blockchain technology. Its goal is to provide the same services that governments provide, but in a decentralized and voluntary manner, unbound by geography. Bitnation has worked out identification solutions such as blockchain passports and marriage certificates.
   - Civic
     Civic's identity verification and protection tools give both businesses and individuals the power to control and protect their identities through the blockchain. They allow users to register and validate their personal identity information and lock their identities in order to prevent identity theft and fraudulent activity on their credit reports.
   - ExistenceID
     This allows users to create a digital identity capsule to store their documents, , somewhat like Dropbox, but with a much higher level of security. Each user account is completely self-authenticated and zero-knowledge of the user's personal account. Identity documents saved to a digital identity capsule are encrypted

and uploaded to the safe network, a secure decentralized data management service.

- Open Identity Exchange (OIX)
  This is a non-profit, technology agnostic, collaborative cross-sector membership organization with the goal of accelerating the adoption of digital identity services based on open standards. They publish white papers to deliver value to the identity ecosystem as whole.
- Cryptid
  Cryptid is the next generation of identification. Current identification methods such as state-issued driver's licenses are insecure and easily tampered with. Cryptid eliminates the possibility of counterfeit identification by adding factors of identification and encryption that are backed by a distributed, global network. All of the data is encrypted with the provided password, after which it is permanently transferred to the blockchain. The customer is then given a unique identification number that points to the information on the blockchain and can be stored on almost anything from magnetic strips to QR codes.

4.4 Conclusion

For digital identity, blockchain supports the implementation of SSI and incorporates ten principles (existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and protection) which strengthen its application. As a decentralized public ledger, blockchain enables users to control their own data without third-party involvement. Unlike other common digital identity systems, the authentication process on blockchain-based system requires a different mechanism, that is, the handshake mechanism. This requires a three-step process: login, verify request, and create response. Some applications have been developed for blockchain-based identity management and authentication. They can be divided based on what type of blockchain that has been used. For instance in closed blockchain there are uPort, Microsoft DIF, Cambridge Blockchain LLC, Netki, KYC-Chain, HYPR, Guardstime's BLT and Evernym. And in open blockchain there are ShoCard, UniquID, Bitnation, Civic, ExistenceID, Open Identity Exchange and Cryptid.

Chapter 5

The Comparison of Digital Identity Categories

A key aspect of examining digital identity categories in order to identify which is most suitably applied to this context is a comparison of each of them based on three characteristics: implementation, advantages, and disadvantages.

5.1 The Implementation of Digital Identity Categories in a Closed Model

As we discussed before, the notion of closed model related to the use of system in an intranet network. Surprisingly, most of the current applications inherent the adoption of closed model since there are many companies which created a business application for digital identity solution. The chosen digital identity management category depends on the product or services that a given company offers. The identity marketplace delivers data mining analysis through machine learning algorithms to predict future economic and societal trends, in this way redefining financial evaluations [71]. There is also increasing collaboration between governments, information technologies companies or group of companies constituting a consortium.

1. **Federated identity**
   In the business world, federated identity also known as generic identity. This solution evolved from a client-server style to a cloud-service style and uses web applications, since many companies want to share resources with their partners [66]. Therefore, this technology is used to create a globally interoperable online business identity, driving relationships or affinity-driven business models between companies [13]. Looking at the history, the FIA initiatives based on the client-server model are [38] Liberty

Alliance[1], Shibboleth[2], and WS-Federation[3]. Some big companies such as Microsoft and IBM have developed their own solutions for federated identity frameworks, for example, Microsoft Azure Access Control Service and IBM Tivoli Security Solution. Even the most federated identity system provides SSO, and practically the solution can be divided on three areas [13]:

- Web-based Single Sign-on - Federated Single Sign-on referred to as F-SSO
- Application-based web services security: secure web services referred to as web services security management
- Identity life cycle: federated provisioning

Since this solution was developed as partnership-based solution for a federation (collaborating companies), federated identity management always refers to company agreements, such as the set of business agreements, technical agreements, and policies that enables companies to lower their overall identity management costs, improve user experience, and mitigate security risks for its implementation, especially on web service-based interactions like F-SSO and web service security.

2. **User-centric identity**
   User-centric identity management has recently taken on the role of handling private and critical attributes that cannot be handled on federated identity systems. In federated identity, the attribute is owned and managed by a group of organizations. This interpretation contrasts with the idea of user-centric identity which allows users to control their own digital identities. Furthermore, looking at the implementation of these, current works focus on the interoperability architecture between identity management systems, while there is limited implementation analysis on portability issues related to IoT or various computer access and secure manners [1]. Popular technologies include OpenID, Attribute-based credentials (ABC), and Information Card [75].
   OpenID is based on the action of verifying the ownership of a resource. This resource is in the form of a publicly available uniform resource locator (URL), specifically, a HTTP- or HTTPS-based URL [60]. The end-user interacts with a relying party (such as a website) that provides an option to specify an OpenID for the purposes of authentication; an end-user typically has previously registered an OpenID (e.g. yourname.openid.example.org) with an OpenID provider (e.g. openid.example.org) [34].

   On the other hand, in the ABC technique, identity information can be categorized into attributes that are stored in the cryptographic container. One of the attributes

[1]Liberty Alliance, a group of more than 200 companies and was launched in 2001
[2]Shibboleth, an academic initiative of university members of Internet 2
[3]WS-Federation, an important component within the secure framework architecture for Web Services.

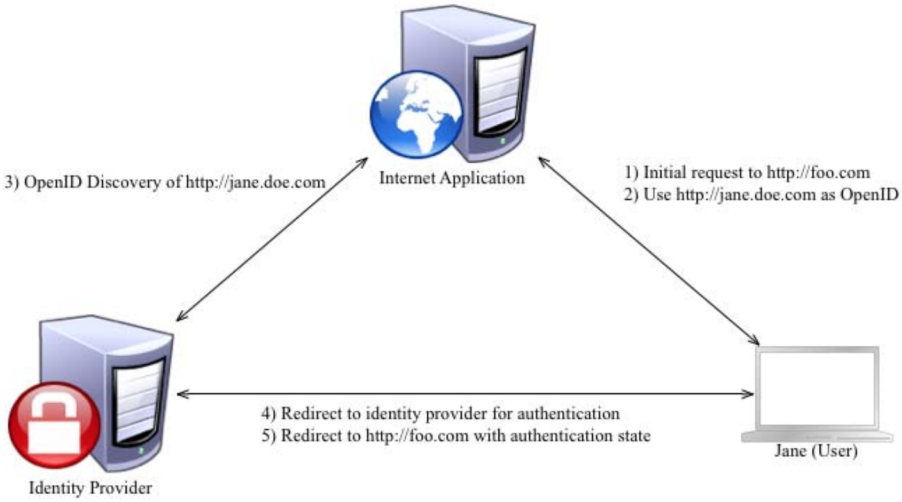

Figure 5.1: OpenID Authentication Steps. Adapted from *An analysis of user-centric identity technology trends, openid's firstact* by Peter Motykowski. Retrieved June 12, 2017.

is a secret key that is only known to the user's device. The ABC components can be described as [3] the credential's name, the secret key, the pairs of attribute names and values, the issuer's identity, and the issuer's signature. In an ABC ecosystem, there are at least four types of operational participant: the user, the card provider, the issuer, and the verifier. The process includes card provisioning, verification, and credential issuance. An ABC card is primarily used as a tool for authorization while the digital content of an ABC card can be dynamic.

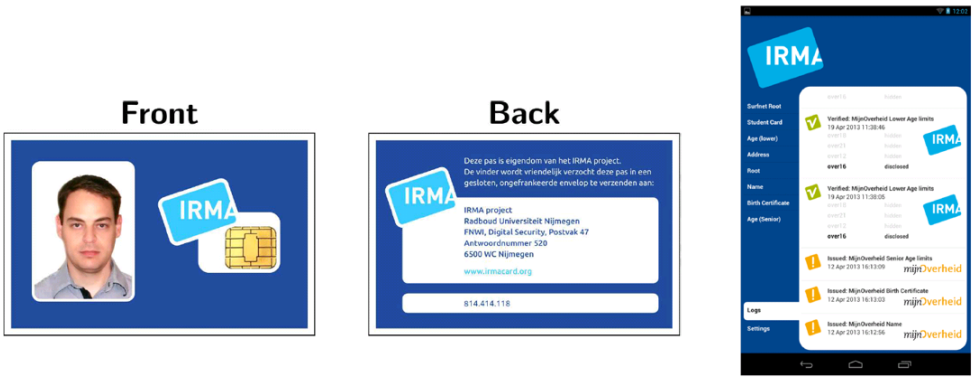

Figure 5.2: An example of an ABC card and mobile app for card identity management within the IRMA project. Adapted from *Attribute-based Identity Management* by Gergely Alpar. Retrieved June 24, 2017.

3. **Hybrid identity**

Hybrid identity management not only deals with user identities but also with device identities. Due to the emerging area of cloud services, this hybrid model is more critical for implementation because of its support for factors such as interoperability and privacy [55]. Microsoft designed software specifically to support a hybrid identity model: Microsoft Azure Active Directory (AD), which provides a powerful set of hybrid identity solutions [45] that connect to hundreds of cloud-based applications. The basic architecture principle for Azure AD is that it separates the data center boundary into two parts: primary replica and secondary replica [57]. The primary replica receives all directory writes and the secondary replica is responsible for directory reads. Additionally, Azure AD can be integrated with an existing Windows server AD[4], giving organizations the ability to leverage their existing on-premises identity investments to manage access to cloud-based SaaS applications.[5]. Another implementation sample can be derived from hybrid identity management for healthcare systems. The motivation for this is that the existing identity management technologies are not ready to cope with user consent revocation in an appropriate way. This is a relevant issue with regard to privacy-enhancing mechanisms, especially in some cases when sensitive data and profiles are shared. In a healthcare scenario, the system must protect the user's privacy and allow authorized entities (including humans) to access medical records conveniently. Moreover, privileges permitting access to user attributes should be revoked in an effective way [73]. Thus, hybrid identity could provide a more flexible user consent-revocation mechanism in healthcare scenarios.

5.2 The Implementation of Digital Identity Categories in an Open Model

The notion of an open model as the vision of future energy systems depends on the mechanisms of autonomous machines such as the self-driving car. Basically, it constitutes a combination of the concepts of AI and IoT, in which everything will be connected to the internet in order to provide services autonomously. The Oxford English Dictionary [6] provides a concise definition of IoT: *"internet of things (noun): the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data"*. In this sense, IoT represents the convergence of a variety of computing and connectivity trends that have been evolving for many decades. At present, a wide range of industry sectors, including automotive, healthcare, manufacturing, home and consumer

[4]Windows Server Active Directory is as directory service for Windows domain networks

[5]SaaS or Software as a service is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).

[6]"Internet of Things." Oxford Dictionaries, n.d. Web. 18 June. 2016.
http://www.oxforddictionaries.com/us/definition/american$_e nglish/Internet - of - things$

electronics, and many others, are considering the potential for incorporating IoT technology into their products, services, and operations [72]. This new paradigm is introducing new alternatives for digital identity management which operate on a global scale. Therefore, in this chapter, digital identity management is discussed in the context of the concept of IoT, in which its role is expanding. It is no longer just about identifying people and managing their access to different types of data, but it must be able to identify devices, sensors, monitors, and manage access to sensitive and non-sensitive data.

1. **Federated identity**
   An IoT network can consist of some IoT cluster and inter-cluster communication. Device-to-device communication within the cluster can be carried by WiFi, bluetooth, Radio Frequency Identification (RFID), etc. Following the principles of federated identity, the mechanisms still retain a single registration or authentication process, even when there is an inter-cluster network. Hence, the federation topologies will be as follows [55];

   - *Local profiling.* All devices are registered on local networks. Profiles for these devices are entirely managed by the local network and a local identity model is used for local profiling. An example of local profiling is the smart home scenario.
   - *Distributed profiling.* After the devices have been registered in the local network, when needed new profiles for the same devices can be created on other new networks. Thus, this new network will create new attributes and the profiles become distributed across multiple networks and attributes synchronization is needed.
   - *Third Party profiling.* In this scheme, the trusted third party within the established federation holds full control of creating and managing profiles, and more IoT networks can be connected to the trusted party.

2. **User-centric identity**
   The essential key for this method is the use of mobile devices as personal authentication devices (PDAs). The expansion of the internet enables a multiplication of the modes of connectivity that lead to interactions between things, places, and people. As a result, identity management should incorporate user identity, device identity, and the relationship between them, so a new layer for device authentication was added based on this model [17]:

   - *Device subsystem (DS)* a middleware layer on a user's device, which provides authentication functions for applications.
   - *Service subsystem (SS)* is located on the Service Provider's server and provides functions to delegate authentication to IdPs and to enforce service access control.

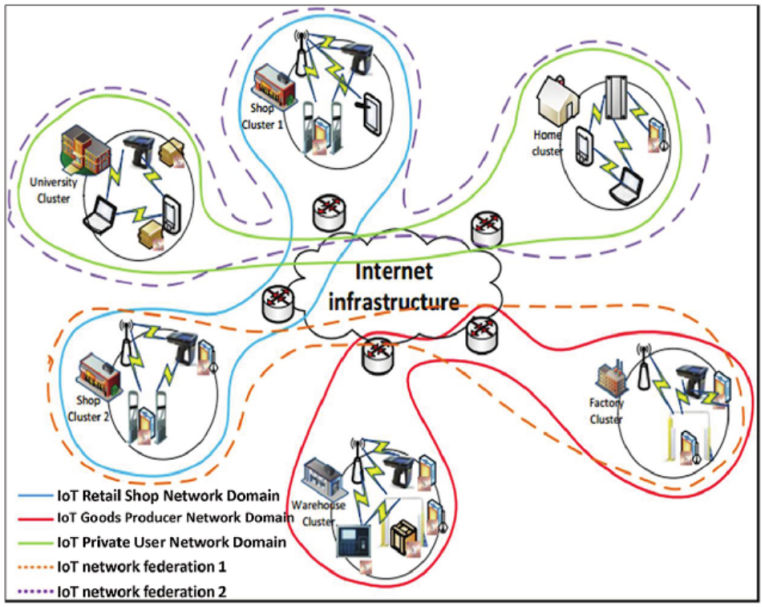

Figure 5.3: An Example of Federated IoT Network. Adapted from *Identity Management for Internet of Things* By Parikshit Narendra Mahalle and Poonam N. Railkar. Retrieved June 18, 2017.

- *Identity provider subsystem (IdPS)* is located on the identity provider's server and is responsible for the storage of all identity data as well as the authentication of users, devices, and services. It can be a private or public entity, installed by a private user at home or a public party in a cloud respectively.

3. **Hybrid identity**
   The use of blockchain and IoT creating a new model of digital identity management. The hybrid identity in an open model is an alternative that will be presented as a proposed solution for the research question in this master thesis. As a result, it is discussed in detail in the next chapter.

5.3 The Advantages and Disadvantages

1. **Federated identity**

   Advantages. This identity management type allows for the joining of partners among companies to deliver service automation to both customers and companies. For example managing employee retirement accounts, pension plans, stock options, and healthcare requires both additional labor and costs if they are done separately.

By using this model, they can leverage the employees' corporate portal authentication to provide access to their services. Additionally, in this model the employer (client) is responsible for managing its users and passwords (the client does not face any additional costs, because they already have to manage these).

Disadvantages. Federated identity still faces common challenges, especially in terms of security and privacy [38]. In relation to security, it is vulnerable to various attacks on web applications, such as replay attacks, man-in-the-middle attacks, session hijacking, etc. Regarding privacy, the service provider may get hold of more user information than is required because it lets users dynamically distribute identity information across security domains, increasing the portability of their digital identities.

2. **User-centric identity**

Advantages. The clear benefit is allowing the user to select the attributes they share with the requesting party. Hence, it ameliorates privacy concerns because users have full control over their data and know who using it and when [75]. OpenID also allows the use of an authentication registration process via SSO, which provides a more user-friendly method that ultimately encourages increased website adoption rates [11]. An ABC card provides a dynamic identity since it is possible for users to collect their attributes from several issuers.

Disadvantages. Even though users know and can control their data, in a decentralized model, only the relying parties such as services or applications know the identity provider; otherwise they would have no basis for making the decision to trust an assertion [75]. The second problem is relates to the use of OpenID. The URL identifying the subject is recyclable, and since OpenID permits URL-based identification, it raises the issue of privacy [55].

3. **Hybrid identity**

Advantages. It is suitable for dealing with unstable environments which require system flexibility since it manages everything, including users and devices. Thus, the system can be extended if there is an increasing amount of work. It also provides better scalability as one of its benefits because it offers connectivity to cloud-based applications.

Disadvantages. For closed-model cases, most of the implementations still experience the lock-in effect, as is the case for Microsoft Azure AD. To use Azure AD to provide simplified access to non-Microsoft cloud service providers like the others do, we must set up and maintain all the federated trusts ourselves.

Table 5.1: A Comparison of Identity Management Categories

Category	Implementation	Advantages	Disadvantages
Federated Identity	Liberty Alliance, Shibboleth, WS-Federation	Join partner among companies to provide simplicity for user portal services	Vulnerable to security and privacy attack since Service Provider might get hold of user information more than required
User centric Identity	OpenID, Information Card, Attribute-Based Credentials	Safe for privacy concern because user has full access control over their data. In ABC method, it also provides dynamic identity in that user can collect their attributes from several issuers	For decentralization, this model could not guarantee the privacy concern, since not only the user but also the relying parties such as services or applications know about the identity provider; otherwise they would have no basis for making a decision to trust an assertion [75]
Hybrid Identity	Microsoft Azure Active Directory, Blockchain	Flexibility and scalability to be extended in cloud-based environment	For Microsoft Azure, it still has lock up effect if want to be connected to the other kind of framework or services

5.4 Findings

Based on these comparisons, the implementation of federated identity and user-centric identity is primarily focused on creating an alliance between the identity provider, third

party even service provider in order to authenticate or store the user's data. Yet the open model as a vision for the future of energy infrastructure focuses more on an interconnected system, heterogeneous environment, and a greater range of physical devices or things, than in a closed model (intranet system), that also delivers a decentralized database mechanism for each user. This is a prominent argument as to why hybrid identity is suitable for adaptation into an open model system. In addition, hybrid identity also provides other superior reasons that parallel open model characteristics:

1. *Scalability.* While federated identity focuses on centralized architecture and user-centric identity solves the privacy issue by letting users control their own data, neither introduces the flexibility to be extended into open environments like cloud-based services. Hybrid identity can enable cloud bursts when needed; in a cloud burst, portable applications and workloads can be scaled up and quickly move between different locations and environments [69]. Although scalability is one of benefits of hybrid identity, previous studies on blockchain challenges also present a scalability issue. The scalability issue here is different to that for blockchain. In blockchain, there is risk as a result of scalability, that is, the tendency towards centralization when a blockchain grows larger; whereas here scalability only refers to the ability of a system to enlarge its processing scale. Therefore, this contradiction regarding scalability could be an advantage as well as a challenge, if we use blockchain as a database technology for hybrid identity.

2. *Hybrid IT and interoperability.* We are currently in the age of hybrid IT. In this environment, all applications and elements of infrastructure work cooperatively, regardless of whether they run on a public or private cloud. In an open model, energy will be delivered in any form that involves dynamic and continuous interaction. An example of this hybrid IT is a self-driving car, which needs to be able to detect and avoid obstacles, as well as understand if an object is a curb, a pedestrian, or a cyclist. It also allows the use of internet applications for ride-sharing or building computer vision with 3D mapping. This requires the integration and interoperability of multiple applications, and hybrid identity is needed to unify identities across these different applications and infrastructures. Regarding ride sharing, Toyota says blockchain could make it easier for companies and communities to come together to analyze the huge amounts of data expected from sensors in cars, roads, and other new transport devices. Eventually, this could lead to efficient smart transit everywhere. They are optimistic that blockchain technology may create transparency and trust among car users, reduce risk of fraud, and reduce or eliminate transaction costs [37].

3. *Self-sovereign identity (SSI).* Another finding that correlates with blockchain characteristics is that hybrid identity also enables the user to take control, providing SSI. Here the user can be people, organization, or devices. There are thousands of applications and each application has a different security model. With the proper identity

story, we can unify access control for all those applications and thus save a lot of time, while still remaining aware of potential dangers. In addition, by using SSI, we can put in-house service identity in the blockchain which will allow us to plan for the future of hybrid IT.

5.5 Conclusion

There are three categories of digital identity management that can be implemented for both closed and open models; federated identity, user-centric identity, and hybrid identity. Each category offers different solutions for different conditions, as well as taking along their own advantages and disadvantages. In a closed model, currently the biggest marketplace for digital identity, there are some implementation examples by companies such as OpenID, Microsoft Azure, IBM Tivoli, etc. While in an open model, renewal systems are proposed by combining features such as the device subsystem layer for user-centric identity and the three topologies (local profiling, distributed profiling, and third-party profiling) for federated identity. However, considering that federated identity and user-centric identity still depend on third-party and centralized mechanism to provide storage and authentication services, hybrid identity is the likely recommended approach, if we want to use blockchain as the backbone for a decentralized system. Besides, hybrid identity could also address scalability and interoperability issues; whereas, it is developed to give flexibility to the system in certain circumstances, such as the use of blockchain with IoT.

Chapter 6

The Proposed Solution

From the results of the comparison of digital identity categories, hybrid identity seems to be a potential choice. This section discusses the design of the hybrid identity system using blockchain technology, how they correlate, what properties are required, and what kind of use case models can be generated.

6.1 The Hybrid Identity on Blockchain

The hybrid identity can be a mixture between federated and user-centric identities. However, to create more adaptable system, this method also proposes more advanced concepts of flexibility, scalability, and interoperability than federated and user-centric identities. Therefore, the suggested digital identity management for an open model in the energy sector is more likely suitable for implementation with a hybrid identity approach.

The relationship between blockchain and digital identity begins with the role of blockchain as an open database service for every transaction and a distributed global identity system through a decentralized mechanism. One identity will be used for an individual and shared on the blockchain system and it serves for multiple systems and applications. The key characteristic of this system is *a combination of the decentralized blockchain principle with identity verification to create a digital identity system.* This enables a wide variety of applications to join, so that it no longer depends on specific third-party services.

To expand upon it in a more concrete way, the journey of a user identity on the blockchain begins as a self-asserted block, containing the user's identity attributes (hashed) and the user's public key, all signed with the user's private key [43]. Then a service provider, like an energy company, is also depicted on the blockchain, including their hashed attributes and public keys. They can sign the user's hashed attributes. For example, the energy company can sign the hashed address, name of the user, if the attribute values that have been asserted by the user match those on record at the passport office.

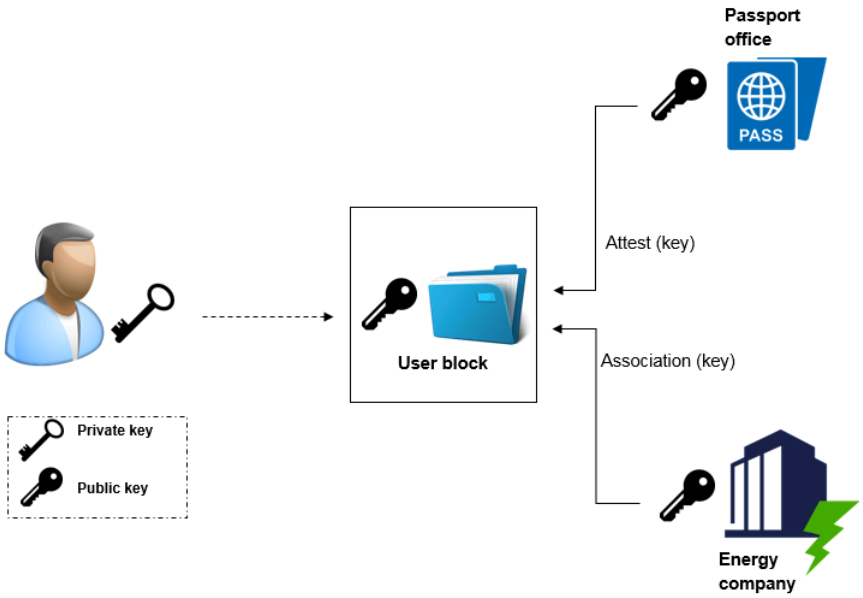

Figure 6.1: A User Identity Representation on Blockchain

Then which blockchain type is suitable with open model system ? As mentioned in the introduction, blockchain will introduce decentralized energy transactions and supply systems. The biggest transformation is from a market and business perspective. In line with this argument, Chapter 2 discusses closed and open blockchains from a business perspective. In that section, we could argue that open blockchain is more likely to suitable with the open model for following reasons:

1. *Disruptive changes.* From innovation point of view, open blockchain leads to radical innovation as it moves from a centralized system to a decentralized system which totally offers a different mechanism. An impact of this transformation is the global economy accelerating down a path of massive technology-driven change. The open blockchain accelerating smart economic system as more devices are connected. This smart economic phenomenon can be called the programmable economy.

2. *Zero-margin economy.* Open blockchain enables machine-to-machine interactions that can reduce the cost of intermediaries. Machine that own themselves will break the barriers of current industries and market models.

3. *No lock-in effect.* Unlike closed blockchains that generate dominant players, open blockchain users will receive services without being forced to buy additional updates or hardware. This is similar to the characteristic of the open model system as mentioned in the introduction.

Furthermore both open blockchain and hybrid identity offers same characteristics for flexibility and interoperability. Thus it strengthens the argument to choose open blockchain.

6.2 The Use Case Model

In the two previous chapters (Chapters 4 and 5), we study the concept of digital identity on blockchain and compare the digital identity categories, but still do not discuss the proposed functionality of a new system. Therefore, this section presents the use case model that describes the interaction between the user and the system. The model is quite straightforward: the user can create their identity on the blockchain, using an application to authenticate it and then share it with the companies that provide services. Here we draw on energy, finance, and autonomous service to represent some sectors in an open model system. All the transactions, responses, or requests, both from the user and the company are encrypted on the blockchain. The digital identity application links the real-world user identity to blockchain-based digital identity. While the application can confirm user identity, because of cryptographic hashing, this app does not actually hold the user's identifying information. The service providers or companies then authenticate users without ever needing the information to pass through the app servers. They can use a software tool which is connected to the blockchain so that they are able to connect individual personal information to hashes inserted into the blockchain [23]. The zoom-in focus on how the user's digital identity work on blockchain is presented in Figure 6.1.

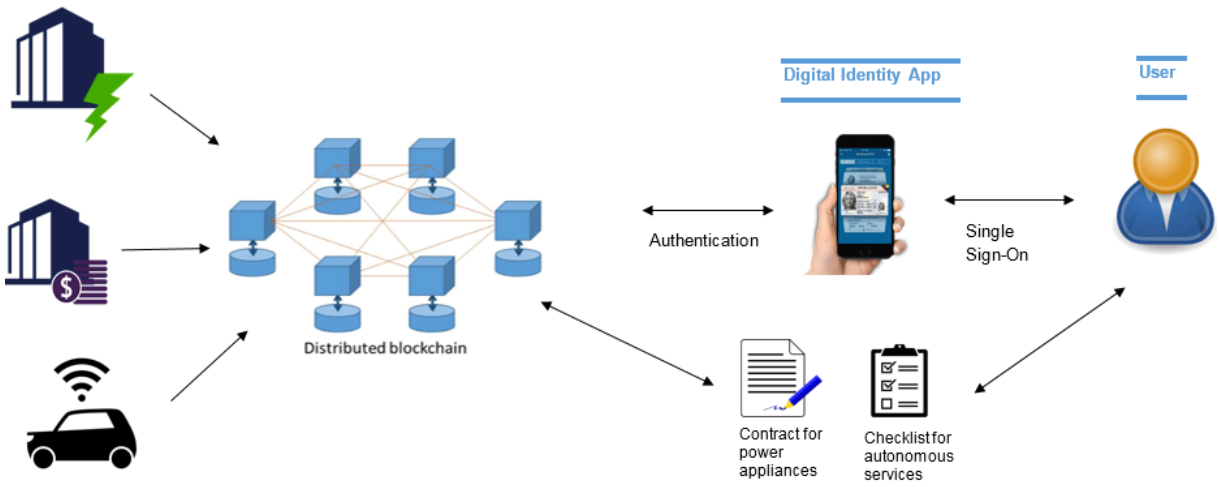

Figure 6.2: The Illustration of the Use Case Model

From the illustration of use case model, we see that smart contracts are used to automate the execution of the transaction. Smart contracts signal to the system when to

initiate specific transactions. This would is based on predefined rules designed to ensure that all energy and storage flows are controlled automatically, so as to balance supply and demand. For instance, whenever more energy is generated than needed, smart contracts could be used to ensure that this excess energy is automatically delivered into storage [42].

6.3 The Properties

Relating to the final research question, what properties are necessary to build the chosen category of digital identity management? the properties mentioned below are the alternative components from the proposed solution, hybrid identity management using blockchain. Based on the literature, these components are basically the essential elements to develop a digital identity management. In this case they have been combined with the hybrid identity, open model and blockchain concepts:

1. **Entity**
   In an open model, identities can be assigned to three main kinds of entities: *institution identity* (e.g., institute-ID, role-ID), *individual identity* (e.g., user-ID, role-ID, passport-ID, driving license, social-ID), and *object identity* (device-ID, network-ID, asset-ID, system-ID, app-ID). Those entities are then securely stored on the blockchain. Furthermore, since we use blockchain, every identity is a keypair, consisting of a public key (used to send data to, like an address) and a private key, needed to read private data and send data [64].

2. **Attribute**
   The energy sector field is huge in terms of open models, consequently an individual's identity is not defined by a single attribute such as a name, address, or user ID. Rather, it is a collection of attributes including, but not limited to, name, age, financial history, work history, address history, social history, energy consumption history (metering and billing) and etc. These attributes work together dynamically to create cross-vendor and cross-platform interoperability in autonomous services for the energy sector. The attributes also include user selected services (that they have subscribed to) and a checklist for the services that can change as the transactions happen for each interaction in the blockchain.
   Unlike another database system, in the blockchain we can create self-organizing attributes. For example, users can add smart contracts as their new attribute, which enables neighbor-to-neighbor transactions recorded on the blockchain. In this case, some consumers are also producers: so-called *prosumers* not only consume energy but also dispose of generation capacity in the form of solar systems or small-scale wind turbines. Blockchain technology could enable them to sell the energy they generate directly to their neighbours [42].

3. **Lifecyle**
   The lifecyle still apply three fundamental steps as introduced in chapter 3; registration, issuance and authentication. However for authentication, since it used blockchain, it will use a handshake mechanism to create direct interaction between user and service provider (chapter 4).

4. **Policies**
   Because of the use of blockchain for this open model system, consequently the policies will look at how energy law dealing with current legal framework for the application of blockchain technology in dealings with consumers and prosumers and future legal challenges presented by blockchain [42].

5. **Technology**
   In the previous properties (lifecycle) basically it derived from chapter 3. From that chapter we mentioned some tools such as QR code, public key infrastructure (PKI), and secure protocol like TLS as basic technique to develop a blockchain-based digital identity. Those technologies are the major technique for this concept. Since PKI has been discuss in chapter 3, then following will discuss about QR code and TLS.

   - QR code
     Quick Respond (QR) code authentication scheme is more user friendly and practical than one time password mechanism. QR code used two dimensional barcode to achieve much higher capacity since it encodes data in both horizontal and vertical directions, holds up to 108 bytes data [22]. In term of usability on blockchain, we could take bitcoin wallet as an example. When a user wants to send Bitcoins to another person, he starts by creating a Bitcoin transaction with the desktop wallet. When the transaction is ready for signing, the desktop wallet displays a QR-Code which contains embedded data such as the IP address of the desktop wallet and the public key for a TLS connection then user opens the smart phone wallet and scans the QR code with the phone's camera [56].
   - TLS connection
     The Transport Layer Security (TLS) is a standardized protocol which allow two parties of an internet connection encrypt their communications. It used a *handshake protocol* that permit the client and server to speak the same language, allowing them to agree upon an encryption algorithm and encryption keys before the selected application protocol begins to send data [30]. First the handshake itself uses asymmetric encryption – two separate keys are used, one public and one private. The public key is used for encryption and the private key for decryption during the handshake only, which allows the two parties to confidentially set up and exchange a newly-created "shared key". The session itself uses this single shared key to perform symmetric encryption, and this is what makes a secure connection feasible in practice [50].

6.4 The Remaining Challenges

When it comes to discussing the challenges, the use of blockchain drives some difficulties. Even though these are mainly derived from the blockchain technology, the concept of digital identity in the future also draws some possible problems. While working on this thesis, we observed that there are three major challenges that need to be considered. These remaining challenges could be the subject of future research to improve the durability of blockchain technology for digital identity management.

1. The maturity level of blockchain technology
   Regardless the advantages of blockchain (decentralization, immutability, public) there are still some red flags regarding the maturity level. Blockchain is considered a new technology that may have still a long way to go. As mentioned in Chapter 2, it may require further development in certain aspect such as performance and scalability. For example, transaction verification needs consensus that requires computation, and computation takes time. As a result, transaction processing is not instantaneous and can often take several minutes. However, the maturity is not only a technical issue, but also resides in the business aspects, especially the familiarity. According to PwC, only 24% of the global financial services sector say they are familiar with the concept [54].

2. Security
   A new IT architecture also introduces new cybersecurity risks, and blockchain poses some weaknesses. The type and amount of data stored on the blockchain will affect the risk profile, as will the permission mechanisms used, especially, the smart contracts that are vulnerable to cybersecurity risk. The exploitation of smart contracts can be due in part to a lack of review and testing prior to deployment activity.

3. Regulatory consideration
   The policy makers and regulators are continuing to find specific responses relating to the implementation of new emerging IT to ensure that the usability, availability, and safety criteria are met by this technology. Blockchain as digital identity management requires new mechanisms and research on the impact of those criteria. Currently there is still lack of regulatory standards for the implementation of blockchain. For instance, in Europe there is regulation on big data but not for blockchain. Even the current standard might evolve and it remains uncertain concerning blockchain applications.

Chapter 7

Conclusion

Blockchain is a currently trending topic in the IT world, and it is not only technically interesting but is also attractive from a business perspective. As a consequence, blockchain is believed to offer less operational costs for an open model system as the future of the energy sector in which many services will have interconnected machines, decentralization, be non-money-driven, and have no lock-in effects. This thesis has analyzed the use of blockchain in digital identity as one of the steps to building an open model system. Blockchain and digital identity introduce a new system for preserving people's credentials for their public services. Digital identity management combined with blockchain technology delivers decentralized online identities. In particular, the relationship between blockchain and digital identity is like the concept of a wallet in which the user can manage their attributes, as well as their public and private keys.

A hybrid digital identity, the selected approach, used in this thesis results from the comparison of three digital identity categories (federated identity, user-centric identity, hybrid identity). Based on this comparison, there are four main reasons why hybrid identity is selected as the most suitable choice:

1. Hybrid identity is a mixture of federated identity and user-centric identity. Since the implementation of both types primarily focuses on creating an alliance between an identity provider, a third-party provider, and even a service provider, the concept of centralization still lies behind those categories. Thus, using hybrid identity can enlarge the implementation cluster aligned with the open model concept, which many service providers could join to create a system with no centralized power.

2. Hybrid identity offers scalability, since it has flexibility because it can be extended into open environments like cloud-based services.

3. Hybrid IT and interoperability. The use of blockchain and IoT is one of the possibilities for such a future hybrid IT system. Moreover, this would allow integration by and interoperability from multiple applications.

4. By using blockchain as the database technology for hybrid identity, the users would be able to take control of their own attributes, specifically called self-sovereign identity (SSI).

As a new technology, blockchain's implementation in digital identity management leads to different properties (entity, attribute, lifecycle, policies, technology) needed especially on authentication technique. This requires a handshake mechanism that includes procedures involving a PKI verification mechanism. Additionally, to support this new mechanism, QR codes and TLS connections are needed to bring secure communication way. Using a QR code in the login process is a method that can make it easier to encode the authentication request. The certificate authority system (CA) that accompanies TLS as communication protocol delivers a simple transition.

Furthermore, from a business perspective, open blockchain is more likely to be suitable in this case. It delivers three aspects that are in line with the open model concept: disruptive changes, zero-margin costs, and no lock-in effect. On the other hand, from a technological perspective, it shares a similarity with hybrid identity in terms of interoperability. We can imagine that we could use any kind of digital identity app to gain access to these services without having limitations regarding which platform we use.

Chapter 8

Discussion

We began this research by making the assumption that blockchain is a suitable solution for creating an open model system. However, as discussed previously, there are still some limitations and uncertainties regarding this claim. Accordingly, building an open model system with another digital identity method must also be considered. The consideration takes into account certain circumstances like the concept of future energy systems. In this thesis, we assume that the open model is a likely the first step towards an abundant system that is a more complex, integrated and readily system. Thus, this leads to another choice and other properties. Perhaps digital identity will be more general, and the authentication mechanism will be more important and no longer use a username, password or QR code, but biometrics instead. This certainly requires new implementations and mechanism flows from a technological perspective.

This possible use case model could be works not only for the energy sector but also for other sectors dealing with public issues, such as financial, medical, and governmental services. There are many publications that discuss the possibility of blockchain applications for those sectors. The energy sector basically one of those cases concerning its great scale and basic needs for public consumptions. Comprehensively, solution proposed in this thesis could work by enhancing the properties according to the situation since it has flexibility of the hybrid identity principles.

Articles

[1] Ahn, Gail-Joon, Ko, Moo Nam, and Shehab, Mohamed. "Portable user-centric identity management". *IFIP International Information Security Conference* (2008), pp. 573–587.

[3] Alpár, Gergely and Jacobs, Bart. "Credential design in attribute-based identity management". *Bridging distances in technology and regulation, 3rd TILTing Perspectives Conference* (2013), pp. 189–204.

[5] Atzori, Marcella. "Blockchain technology and decentralized governance: Is the state still necessary?" (2015).

[7] Babich, Aleksandra et al. "Biometric Authentication. Types of biometric identifiers". *Bachelor's Thesis in Business Information Science HAAGA-HELIA University Applied of Science* (2012). URL: `https://www.theseus.fi/bitstream/handle/10024/44684/Babich_Aleksandra.pdf`.

[12] Boucher, Philip. "What if blockchain technology revolutionised voting?" *Scientific Foresight Unit (STOA)* (Sept. 2016).

[15] Buterin, Vitalik et al. "A next-generation smart contract and decentralized application platform". *Ethereum White Paper* (2014). URL: `http://www.ethereum.org/pdfs/EthereumWhitePaper.pdf`.

[17] Butkus, Pranas et al. "A user centric identity management for Internet of things". *IT Convergence and Security (ICITCS), 2014 International Conference on* (2014), pp. 1–4.

[18] Cakir, Ece. "Single Sign-On: Risks and Opportunities of Using SSO (Single Sign-On) in a Complex System Environment with Focus on Overall Security Aspects". *Master Thesis in Software Technology Linnaeus University* (2013).

[19] Castro, Miguel, Liskov, Barbara, et al. "Practical Byzantine fault tolerance". *OSDI* 99 (1999), pp. 173–186.

[21] Chadwick, David W. "Federated identity management". *Foundations of security analysis and design V* (2009), pp. 96–120.

[22] Chen, Changsheng. "QR Code Authentication with Embedded Message Authentication Code". *Mobile Networks and Applications* 22.3 (June 2017), pp. 383–394. ISSN: 1572-8153. DOI: 10.1007/s11036-016-0772-y. URL: http://dx.doi.org/10.1007/s11036-016-0772-y.

[26] Croman, Kyle et al. "On scaling decentralized blockchains". *International Conference on Financial Cryptography and Data Security* (2016), pp. 106–125.

[27] Crosby, Michael et al. "Blockchain technology: Beyond bitcoin". *Applied Innovation* 2 (2016), pp. 6–10.

[28] David, Bernardo Machado, Nascimento, Anderson CA, and Tonicelli, Rafael. "A Framework for Secure Single Sign-On." *IACR Cryptology ePrint Archive* 2011 (2011), p. 246.

[30] Dierks, Tim and Allen, Christopher. "The TLS protocol" (1999).

[32] Dittmar, Ben Cresitello. "Application of the Blockchain For Authentication and verification of Identity" (Nov. 2016). URL: http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf.

[35] English, Matthew, Auer, Sören, and Domingue, John. "Block chain technologies & the semantic web: A framework for symbiotic development". *Computer Science Conference for University of Bonn Students, J. Lehmann, H. Thakkar, L. Halilaj, and R. Asmat, Eds* (2016), pp. 47–61.

[38] Fragoso-Rodriguez, Uciel, Laurent-Maknavicius, Maryline, and Incera-Dieguez, José. "Federated identity architectures". *Proc. 1st Mexican Conference on Informatics Security 2006 (MCIS'2006)* (2006).

[39] Gervais, Arthur et al. "On the security and performance of proof of work blockchains". *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), pp. 3–16.

[41] Halim, Roohul, Shaharyar, Syed Atif, and Vapen, A. "Digital Identity Management" (2009).

[42] Hasse, Felix et al. "Blockchain – an opportunity for energy producers and consumers?" *PwC White Paper* (2016). URL: https://www.pwc.fr/fr/assets/files/pdf/2016/12/blockchain_opportunity_for_energy_producers_and_consumers.pdf.

[47] Jøsang, Audun and Pope, Simon. "User centric identity management". *AusCERT Asia Pacific Information Technology Security Conference* (2005), p. 77.

[48] Kallela, Jyri. "Federated identity management solutions". *Seminar on Internetworking, TKK T110* 5190 (2008).

[49] Keele, Staffs. "Guidelines for performing systematic literature reviews in software engineering". *Technical report, Ver. 2.3 EBSE Technical Report. EBSE* (2007).

[51] Kosba, Ahmed et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts". *Security and Privacy (SP), 2016 IEEE Symposium on* (2016), pp. 839–858.

[56] Mann, Christopher and Loebenberger, Daniel. "Two-factor authentication for the Bitcoin protocol". *International Journal of Information Security* 16.2 (2017), pp. 213–226.

[62] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system" (2008).

[63] Oecd. "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers". 186 (2011). URL: `http://EconPapers.repec.org/RePEc:oec:stiaab:186-en`.

[65] Olson, Eric T. "Personal Identity". *The Stanford Encyclopedia of Philosophy* (2016). Ed. by Zalta, Edward N.

[72] Rose, Karen, Eldridge, Scott, and Chapin, Lyman. "The internet of things: An overview". *The Internet Society (ISOC)* (2015), pp. 1–50.

[73] Sánchez-Guerrero, Rosa et al. "An event driven hybrid identity management approach to privacy enhanced e-health". *Sensors* 12.5 (2012), pp. 6129–6154.

[74] Semančık, Radovan. "Choosing the Best Identity Management Technology for Your Business". *Proceedings of InfoSecOn 2006 Conference, Cavtat, Croatia* (2006), pp. 1–10.

[76] Smedinghoff, Thomas J. "Introduction to Online Identity Management" (2011).

[82] Vasin, Pavel. "Blackcoin's proof-of-stake protocol v2. 2014". *URL: http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf* (2015).

[84] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger". *Ethereum Project Yellow Paper* 151 (2014).

[86] Zheng, Zibin et al. "Blockchain Challenges and Opportunities: A Survey" (2016).

Books

[4] Antonopoulos, Andreas M. *Mastering Bitcoin : Chapter 7. The Blokchain*. O'Reilly Media, Inc, 2013. URL: http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#merkle_trees.

[6] Ayed, Ghazi Ben. *Architecting User-centric Privacy-as-a-set-of-services: Digital Identity-related Privacy Framework*. Springer, 2014.

[55] Mahalle, P.N. and Railkar, P.N. *Identity Management for Internet of Things:* River Publishers Series in Communications. River Publishers, 2015. ISBN: 9788793102903. URL: https://books.google.nl/books?id=SR%5C_jBQAAQBAJ.

[60] Motykowski, Peter. *An Analysis of User-Centric Identity Technology Trends, Openid's First Act*. Regis University, Dayton Memorial Library, 2011.

[75] Sharman, R. *Digital Identity and Access Management: Technologies and Frameworks: Technologies and Frameworks*. Premier reference source. Information Science Reference, 2011. ISBN: 9781613504994. URL: https://books.google.nl/books?id=rAjoyoTv6qcC.

[78] Swan, Melanie. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[79] Tapscott, Don and Tapscott, Alex. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin, 2016.

[85] Zhang, Y., Zheng, J., and Ma, M. *Handbook of Research on Wireless Security*. Handbook of Research on Wireless Security. Information Science Reference, 2008. ISBN: 9781599048994. URL: https://books.google.nl/books?id=b3r81GCpOnYC.

Online resources

[2] Allen, Christopher. *Path to Self-Sovereign Identiy*. Apr. 2016. URL: https://www.coindesk.com/path-self-sovereign-identity/.

[8] Birr, Thomas and Stocker, Carsten. *Goodbye car ownership, hello clean air: welcome to the future of transport*. Dec. 2016. URL: https://www.weforum.org/agenda/2016/12/goodbye-car-ownership-hello-clean-air-this-is-the-future-of-transport/.

[9] *Blockchain Technologies for Business*. URL: https://www.hyperledger.org.

[10] BlockchainHub. *Types of Blockchain*. URL: https://blockchainhub.net/blockchains-in-general/.

[11] Bogiolie, Bonnie. *OpenID Pros and Cons*. Jan. 2011. URL: http://www.socialtechnologyreview.com/articles/openid-pro%5C's-and-con%5C's.

[13] Buecker, Axel et al. *Federated Identity Management and Web Services Security*. URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf.

[14] Bulters, Jeroen and Broersma, Jacob. *Blockchain – the benefits of smart contracts*. Nov. 2016. URL: https://www2.deloitte.com/nl/nl/pages/financial-services/articles/3-blockchain-the-benefits-of-smart-contracts.html.

[16] Buterin, Vitalik. *On Public and Private Blockchain*. Aug. 2015. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[20] CGI. *White Paper : Public Key Encryption and Digital Signature - How do they work?* 2004. URL: https://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf.

[23] Chester, Jonathan. *How The Blockchain Will Secure Your Online Identity*. Mar. 2017. URL: https://www.forbes.com/sites/jonathanchester/2017/03/03/how-the-blockchain-will-secure-your-online-identity/#4ae04d125523.

[24] Christensen, Clayton. *Disruptive Innovation*. 2017. URL: http://www.claytonchristensen.com/key-concepts/.

[25] Clark, Julia et al. *A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper : Digital Identity Towards Shared Principles for Public and Private Sector Cooperation.* URL: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf.

[29] Dickson, Ben. *Decentralizing IoT networks through blockchain.* June 2016. URL: https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/.

[31] *Digital currencies: call for information.* Mar. 2015. URL: https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information.

[33] Duncan, Richard. *An Overview of Different Authentication Methods and Protocols.* Oct. 2001. URL: https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-118.

[34] Eldon, Eric. *Single sign-on service OpenID getting more usage.* Apr. 2009. URL: https://venturebeat.com/2009/04/14/single-sign-on-service-openid-getting-more-usage/.

[36] Eysden, Roeland Assenberg van. *A blueprint for digital identity.* URL: https://www2.deloitte.com/nl/nl/pages/financial-services/articles/a-blueprint-for-digital-identity.html.

[37] Fermoso, Jose. *Why Toyota thinks blockchain could enable self-driving cars.* June 2017. URL: https://www.greenbiz.com/article/why-toyota-thinks-blockchain-could-enable-self-driving-cars.

[40] Greenspan, Gideon. *MultiChain Private Blockchain — White Paper.* 2015. URL: http://www.multichain.com/download/MultiChain-White-Paper.pdf.

[43] Hazari, Gautam. *The Relationship Between Blockchain and Digital Identity.* Nov. 2016. URL: http://www.gsma.com/identity/the-relationship-between-blockchain-and-digital-identity.

[44] Higgins, Stan. *Inside R3CEV's Plot to Bring Distributed Ledgers to Wall Street.* July 2015. URL: http://www.coindesk.com/r3cev-distributed-ledger-wall-street/.

[45] *Hybrid Identity Management.* Nov. 2015. URL: https://technet.microsoft.com/en-us/library/dn761716(v=ws.11).aspx.

[46] James-Lubin, Kieren. *Blockchain scalability : A look at the stumbling blocks to blockchain scalability and some high-level technical solutions.* Jan. 2015. URL: https://www.oreilly.com/ideas/blockchain-scalability.

[50] Kemmerer, Chris. *The SSL/TLS Handshake: an Overview*. Mar. 2015. URL: https://www.ssl.com/article/ssl-tls-handshake-overview/.

[52] Levy, Heather Pemberton. *The CIO's Guide to Blockchain*. June 2016. URL: http://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/.

[53] *Logical access security: The role of smart cards in strong authentication*. 2004.

[54] Macheel, Tanaya. *5 Charts That Show That Blockchains Are Too Immature For Finance*. Apr. 2017. URL: http://www.tearsheet.co/blockchain/5-charts-that-show-that-blockchains-are-too-immature-for-finance.

[57] Markus Vilcinskas, Lori Laschultz. *Understand Azure Active Directory architecture*. May 2017. URL: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-architecture.

[58] McNell, Paul. *Why The Future Of IoT Needs Blockchain And Distributed Ledgers*. June 2017. URL: http://www.huffingtonpost.co.uk/paul-mcneil/why-the-future-of-iot-nee_b_16948414.html.

[59] Mesropyan, Elena. *21 Companies Leveraging Blockchain for Identity Management and Authentication*. Feb. 2017. URL: https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/.

[61] MSDN. *Understanding Enterprise Single Sign-On*. Oct. 2012. URL: https://msdn.microsoft.com/en-us/library/aa745042(v=bts.10).aspx.

[64] O'Higgins, Conor. *Digital Identity Part I – Storing Sovereign Identities on the Blockchain*. May 2017. URL: https://cryptoinsider.com/digital-identity-part-storing-sovereign-identities-blockchain/.

[66] Pace, Eugenio. *Federated Identity for Web Applications*. URL: https://msdn.microsoft.com/en-us/library/ff359110.aspx.

[67] Parker, Luke. *Bitnation starts offering blockchain public notary service to Estonian e-Residents*. Dec. 2015. URL: https://bravenewcoin.com/news/bitnation-starts-offering-blockchain-public-notary-service-to-estonian-e-residents/.

[68] Piran. *Digital Iden-tity : An Introduction*. Dec. 2014. URL: http://piranpartners.com/wp-content/uploads/2014/12/An-Introduction-to-Digital-Identity.pdf.

[69] Preda, Diana. *7 things to know about hybrid cloud and hybrid IT*. May 2016. URL: https://www.ibm.com/blogs/cloud-computing/2016/05/7-things-know-hybrid-cloud-it/.

[70] *Reclaiming Financial Privacy With HD Wallets*. July 2013. URL: http://bitcoinism.blogspot.nl/2013/07/reclaiming-financial-privacy-with-hd.html.

[71] *Research on Identity Ecosystem : Decentralised Citizens Engagement Technologies*. June 2015. URL: https://www.nesta.org.uk/sites/default/files/research_on_digital_identity_ecosystems.pdf.

[77] Sprecher, Christian and Gallersdörfer, Ulrich. *Challenges and Risks of Blockchain Technology*. Feb. 2017. URL: https://wwwmatthes.in.tum.de/file/yxhmgsrmby7k/Sebis-Public-Website/-/Master-s-Thesis-Ulrich-Gallersdoerfer/170224%5C%20Gallersdoerfer%5C%20IRIS%5C%202017.pdf.

[80] Thompson, Collin. *The Difference Between a Private, Public Consortium Blockchain*. URL: http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html/.

[81] Troy, Sue. *Blockchain Ledger Lays Foundation For Programmable Economy*. URL: http://searchcio.techtarget.com/feature/Blockchain-ledger-lays-foundation-for-programmable-economy.

[83] Woochul, Song et al. *Advantages and Disadvantages of Blockchain Technology*. Nov. 2016. URL: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/.