

CAS Report:

CAS Big Data and Machine Learning 2018

A Study on Blockchain-based Digital Identity for the Financial Industry
June 2018

by Christian Stoecklin, PhD

Supervisors:
Prof. Dr. Burkhard Stiller
Bruno Rodrigues
Eder John Scheid

Department of Informatics
OR Institute of Computational Linguistics
University of Zurich



University of
Zurich^{UZH}

Abstract

In the age of digitalization, the concept of "identity" of natural or legal persons is evolving and is going to take on a new meaning. The today's well-known processes for verifying identity based on *e.g.*, passport, ID cards or birth certificates will change rapidly in the near future.

This article describes the importance of digital identity as we interact in the way we will do with public authorities or financial institutions and introduces the concept of a self-sovereign digital identity. The existing systems providing digital identity solutions only cover certain functional areas and often have conceptual deficiencies, so that new concepts and technologies are required for the realization of a self-sovereign digital identity. Blockchain-based solutions offer core functionalities for a new generation of self-sovereign identity systems in which the financial industry may play a significant role.

Besides the presentation and evaluation of different technologies, which are suitable for the realization of such self-sovereign identity systems, the role of the financial industry is also discussed. Due to its particular interests (*e.g.*, efficiency increase, cost reduction, new business services) and already existing capabilities for client identification and validation, the financial industry is in an ideal position to play a leading role in design and development of an overarching, self-sovereign digital identity system.

Open questions, technical and operational limitations of the blockchain-based solutions are also described in the study.

Contents

Abstract	ii
1. Introduction	1
1.1. Problem Space	1
1.2. Methodology	2
1.3. Scope of the Study	2
2. Background	3
2.1. Blockchain Basics	3
2.1.1. General Concepts	3
2.1.2. Blockchain Deployment Types	4
2.2. Landscape of Blockchain Application areas	6
2.2.1. Financial Applications	6
2.2.2. Non-Financial Applications	7
2.3. Discussion	7
3. Blockchain-based Digital Identity	9
3.1. General Concepts	9
3.1.1. Motivation	9
3.1.2. Identity Categorization	10
3.1.3. Lifecycle	11
3.1.4. Roles & Functions	12
3.2. Landscape of Digital Identity Systems	13
3.3. Digital Identity on Blockchain	16
3.4. Discussion	17
4. Self-Sovereign Identity	18
4.1. General Concepts	18
4.1.1. The Evolution of Digital Identity	18
4.1.2. SSI Concept	19
4.1.3. Architecture & Operating Mode	20
4.1.4. Operating Mode	20
4.2. Landscape of SSI Systems	22
4.3. Comparison of SSI Systems	26
4.3.1. Criteria	26
4.3.2. Evaluation	26
4.4. Discussion	29
4.4.1. Limitations	29
5. Impact and Opportunities in the Financial Industry	31
5.1. Role	32
5.2. Business Case	32
5.3. Improved and Novel Capabilities	33
5.3.1. Platform selection:	33
5.3.2. SSI Potential	34

Contents

5.4. Discussion	35
6. Final Considerations	36
6.1. Remaining Challenges	36
A. Appendix	38
A.1. Blockchain-based identity management and authentication solutions for cross-industry applications	38
A.2. Business Problems in the Financial Industry	40
Bibliography	41

1. Introduction

Identity is a critical point in the digital world. Many financial institutions and FinTech (Financial Technology) innovators aim to deliver pure digital offerings, but the process of identifying users consistently requires the use of physical channels, *e.g.* paper-based onboarding. The development of a new generation of digital identity systems is crucial to continuing innovation and delivering efficient, secure, digital-based financial service offerings, such as *e.g.* payments or loans transactions [For16].

The Internet was built without standards establishing guidelines towards the development of identity systems. Thus, in the end of the last century, websites simply began offering their own local accounts with usernames and passwords, and this has been the predominant solution ever since [TR16]. But the Internet has expanded quickly, and people use more and more services daily. This silo-based approach, where users must maintain identities for every site has become untenable. It is not just a usability disaster for individuals, it also creates a multitude of data honeypots for hackers – the breach of these systems can compromise trust in all Internet services. To solve this problem, a new approach based on the blockchain technology is needed.

Generally, physical or classical paper based identity systems currently put users at risk due to overexposure of information and the high risk of information loss or theft, *e.g.* documents can easily be lost, stolen or replicated by illicit actors, as well as read by entities with no legitimate reason to have the user information. They also put society at risk due to the potential for identity theft, allowing illicit actors to access public and private services. The digital identity would mitigate this problems and significantly minimize such risks.

New and maturing technologies, as *e.g.* Blockchain, have an important role and enable the creation of reliable and robust digital identity systems in the near future. These technologies hold considerable promise for identity, and are being explored by many different players, such as financial institutes. Conceptually, three main areas for application of blockchain-based digital identities can be identified:

- **Data Storage:** may offer improved methods of storing user information and increasing user control, privacy and security. For example Distributed Ledger Technology based on Blockchain technology combined with encryption and cloud storage or federated identity standards to create interoperability between identity management networks and external applications.
- **Data transfer:** Encrypted attribute exchange protocols allow information to be securely shared between endpoints without risk of interception or decryption, and with more controls that create privacy for users.
- **Authentication Information:** Many techniques for authenticating users are being explored for their potential to increase information security and user control in certain circumstances by linking users to their digital activities in more robust and persistent ways. For instance storing of biometric information, including fingerprint, retina scanning and facial recognition based on mobile devices which have potential to provide greater convenience and security.

1.1. Problem Space

As of today, many different "Digital Identity"-concepts are being designed or are already implemented and in use. Depending on the functional scope and purpose, not all have been successful, illustrating some of the pitfalls inherent in the construction of identity systems [For16]:

- **Stakeholder rejection:** Users may not adopt the system due to poor design or mistrust of the system's purpose or structure. They may perceive systems with limited scope and scale as valueless, and therefore not adopt them.

1. Introduction

- **Ineffective technology:** A constrained technology platform can reduce system functionality, preventing user integration or transaction completion. Insufficient data protection results in breaches, system compromise and data leakage.
- **Limited support:** Systems that have support of a narrow set of interests may fail due to inconsistent efforts. Key stakeholders of systems that lack support, may not experience sustainable and continuous uptake.
- **Unsustainable operation:** Systems with unsustainable operating or business models may fail.
- **Policy Changes:** Large and complex programs such as ID cards can be susceptible to political and/or ideological shifts.

1.2. Methodology

There are several efforts, based on the current situation in the financial industry, which try to shed light on the topic of "digital identity" from a business perspective [Pla17]. The resulting findings and initial conclusions show that the scope for action with regard to technology and functional requirements has not yet been exhausted [PBPW18].

Based on these existing approaches, the fundamental question regarding the requirement of digital identity was then extracted and searched for possible technical solutions using systematic literature searches.

1.3. Scope of the Study

The primary goal of this work is to study, under a business-oriented perspective, the use of blockchain in an identity system applied to financial institutions and their role. This article describes the way it is used for organizational business within the perspective of information technology such as the components or technology it needs, and the possible challenges it presents. Thus, this document does not investigate the technical aspects like the cryptographic technique, network architecture or implementation details.

This article provides an overview and introduction to the concept of digital identity and highlights the requirements regarding security, trust and usability. At the beginning (Section 2), a short technical introduction into the blockchain technology is given and an overview of existing systems is presented.

As of today, there are different technical approaches to implement such a specific digital identity concept as *e.g.* technical solutions based on blockchain technology which are described in Section 3. An important topic is the concept of "Self-sovereign Identity", which is described more detailed in Section 4. Due to the fact, that financial institutions are deeply impacted by the evolvement of such a "Digital Identity" [For16] and have a significant interest in a standardized, secure and reliable solution, the role of the financial industry will be discussed in Section 5.

In the last Section 6, some final considerations are discussed.

2. Background

2.1. Blockchain Basics

2.1.1. General Concepts

Blockchain technology has become popular since the introduction of bitcoin [Sat08] as digital currency. 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 [CNP⁺16] across peer-to-peer networks.

Blockchain has three fundamental features:

- **Blockchain is distributed:** instead of existing in a centralized database, the total history of each unit of currency is part of a database that is hosted on thousands of computers throughout the world, which are synchronized at each new block.
 - **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 is secure:** 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

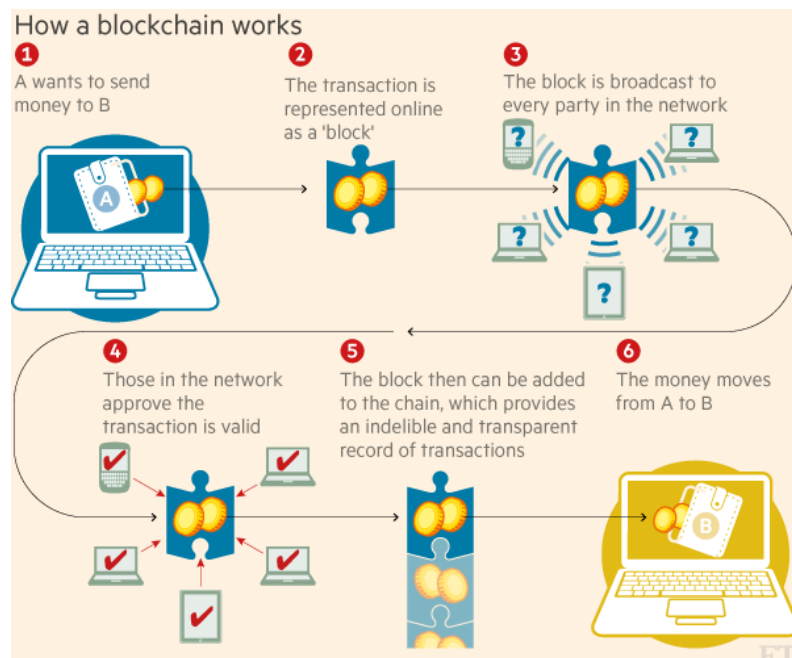


Figure 2.1.: Simple, schematic overview of how blockchain works based on 6 steps [VK16].

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 each other (like a chain) in a linear, chronological order, with every block containing the hash of the previous block. The technical architecture and details of blockchain is described in [VK16].

2.1.2. Blockchain Deployment Types

Many people have tried to classify blockchains, but there is no consensus on how to accurately distinguish between different types of blockchains [noab]. For simplicity's sake, the types of blockchain are discussed from two perspectives: first, with a high level of abstraction for the business view, and then from a technological perspective. In principle, there are two base types of blockchains: *private* blockchain and *public* blockchain, while private blockchains are often used in a *consortium* model. Those types are 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 (c.f. Figure 2.2).

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.

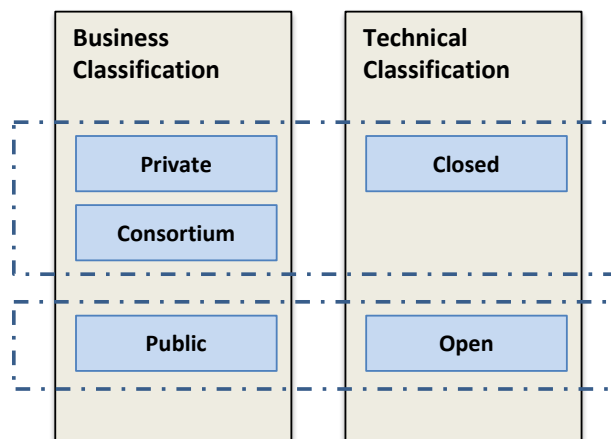


Figure 2.2.: Classification and grouping of different types of blockchain.

Private Blockchain

For a fully private blockchain, 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 [But15].

Examples:

- **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 [noaa].
- **MultiChain**: is a platform enabling the creation and deployment of private blockchains, either within or between organizations. As private deployment type, it solves the related problems of mining, privacy and openness via integrated management of user permissions. The core aim is threefold: (a) to ensure that the blockchain's activity is only visible to chosen participants, (b) to introduce controls over which transactions are permitted, and (c) to enable mining to take place securely without proof of work and its associated costs [Gre15].

Consortium Blockchain

Consortium blockchain is a private blockchain, in which the participation is extended to an arbitrary number of participants. It can be implemented by a single organization, which may contain several departments or cross-national instances that may implement different organizational schemes and thus, may not trust each other. The

2. Background

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 [noab]. 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 [Tho16]. Consortium blockchains operate under the leadership of a group instead of a single entity. An example of this type is Corda developed by R3.

Example:

- **R3:** is a distributed database technology company developing an enterprise-grade blockchain platform that removes costly friction in business transactions by enabling institutions to transact directly using smart contracts, while ensuring the highest levels of privacy and security. Corda was originally built by the financial industry, for the financial industry. It was developed in close collaboration with a vast network financial of institutions, regulators, trade associations, professional services firms and technology companies to leverage the power of blockchain to address their specific business challenges.

Public Blockchain

This type of blockchain maintains the principle that anyone in the world can not only access, but also write the data. This includes the consensus process to append blocks into the public blockchain or to block it. Public blockchain is an open-source system which is secured by the use of cryptographic verification backed up by consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS). Cryptoeconomics, is then a good incentive for the developer to develop systems with specific properties, such as performance, in which higher fees result in faster transactions, where new blocks can be added to the blockchain, but once blocks are broadcasted, they cannot be removed. [noab, VK16, Vos16]. An important example of a public blockchain is bitcoin.

Examples:

- **Bitcoin:** is the first and most popular digital currency. It uses a payment scheme in which encryption techniques regulate the generation of units of currency and verify the transfer of funds without interacting with a central financial institute. The bitcoin value chain is composed of several different constituents: software developers, miners, exchanges, merchant processing services, wallet companies, and users or consumers [Sat08].
- **Ethereum:** is a decentralized blockchain platform for "building unstoppable applications", while Ether is the cryptocurrency used on this platform. It provides a way to create sophisticated "smart" contracts or agreements. The agreement can have few, to no, middlemen. In this sense, it is a way to build applications that are more "decentralized", meaning, less dictated by companies, or other central authorities [Woo14].

It can be used for virtually any kind of transaction or agreement (to put it another way, any kind of activity that has an economic or governance aspect), at a lower cost than conventional alternatives, such as debit card payments, in a way that is trustless, secure, safe and censorship-resistant, all with high probability. The impressive list¹ of uses is growing fast and covering different types of functional areas.

Closed Blockchain

Private or consortium blockchains are categorized as closed blockchains due to the similar advantages that both offer an enterprise for organizations. This solution uses blockchain in a controlled environment or, in another words, is an enterprise-focused solution. Changes in the environment can only be made as long as they are approved by the single organization or consortium, thus 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.

¹[https://github.com/ethereum/wiki/wiki/Decentralized-apps-\(dapps\)](https://github.com/ethereum/wiki/wiki/Decentralized-apps-(dapps))

2. Background

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. Technical and functional optimization (*e.g.*, performance) 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). It is possible to 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 a commercial perspective, a dominant solution for identity would lead to an advantageous position in the market, because every transaction (that concerns the transmission of a scarce 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, but by an attribute that has been verified in the blockchain.

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 economy². In this economic model, new market players like machines, breaking the barriers of current industry and market models, enable 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 Artificial Intelligence (AI) constitute a logical next step in evolution of open blockchain applications.

2.2. Landscape of Blockchain Application areas

The evolvement of the blockchain technology and its scope of application is still a dynamic and ongoing process. The popularity started with the introduction of bitcoin and was developed to enhance the system for financial applications, due to its transparency as a result of its decentralized principle [CNP⁺16]. Later, more sophisticated applications based on the blockchain technology were developed for financial applications, such as *e.g.* smart contracts, insurance and crowdfunding. Furthermore, the usage of this technology is not restricted to the financial industry, it can be used in a wide range of non-financial services as *e.g.* governmental affairs, voting systems or smart data storage. In this regard, the usage of blockchain can be divided into two areas: financial and non-financial applications. Among the different approaches to categorize blockchain applications, these two categories are considered in this paper.

2.2.1. Financial Applications

Smart Contract: Smart contracts are computer programs that autonomously facilitate, verify, or enforce the negotiation or execution of an agreement. Smart contracts often emulate the logic of regular contractual clauses. Therefore, many kinds of contractual clauses can be made partially or fully self-executing, self-enforcing, or both. [BB16]. However, it should be noted, that the legal basis is still in verification and has not yet been fully clarified.

Digital Payment: This is basically the core function of bitcoin as digital currency. The birth of bitcoin brought about an evolution and a disruption of conventional payment systems managed by banks or other financial organizations (*cf.* Section 2.1.2). 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).

²<https://www.weforum.org/agenda/2016/12/goodbye-car-ownership-hello-clean-air-this-is-the-future-of-transport/>

2. Background

Securities settlement systems: Project Stella is a joint research effort by the Bank of Japan (BOJ) and the European Central Bank (ECB) on blockchain technology for financial market infrastructures [noa18]. For Project Stella, prototypes for "Delivery-versus-Payment" (DvP) on DLT were developed using Corda, Elements, and Hyperledger Fabric³. The result of the Proof-of-Concept (PoC) is promising and has proven that - from a conceptual and technical perspective - the settlement of securities against cash can follow different designs in a blockchain environment and does not require any connections between ledgers.

2.2.2. Non-Financial Applications

Decentralized Governance Services: One of 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 [CNP⁺16]. The Estonian government, in partnership with the world's first blockchain powered virtual country, Bitnation, which will start offering a public notary service to their e-residents [Par15].

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 [Bou16]. Therefore, blockchain technology could encourage transparency in governmental systems.

Music Industry In the music industry, the blockchain could transform publishing, monetization and the relationship of artists with their communities. First, music can be published on the ledger with a unique ID and time stamp in a way that is effectively unalterable. This solves the historic problem of digital content being downloaded, copied and modified at the leisure of users. Each record stores metadata containing ownership and rights information in a transparent and immutable way for everyone to see and verify. Additionally, smart contracts based programs that can be run on the blockchain along with the payment transactions.

Proof of existence of Documents: Proof of Existence is a simple service that allows one to anonymously and securely store online proof of existence of any document. This service simply stores the cryptographic digest of the file, linked to the time in which a user submits a document. It is to be noted here that cryptographic digest or fingerprint - not the actual document - is stored in blockchain, so user need not be worried about the privacy aspect.

Decentralized IoT: The Internet-of-Things (IoT) is increasingly becoming popular technology in both the consumer and the enterprise space. The blockchain technology facilitates the implementation of decentralized IoT platforms such as secured and trusted data exchange as well as record keeping. In such an architecture, the blockchain serves as the general ledger, keeping a trusted record of all the messages exchanged between smart devices in a decentralized IoT topology.

2.3. Discussion

The blockchain technology has made progress in recent years and the field of application is expanding. Nevertheless, it has to be considered, that blockchain will not solve all problems. However, various challenges remain in these applications, which must be solved in the foreseeable future. The most important problem areas – especially public blockchains – are the following:

³<https://hyperledger-fabric.readthedocs.io/en/release-1.1/>

2. Background

1. **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: (1) computationally complex and costly *signature verification*, (2) complex *consensus mechanisms* and (3) *redundancy* due to the total amount of computation that a blockchain requires. It can therefore be assumed that performance issues on blockchain result essentially from shifting the mechanism from being centralized to decentralized.
2. **Scalability:** In public blockchain, scalability is a major issue. This issue is often raised in technical discussions of the bitcoin protocol. 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 [JL15].
3. **Energy Consumption:** Calculation of PoW block in a common public blockchain consumes a huge amount of energy/cpu power. This computational power is used only for this purpose and the result does not have any other benefit that for sake of the blockchain.

There is still the question of the general differences between the open and private blockchain types. The idea that there is "one true way" to be blockchaining is naive – both categories have their own advantages and disadvantages. In principle, the following conclusions can be drawn [But15].

Private blockchains compared to public blockchains have following different characteristics:

1. The consortium/private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc. In some cases, *e.g.*, in national land registries, this functionality is required.
2. All validators are known and trusted, so the risk of a "51% attack" from miner collusion is not relevant.
3. Transactions are cheaper, since they only need to be verified by a few nodes that can be trusted to have very high processing power.
4. Nodes can be trusted to be very well-connected, and faults can quickly be fixed by manual intervention, allowing the use of consensus algorithms which offer finality after much shorter block times.
5. If read permissions are restricted, private blockchains can provide a greater level of privacy

It seems like private blockchains are unquestionably a better choice for institutions. However, even in an institutional context, public blockchains still have a lot of value, and in fact this value lies to a substantial degree in the philosophical virtues that advocates of public blockchains have always prompted, including freedom, neutrality and openness. For example, public blockchains provide (1) 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 and (2) are open, and therefore are likely to be used by very many entities and gain some network effects.

If one considers all already existing application areas and types of blockchain technologies, with all their functionalities and characteristics, there is still a great potential for the handling of personal data in the digital area.

3. Blockchain-based Digital Identity

3.1. General Concepts

For individuals (natural persons), legal entities and devices alike (*e.g.* machines [Ses17]), a verifiable and trusted identity is necessary to interact and transact with others. The concept of identity is not new, credentials have been used from beads and wax seals to passports, ID cards and birth certificates, to prove who we are. In general, personal identity in philosophy refers to the question: 'Who am I?'. It consists roughly of properties that make the individual unique and different from others [BB16].

The problems in proving identity – fraud, stolen credentials and social exclusion – is a well-known problem. However, the ways in which humans, devices and other entities interact are quickly evolving – and how we manage identity will have to change accordingly.

As an increasing number of people have access to stationary and portable devices connected to the Internet, there is a need for a digital representation of one's, this applies to

- **Humans:** proof of identity is a fundamental pre-requisite to access critical services and participate in modern economic, social and political systems.
- **Devices:** digital identity is critical in conducting transactions, especially as the devices will need to transact relatively independent of humans in the near future.
- **Legal Entities:** the current state of identity management consists of inefficient manual processes that could benefit from new technologies and architecture to support digital growth.

As the number of digital services, transactions and entities grows, it will be increasingly important to ensure the transactions take place in a secure and trusted network where each entity can be identified and authenticated.

Identity is the first step of every transaction between two or more parties. Over the ages, the majority of transactions between two identities has been mostly viewed in relation to the validation of a credential ("Is this genuine information?"), verification ("Does the information match the identity?") and authentication of an identity ("Does this human/thing match the identity? Are you really who you claim to be?"). These questions have not changed over time, only the methods to proof have changed.

3.1.1. Motivation

The advent of the Internet has moved us into the digital world and, for the past several decades, our identities have become redundant with each new service provider and authority. Data related to identities and the number of instances of identities have proliferated to an unmanageable state.

As digital forms of identity are required to conduct our lives, it is becoming clear that the current approach to identity and identity proofing is incompatible with the way we transact and behave across digital and physical worlds. Mandatory processes, which are used to verify, authenticate and manage an identity throughout its life cycle, are cumbersome and repetitive, requiring manual data reconciliation and validation processes in the background.

For individuals, this fragmented process leads to daily frustrations with countless usernames, forgotten passwords, ID documents and time wasted waiting to be verified and authenticated to complete a task such as gaining access to a building, boarding a plane, getting a job, etc. Challenges cited by individuals in both developed and developing country contexts include:

3. Blockchain-based Digital Identity

- **Limits to portability and acceptability:** "Recognized" identity differs widely among countries, organizations and contexts. Broadly, the issue arises as a result of a lack of trust between identity regimes and systems. As a result, individuals end up with thousands of digital and physical credentials for each service.
- **Social and financial inclusion:** For those who have no form of officially recognized identity, access to essential services as well as social and financial inclusion is extremely difficult or impossible.
- **Inability to manage data:** Globally, individuals have no ability to manage or know which entity has what parts of their data, where it is, how long the entity has access to the data, and who is monetizing that data.
- **Sharing of personal identification information:** Individuals have limited ability to select the persona and specific data that they want to share depending on the context and the entity with whom they are interacting.
- **Not user-friendly:** Authentication processes (*e.g.* banking, utilities) are often tedious and repetitive and provide the same set of documents for each service, sometimes from the same organization.

Digital identity causes problems for many organizations and are not easy to manage. Most identity-related industry practices and standards are developed and implemented based on industry-specific contexts, but as the need for digital identity evolves, a number of common issues have been identified:

- **Inefficiency:** Existing identity approaches are often inefficient, costly but mandatory (*e.g.* Know-Your-Customer (KYC), border control, global trade).
- **Data Quality:** Identity data is disparate, difficult to find and often inaccurate.
- **Interoperability:** Most identity systems and data are typically not designed to be interoperable, requiring significant, duplicate investments – even within a single organization.
- **Data Protection:** regulations are different from country to country and compliance is difficult and expensive to manage.
- **Implementation:** Large investments have been made into these regimes globally; any changes would be highly disruptive.
- **Scope of Digital Identity:** To date, the primary focus on identity is on identification of humans, most standards, systems and architecture for non-human identities range widely in terms of maturity, reusability, suitability and usability for legal entities, devices and beyond.

Digital and physical selves are here to stay and there is new hope from emerging technologies to provide a better structure for identity. Change from our traditional means of creating and using an identity is required. It no longer makes sense to rely on physical documents as the only means of identification, as they are inefficient and difficult to handle in the digital context.

3.1.2. Identity Categorization

The identity concept is applicable in different domains, depending on the objective for which digital identity is used. Basically, as mentioned in Section 3.1, the digital identity answers the question "Who am I?". To be more precise, it refers to a set of qualities and characteristics that make an entity definable, distinguishable, and recognizable compared to other entities. However, it is a collection of individual attributes that describe an entity and determine the transactions in which that entity can participate. While the total existing set of attributes is endless, they can be broadly categorised into three groups: *inherent*, *inherited/accumulated* and *assigned* attributes. These attributes differ for members of three main user groups: individuals, legal entities and assets [For16].

1. **Inherent Attributes:** are intrinsic to an entity and are not defined by relationships to external entities, *e.g.*

3. Blockchain-based Digital Identity

individuals: Age, height, Date of Birth, Fingerprints
legal entities: Industry Business Status
assets: Nature of the asset, Asset issuer

2. **Accumulated Attributes:** are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's lifespan, *e.g.*

individuals: Health records, Preferences & behaviors
legal entities: Business record, Legal Record
assets: Ownership of the asset, Transaction history

3. **Assigned Attributes:** are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies.

individuals: National identifier number, Telephone number, Email address
legal entities: Identifying numbers, Legal jurisdiction, Directors
assets: Identifying numbers, Custodianship

These attributes enable entities to participate in transactions, by proving to their counterparty that they have the specific attributes required for that transaction, *e.g.* for an individual to purchase alcohol, he must prove that they are over the legal drinking age in that jurisdiction

The purpose of a formal identity system is to allow counterparties without a previously established relationship to engage in trusted transactions. In a formal identity system, the users' attributes are attested to by trusted third parties; these third parties issue credentials that tie their attestation to the specific attributes, with some method of authenticating the credential to the entity that is presenting it. Users can use their wallet of credentials to engage in transactions with other entities that require some proof or knowledge of their attributes.

3.1.3. Lifecycle

Digital identities are created, used and changed as part of certain lifecycle of different stages. It starts with the registration, containing enrollment, validation and issuance, and finally the management of the identity, including updating, revocation or termination [CDD⁺16]:

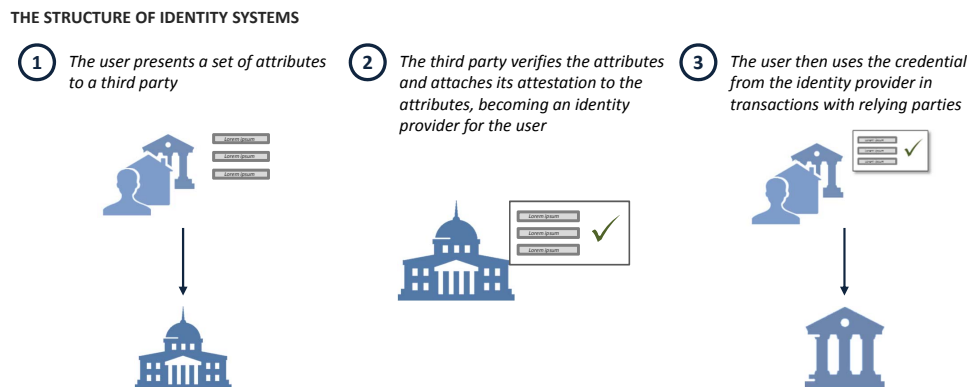


Figure 3.1.: Structure of the identity system [For16].

1. **Registration:** 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.
2. **Validation & Issuance:** identity is validated by checking the presented attributes against existing data. Then, the registered identity goes through an issuance/credentialing process before it can be used. For an

3. Blockchain-based Digital Identity

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.

3. **Usage:** After users have been registered and credentialed, it is possible to 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.

3.1.4. Roles & Functions

Within any identity system, different roles and functions are required for the identification and authentication process. Usually, processes are varying depending on the country context, type and scope of the digital identity. In general, individuals as *e.g.* citizens or clients, are the primary end-user in such a system, while government bodies and private companies are the primary digital identity providers (IdP) [For16] and [CDD⁺16] (*c.f.* Figure 3.2).

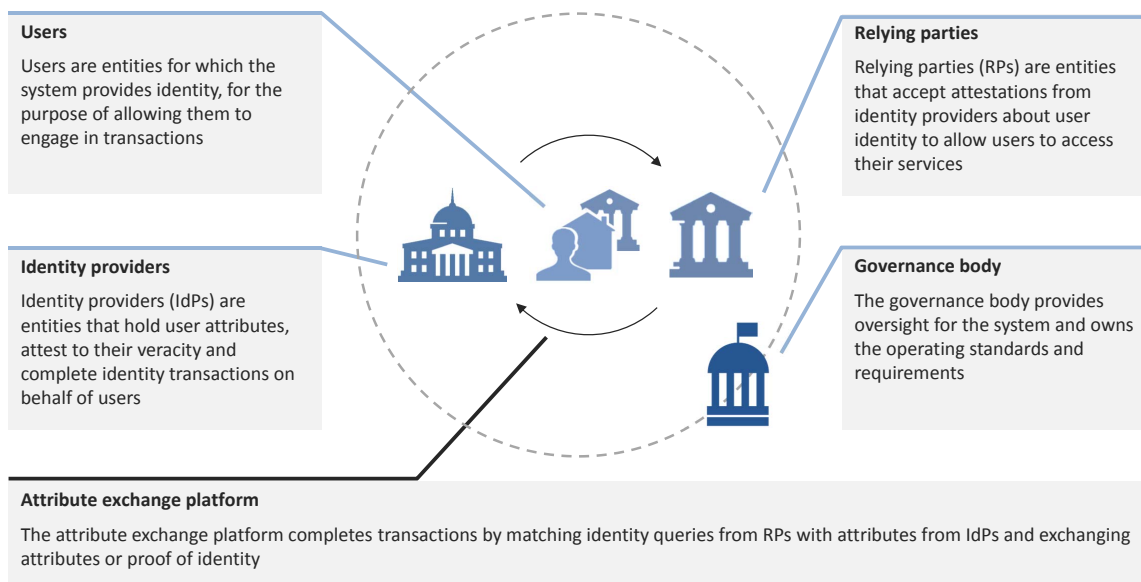


Figure 3.2.: Certain roles and function required in any identity system [For16].

- **Users:** Individual citizens/clients enroll in the identity system and use the credentials they receive to access services of a given country or company.
- **Digital Identity Provider (IdP):** Depending on the digital identity model, the IdPs can create digital identities for users by registering them and issuing the credentials. They may also store and manage data and credentials on behalf of the users. In the public sector, legal registers are the most common digital identity providers. Commercial service providers are also frequently digital identity providers. For example, mobile companies provide SIM cards and banks issue debit cards, in each case, after enrolling and verifying the identities of their customers. Oftentimes, private identity providers rely upon or use legal identity provided by the public sector (*e.g.*, SIM cards may be linked to a national identity number).
- **Relying Party (RP):** organization, service provider or online retailer that requires proof of identity and/or information about the individual in order to grant access to an online service or resource. This organization outsources identity management and may accept Digital Identities from more than one IdP.

- **Attribute Exchange Platform:** in order to enable the exchange of data between the IdPs, users and RPs in an efficient and secure way, a technical platform is needed in between that provides the relevant functions. There are different concepts and technologies how such a platform can be implemented. Each of them has its specific characteristics with the corresponding advantages and disadvantages. In the following Section 3.2 different concepts will be described in more detail.

3.2. Landscape of Digital Identity Systems

Digital identity systems that exist today fall across broad ranges of purpose, scope and sophistication. Some systems have a digital element added on top of their legacy core functionality what is still fundamentally a physical identity system, while others are fully digital and are built to scale and expand as user needs evolve.

Generally, there is no formal definition or classification of the individual systems existing. However, the following functional categorization is often found [For16] and [Del16]:

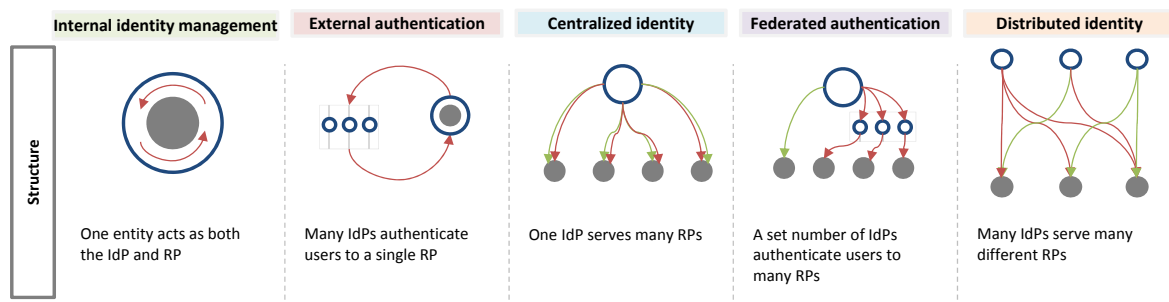


Figure 3.3.: Archetypes of Identity Management Systems with significant differences in structure and purpose [For16].

Internal Identity Management: the same entity acts as an IdP and RP. The entity uses information that it holds on users to permission them to access various internal services.

Key Features:

- The IdP/RP owns the required attributes needed to determine user permissions within the organization.
- The system is used to control which users within a single organization or entity have permission to access certain services.
- These types of solutions are generally developed by private organizations and sold as a product or service to various entities and institutions.

Case Studies:

Closed Internal Management Systems: Private solutions, (global). Leading Software-as-a-Service (SaaS) providers such as Salesforce, Oracle, SAP and Microsoft provide solutions that help their customers better understand, manage and interact with a set of users. These solutions serve a variety of industries and user groups (e.g., customers, employees, citizens, etc.).

External Authentication: one entity acts as both the IdP and the RP but uses an additional external set of IdPs to authenticate its users. It allows to streamline user access to a suite of services that are offered by a single entity, eliminating proprietary logins.

Key Features:

- The system has one RP, often a government, that holds user information and leverages a set of established institutions as IdPs (e.g., Financial Industries, telecom providers).
- The IdPs are usually trusted entities that perform strong authentication in user onboarding and are therefore trusted to provide a high level of assurance in identity transactions.

3. Blockchain-based Digital Identity

- Users can use their existing authentication methods through this group of IdPs to gain access to the RPs services.
- Both the RP and IdPs store user attributes – the authentication system is used to verify that the entity authenticating through the IdP should be permitted to transact with the RP.
- *No attributes* are transferred from IdPs to the RP.

Case Studies:

*GOV.UK Verify*¹: Public-private program, (United Kingdom). The GOV.UK Verify program is an external authentication system that allows UK citizens to access government services online. Users verify their identity online with one of nine IdPs. Once the users are authenticated through one of these providers, they are granted access to the government service they are trying to access.

*SecureKey Concierge*²: Public-private solution, (Canada). SecureKey Concierge is a digital authentication system that allows individuals to choose a trusted credential they already have with one of a set of financial institutions to access government services online. The users log in with their online banking username and password and are authenticated by their bank. Once authenticated, the users are granted access to the service. No attributes are transferred in the system.

Centralized Identity: a single entity acts as an IdP that authenticates users to RPs and transfers their attributes. These systems are often designed to streamline service delivery, enable data aggregation and provide a single view of users across multiple RPs.

Key Features:

- A single IdP holds all user attributes and owns the identity system; this is often the government or another central governing body.
- The IdP authenticates the user to the RP and transfers either a fixed or a tailored set of attributes to the RP to enable it to complete a transaction on behalf of the user.
- Some systems require RPs to pay a fee to use the system and to gain access to user attributes.
- Identity information can be transferred directly through a physical form factor (*e.g.*, a smart card) or through a digital brokerage system.

Case Studies:

*DigID*³: Government program, (Netherlands). Digital authentication system for Dutch residents accessing government services online. Individual attributes are held in a national citizen registry, which are used to authenticate users when they apply for a DigID. Individuals can then use their DigID username and password to authenticate themselves to government agencies. Their national identifier number is transferred from the national citizen registry to the RP.

Population Registry: Government program, (Finland). National database owned and maintained by the Finnish government. The government acts as the IdP, transferring attributes to public and private RPs. The purpose of the system is to collect data that can be used for elections, tax filing, judicial administration, etc. Private RPs may also access this data if they pay a fee and have received user consent.

Federated Authentication: one IdP uses a set of third parties to authenticate users to a range of RPs. The primary IdP is the entity that stores and transfers user attributes. These systems are designed to improve the login and transaction processes for users who are accessing online services by allowing them to use a single set of credentials to authenticate, and transferring attributes to RPs on their behalf.

Key Features:

- Identity information is stored centrally by one IdP.

¹<https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>

²<https://securekeyconcierge.com/resources/>

³<https://en.wikipedia.org/wiki/DigID>

3. Blockchain-based Digital Identity

- A set of third-party IdPs act as brokers that authenticate users to the RPs with which they are attempting to transact.
- RPs are able to access user attributes from the primary IdP, often for a fee (many systems require explicit user consent for attributes to be transferred).
- In systems that allow for the discretionary transfer of attributes rather than a fixed set of attributes, the user must explicitly consent to the transfer of specified attributes from the primary IdP to the RP.
- These systems are often government-driven, and the government acts as the central IdP that holds citizen or entity data.

Case Studies:

*NemID*⁴: Private sector solution, (Denmark). Electronic ID, digital signature and secure email solution that provides individuals access to public and private services. The government tendered the system to the private sector. Users define a common NemID login and password, as well as unique onetime passwords to authenticate themselves to online services. User attributes are stored in a central registry.

*Sweden BankID*⁵: Public-private service, (Sweden). eID system that provides citizens and businesses access to over 300 public and private services. Digital identities are issued by a set of private entities, including large banks and a major telecommunication provider. The public sector buys identity validation services from the private sector. Private sector service providers can join the BankID system by signing contracts with eID providers for authentication.

Distributed Identity: many IdPs collect, store and transfer user attributes to many RPs. These systems are notable in that they do not rely on attributes from a single IdP. The purpose of these systems is to allow users to interact easily with many different entities in an online environment by giving them a digital "wallet" of credentials.

Key Features:

- Identity information may be stored by multiple IdPs, on a distributed protocol (*e.g.*, *blockchain*), or may be collected from a variety of sources and aggregated by a single entity that operates the system.
- Attributes can be transferred from IdPs to RPs through a variety of methods, including smart cards or digital/mobile protocols.
- These systems are often privately owned and funded – governments or other public sector bodies may not play an active role within the network.
- Users *own* their own identities and often control which transactions occur and what attributes are transferred from one or more IdPs to the RP.
- These systems may not have a governance body and instead rely on common operating standards for interoperability.

Case Studies:

TUPAS: Private sector solution, (Finland). Identity system in which over 10 banks act as IdPs. Individuals can log into a wide range of services with credentials from their bank. The users' full names and National ID numbers are transferred from the IdP to the RP.

Global Legal Entity Identifier Foundation (GLEIF): Non-profit organization. Implementation of the Legal Entity Identifier (LEI) standard [Wol16]. This system assigns LEIs to every entity that engages with financial institutions; entities can use their counterparty's LEI to access their identity information from the GLEIF's partner network.

Mobile Connect: GSMA, (global) Digital identity system that authenticates the users through their device, allowing users to access a variety of services. This eliminates the need for users to have many usernames and passwords to access online services.

⁴<https://en.wikipedia.org/wiki/NemID>

⁵<https://developer.signicat.com/id-methods/swedish-bankid/>

Federated identities allow 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 information to share and to give him the exclusive control of his own information, a user-centric identity is required (*c.f.* Section 4.1). Such a system focuses particularly on the user context rather than the organization or enterprise.

3.3. Digital Identity on Blockchain

Digital identity is critical in many business and social transactions. However most recent conventional identity systems are costly, depending on proprietary systems and hindering innovation and greater customer experience.

In all the non-decentralized solutions, a third party owns and controls a repository of many peoples's identities. These models have different crucial problems [Ant17]:

- **Toxic data:** Operators are charging for a convenient utility and the data is a liability to the operator: such centralized based identity management systems are goldmine for hackers, and require specific cybersecurity protection.
- **Jurisdictional politics:** Regulators want personal data to be stored within the geographical boundaries of the jurisdiction under their control. Therefore, it can be difficult to create international identity repositories because there is always the argument about which country to warehouse the data and who can access it, from where.
- **Monopolistic tendencies:** This is not a problem for the central repository operators, but it is a problem for the users. If a utility operator gains enough traction, network effects lead to more users. The utility operator can become a quasi-monopoly. Operators of monopolistic functions tend to become resistant to change; they overcharge and do not innovate due to a lack of competitive pressure. This is wonderful for the operator, but is at the expense of the users.

By using blockchain or distributed ledger technology (DLT) as the underlying technology (*c.f.* Section 2.1), these problems can be avoided in a simple way by introducing a new way of managing identities. It allows data to be shared directly between entities in a network, without intermediaries and has certain key features that hold potential for identity systems:

- **Low transaction cost:** Distributed ledgers eliminate the need for intermediaries and therefore lower the cost of completing transactions.
- **Immutability:** Transaction history is maintained and verified through the network, preventing the falsification of information.
- **Convenience:** Record-keeping and transactions can be executed from any device, on- or offline.

DLT has potential in identity applications as an information storage and transfer mechanism within different types of systems. DLT could be applied as a distributed protocol, giving users the ability to store their identity attestations on a ledger and expose them to different RPs, or in a centralized system where the ledger would be owned by a single entity that would provide a consolidated view of the users' attestations for use in transactions, but would not reveal the nature of the credentials.

Distributed identity systems are the best fit to provide identity for individuals at large scale. They are built to scale to large numbers of IdPs and RPs, enabling a full set of convenient and efficient transactions for users. These systems intent to protect user privacy and increase control by allowing users to choose which entities hold their information, and by removing a single point of failure from the system.

3.4. Discussion

The structure and characterization of the various identity management systems described in Section 3.2 show that the individual types differ significantly in their concepts. Depending on the application area and purpose, one or the other type is better suited [For16]

- **Internal identity management:** management of user permissions inside a single entity based on internal information, *e.g.* identity access and management solution to control access to an internal services with a select user group (*e.g.*, employees, customers, etc.).
- **External authentication:** streamline user access to a suite of services that are offered by a single entity and eliminate proprietary logins, *e.g.* government offering online services to its citizens.
- **Centralized identity:** single version of the truth and a complete, accurate and standardized view of non-confidential data across different users, *e.g.* industry utility offering a comprehensive view of the entities in that industry to manage risk and exposure.
- **Federated identity:** single version of the truth and a complete, accurate and standardized view of data while allowing users to authenticate to a set of third parties, thereby eliminating proprietary logins, *e.g.* government enabling identity transactions for its citizens through collaboration with third parties.
- **Distributed identity:** incorporate large numbers of IdPs and RPs, providing user convenience, control and privacy in an online environment, *e.g.* full digital economy requiring multiple independent connections between IdPs and RPs to enable user transactions.

In order to (1) overcome the inconveniences of the non-decentralized systems introduced in Section 3.2, (2) to allow individual users to manage their own identities and (3) to grant control over who has access to their personal information, the blockchain technology is a valid solution to mitigate the current deficiencies. Such a solution can also answer the question of the ownership of one's own digital identity. In the next chapter 4, the concept of "self-sovereign identity" is introduced and some implementation models are explained.

Regardless of all these promising properties of decentralized and blockchain-based solution concepts, there are some problems that cannot be solved by using blockchain as a general remedy (*c.f.* Section 4.4.1).

4. Self-Sovereign Identity

4.1. General Concepts

4.1.1. The Evolution of Digital Identity

Based on the functional classification of Section 3.2, the characterization of the digital identity can also be represented by describing the development of user-specific properties [All16] instead by its functional implementation. The models for digital identity have advanced through four broad stages since the advent of the Internet: *centralized* identity, *federated* identity, *user-centric* identity, and *self-sovereign* identity.

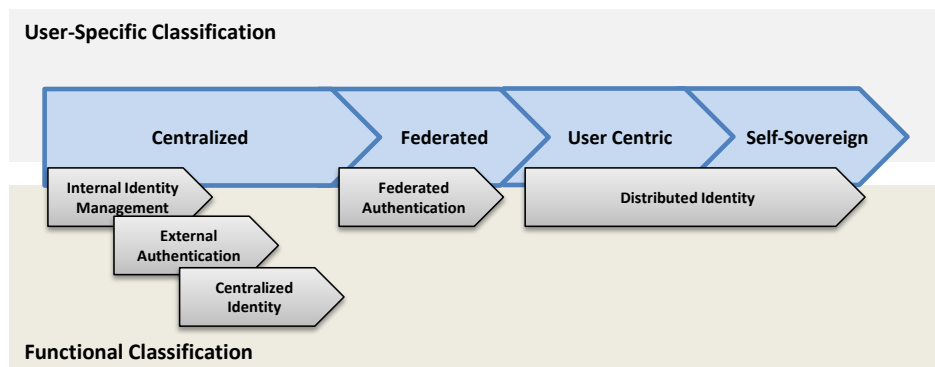


Figure 4.1.: Evolution of the digital identity.

The evolution is a result of trying to satisfy three basic requirements:

- **Security:** the identity information must be protected from unintentional disclosure.
- **Control:** the identity owner must be in control of who can see and access their data and for what purposes.
- **Portability:** the user must be able to use their identity data wherever they want and not be tied to a single provider.

The characterization of "user-specific" identity types is very similar to that described in Section 3.2. They differ primarily in the user's point of view rather than the digital identity providers.

- **Centralized:** this model corresponds to the internal/external-& centralized functional identity management classification (Section 3.2). The identities are centralized, owned and controlled by a single entity (*e.g.*, social network). Because the users do not own their identity record, it can be invalidated at any time. The corresponding regulations are recorded in the terms and conditions as a preventive measure, *e.g.*
 - *Instagram*¹: We reserve the right to refuse access to the Service to anyone for any reason at any time.
 - *Facebook*²: If we determine that you have clearly, seriously, or repeatedly violated our terms or policies, including in particular our Community Standards, we may suspend or permanently disable access to your account.[...]

¹<https://help.instagram.com/478745558852511>

²<https://www.facebook.com/terms.php>

4. Self-Sovereign Identity

- **Federated:** gives a degree of portability to a centralized identity, for example enabling a user to login into one service using the credentials of another. In its simplest form, federation is visible in services such as Facebook Login, where websites enable users to create accounts and sign in using their Facebook credentials, or in a government model as *e.g.* the "GOV.UK Verify" (Section 3.2, page 13). This model can be used to realize Single-Sign-On (SSO) capabilities.

Although federation provides a appearance of portability, the power still remains with the identity provider. In fact the implications to a user of having their centrally federated account deleted or compromised are much more profound if that account is their key to many other third party services.

- **User-Centric:** this model is most frequently implemented in the form of independent personal data stores, where the system puts the user in control, accumulation and release to third parties of their own data. It allows users to store identifiers and credentials for different service providers in a single tamper-resistant hardware device, as *e.g.*, smart card.

One fundamental problem remains that, in a mature personal data store ecosystem, relying parties will need to connect to many such providers to reach a wide customer base, resulting in complex and time consuming integration without economies of scale.

- **Self-Sovereign (SSI):** this identity model is independent from any individual silo, and provides all three required elements: *individual control*, *security*, and *full portability*. It removes centralized external control aspects from the three previous models. The individual (or organization) to whom the identity pertains, completely owns, controls and manages their identity. In this sense, the individual is their own identity provider as there is no external party who can claim to "provide" the identity for them because it is intrinsically theirs. The individual's digital existence is independent of any single organization. Nobody can take your self-sovereign identity away from the user.

A SSI system creates new requirements – which are introduced in Section 4.1.2 – on the technology that is used to create such a system. The blockchain technology fulfills most of these requirements. In the next Section the concept of "Self-Sovereign Identity" is described more detailed.

4.1.2. SSI Concept

Sovereignty is a supreme power or authority, which governs itself without any outside influences. Sovereignty for identity management means that the user's identity data are fully owned and controlled by herself. The concept of Self-Sovereign identity can be seen as the next stage of evolution in identity management.

The blockchain technology provides a good basis to create a SSI system [Win18, Abr17]. The requirements of such a system are detailed as follows:

1. *Each individual has to have the full control over his data:*
Each user must have full control over his own identity data. This includes not only *what* identity data are being stored but also *who* has access to these data. The user should be able to include or import identity attributes as well as delete or revoke them. All access of identity data of a user should be logged for later verification.
2. *Ensure security and privacy of user's identity data:*
Identity data have to be stored and processed in a highly secure manner, while user's privacy has to be preserved. For instance, unlinkability between the user wallet and his identity data increases the user's privacy.
3. *Fully portability of the data (Interoperability):*
Identities should be as widely usable as possible, *e.g.*, a SSI system can be used as identity provider when the user tries to access an online service. Regimes may change, users may move to different jurisdictions, but transportable identities ensure that users remain in control of their identities regardless of this.

4. Self-Sovereign Identity

4. No trust in a central authority is required:

The underlying blockchain technology solves the required trust related to a central authority.

5. Ensure data integrity:

The integrity of identity data can be ensured by utilizing the blockchain. This is one of the main advantages using the blockchain technology.

6. Transparency of the identity data is maintained

The blockchain technology provides data transparency of all in the blockchain stored data. All changes to the data in the blockchain are fully transparent so that no one can alter or delete data without someone else noticing it.

SSI is a relatively new concept and is undergoing rapid changes. Standards for decentralized identifiers and verifiable claims are being developed to provide interoperability. Ultimately, these systems should promote human dignity and protect the basic human desire for self-determination.

4.1.3. Architecture & Operating Mode

The architecture of a SSI system based on the blockchain technology offers the possibility to realize a system without semi-trusted parties such as central certificate authorities (CAs) or registration authorities (RAs). Nevertheless, the degree of required trust depends on the specific blockchain implementation. Only public or permissionless blockchains provide a fully semi-trustless environment. If a blockchain is private or permissioned, only authorized parties have access to the ledger, which requires at least some kind of trust relationship to these entities (*e.g.* Sovrin *c.f.* Section 4.2). Even though authorized parties are independent of each other, trust in the chosen parties or in the selection process of becoming a trusted party is still necessary.

The blockchain ledger is the central part of such a SSI system. Nevertheless, depending on the usage of underlying blockchain technology, there are additional parts required to fully support all features and use cases which are described in Section 4.1.2. Therefore, the distributed ledger may be extended by at least two additional parts: *off-ledger storage* and the *data import* part [Abr17]:

- **Off-Ledger Storage:** Storing sensitive documents in the blockchain might not be a good idea even though these data is encrypted. The problem that occurs by storing data in the blockchain is that these data cannot be modified or deleted anymore afterwards. This might be an important feature in some cases.

In the SSI system, person related data are stored off-ledger, only a unique identifier is stored in the blockchain. This special identifier is cryptographically linked to the off-ledger data storage. Different storage services such as cloud storages can be used as off-ledger storage.

- **Data Import:** Identity data can have different levels of quality. For instance, a national authority can issue qualified identity data of a person. In contrast, a person enters person related data himself. The authenticity of these self-entered data cannot be guaranteed. Therefore, it can be beneficial for a user that the SSI system supports the import of qualified data.

The qualified data import is not straightforward because a special transformation of the data during the import process has to be performed. This transformation process converts the data format from the received format to the SSI system supported format. The received data format can vary depending on its source. This is a necessary step in order to provide selective disclosure and attribute attestation at a later point.

4.1.4. Operating Mode

Besides the theoretical concept and architecture, the question now arises, how such a self-sovereign solution works. Basically, the data is stored on a specific device (*e.g.* smartphone or computer) and maybe backed up on an another device or personal backup solution, but *not* stored in a central repository. Additionally, some sort of "identity wallet" is needed to access and manage the identity data.

4. Self-Sovereign Identity

Process: Claim, Proof & Attestation

1. The identity wallet starts empty with only a self-generated identification number derived from public key and a private key. At this stage, the identification number is not public. The identification number has first to be issued to the user (Figure 4.2). It is important to note that the identification has been created by the user himself and is therefore – per definition – self-sovereign. The laws of big numbers and randomness ensure that no one else will generate the same identification number.
2. The identification number is then used with the identity claims in order to get the attestation from the relevant authorities.
3. The attested information is then used as approved identity information

Public Key Model (simplified)

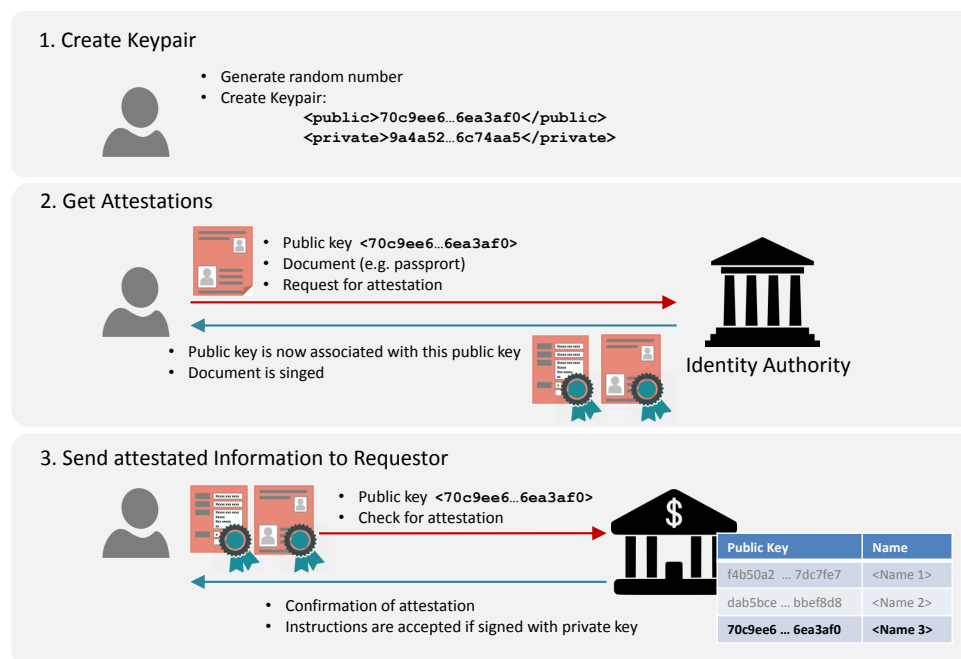


Figure 4.2.: Key generation and attestation of documents [Ant17].

- **Claims** are stored by typing text into standardized text fields, and saving photos or scans of documents.
- **Proofs** are stored by saving scans or photos of proof documents. However this would be for backward compatibility, because digitally signed attestations remove the need for proofs as we know them today.
- **Attestations** are stored in this wallet too. These are machine readable, digitally signed pieces of information, valid within certain time windows. The relevant authority would need to sign these with digital signatures – e.g. passport agencies, hospitals, driving license authorities, police, etc.

An important aspect of the SSI concept is the “*need to know, but not more*”-principle. This means that the user can exchange only the minimum subset of information that is required. Under this aspect, the data scope can be further reduced by the authorities if they provide specific functional “bundles” of attested claims, as e.g. “over 18”. The user is then able to choose which piece of the identity information to pass to any requester. Therefore, if the user has to prove that he is over 18, he does not need to share his date of birth, the statement saying “over 18”, signed by the relevant authority, must be sufficient. Sharing this kind of data is safer both for the identity provider and the recipient. The provider does not need to overshare, and the recipient does not need to store unnecessarily sensitive data.

Data sharing

Data would be stored on the person's device (as pieces of paper are currently stored at home today). Then, when requested, the person would approve a third party to collect specific data, by tapping a notification on his device. Something similar to this is already existing – using a service by "linking" a Facebook or LinkedIn account – but instead of going to Facebook's servers to collect the personal data, it requests it from the phone, and the user has granular control over what data is shared.

Self-Sovereign Identity Platform

- Platform creates and enforces rules governing the process and approvals need for data updates
- The platform does not store identity data
- Data transfer is secure, encrypted, point-to-point, over the net

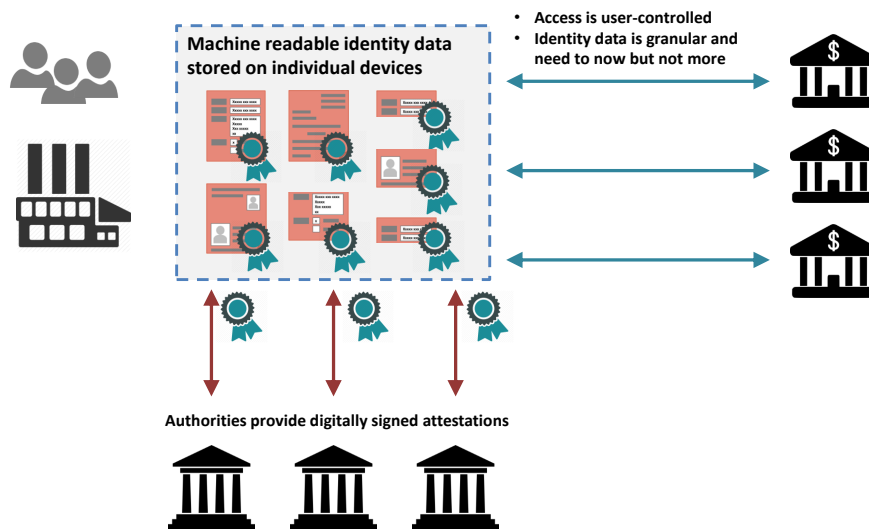


Figure 4.3.: Data exchange based on the SSI platform.

It has to be noted, that digital signatures require public and private keys that need to be managed, and certificates need to be issued, revoked, refreshed. Identity data isn't static, it needs to evolve, according to some business logic. All these functionalities need to be built and handled separately.

4.2. Landscape of SSI Systems

Several self-sovereign identity systems exist now in various stages of development. Each of these support decentralized, self-sovereign identity but differ in how claims are issued and presented. This Section gives a short overview of the technologies, which are relevant for a SSI system.

There are many companies developing blockchain-based digital identity management and authentication systems³ (c.f. Appendix Section A.1). Some solutions have not been considered in this Section, because they have a different focus than the goals of this work (e.g. BlockVerify), are premature, or are commercial projects with no or restricted access to technical information (e.g. KYC-Chain, Shocard) [Abr17]. Following five solution are compared: Sovrin⁴, Blockstack⁵, Multichain⁶, Ethereum⁷ and uPort⁸.

³<https://gomedici.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/>

⁴<https://sovrin.org/>

⁵<https://blockstack.org/>

⁶<http://www.multichain.com/>

⁷<https://www.ethereum.org/>

⁸<https://www.uport.me/>

Sovrin

Sovrin is an open source project that focuses on self-sovereign identity. It is based on a permissioned, distributed ledger technology and using Plenum⁹ as crypto library, which offers an advanced distributed consensus algorithm. Sovrin allows the import of certified identity data and offers attribute redaction. Each attribute has to be signed by the issuing authority, which enables the selective disclosure. The platform enables "bundled" functionality (as described in Section 4.1.4) to increase the privacy of users when for instance a service provider wants to verify if a user is over 18 and hides the actual birthdate.

Write permission is granted by the Sovrin foundation who decides who is going to be one of these "validator" nodes. Two kinds of nodes have to be distinguished (*c.f.* Figure 4.4). First, the validator nodes – placed in the validator pool – that are responsible for the write operations to the Sovrin ledger. 60 to 120 of these nodes are worldwide expected. Second, the observer nodes, which handle the read operations as well as keeping their state synchronized with the validator nodes. A few thousands of these nodes are expected worldwide [WR18].

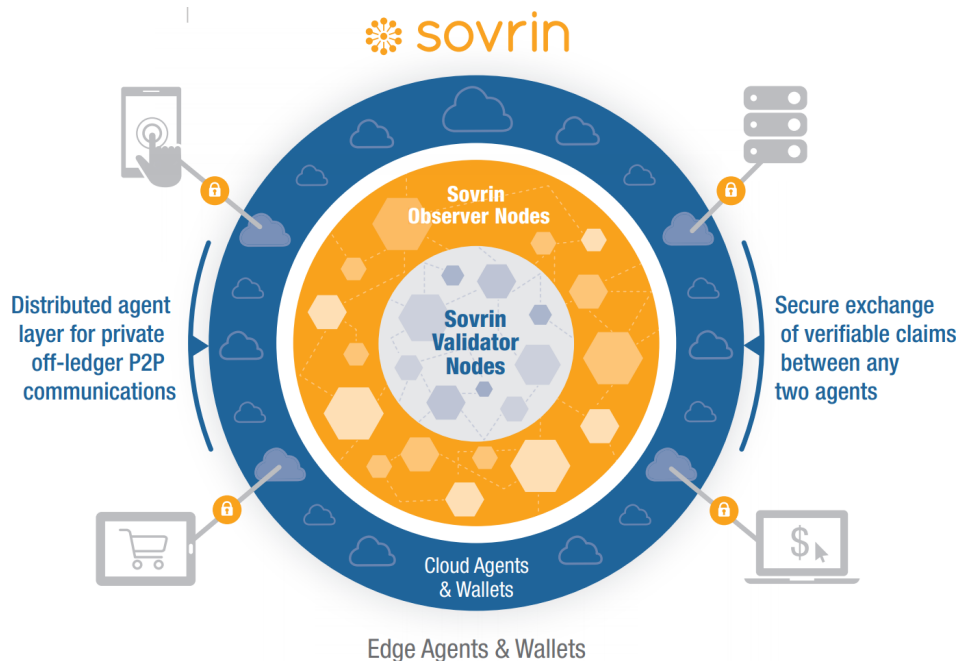


Figure 4.4.: Sovrin Architecture Overview [WR18]. Each circle identifies a different purpose, while the Sovrin agents can be seen as middle layer between the clients and the inner ledger.

Blockstack

Blockstack implements an Decentralized Domain Name Service (DDNS) with an alternate Public-Key Infrastructure (PKI) on top of the Bitcoin blockchain [ASNFI17]. The architecture has three layers as shown in Figure 4.5, with one layer (the blockchain layer) in the control plane and two layers (the peer network and data-storage) in the data plane.

Layer 1: Blockchain it is the lowest layer and serves two purposes: storage medium for operations and provides consensus on the order in which the operations were written. Virtualchain encodes operations in transactions on the underlying blockchain. The complexity, like mining operations, consensus algorithms, etc., are hidden underneath this abstraction. The higher layers only care about reading/writing totally ordered operations and can operate on top of any blockchain.

⁹<https://github.com/hyperledger/indy-plenum>

4. Self-Sovereign Identity

1. **Layer 2: Peer Network** is used for discovery and is part of the data plane. It separates the task of discovering resources (e.g., routing to data) from the storage of data.
2. **Layer 3: Storage** hosts the actual data values and is part of the data plane. All stored data values are signed by an owner key defined in the control plane. By storing data values outside of the blockchain, values of arbitrary size and variety of storage backends are allowed. Users do not need to trust the storage layer and can verify their integrity in the control plane.

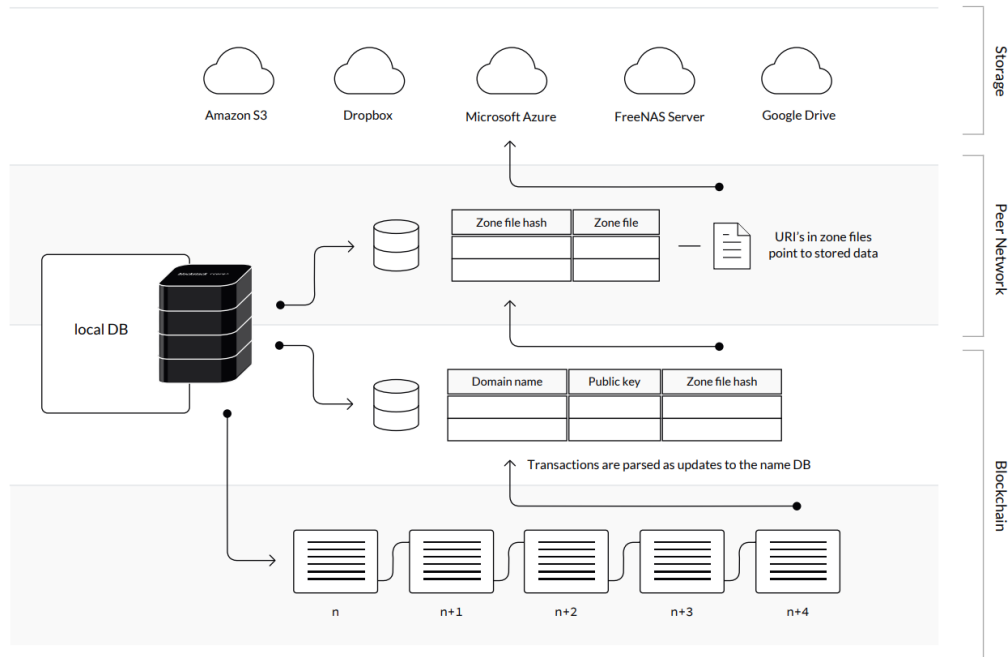


Figure 4.5.: Blockstack architecture, separation of control and data plane with 3 layers [ASN17].

Multichain

Multichain is a fork of the Bitcoin blockchain and aims to overcome a key obstacle to the deployment of blockchain technology in the institutional financial sector, by providing the privacy and control required [Gre15]. It provides a platform for creating private blockchains with integrated user permission management, native assets and data streams. Such private blockchains can be used within or between organizations and aims three main goals:

1. Blockchain and its activity is only visible to chosen participants.
2. Introduction of control over which transactions are permitted.
3. Enablement of secure mining without the need and the related cost of calculating the proof-of-work (permission-based mining). Only authorized participants are permitted to mine.

In contrast to Bitcoin or other blockchain technologies, Multichain supports not only a single blockchain, instead it supports different blockchains at the same time. Running more than one blockchain simultaneously can offer institutions advantages such as using one blockchain to monitor incoming funds, which then triggers a transaction on another blockchain.

4. Self-Sovereign Identity

Ethereum

Ethereum¹⁰ is an open blockchain platform used to build decentralized applications that run on blockchain technology. But unlike the Bitcoin protocol, Ethereum was designed to be adaptable and flexible. It was the first blockchain technology, which introduced smart contracts. Smart contracts are applications where its state can be stored in the blockchain. They contain code and can interact with other smart contracts [But15].

Ethereum does not directly focus on SSI but due to its functionalities with support of smart contracts, it could be used as platform to realize such a system.

uPort

uPort is based on Ethereum and focuses on sovereign identity for people, businesses, organizations and devices. The platform currently consists of three components: mobile app, Ethereum smart contracts and developer libraries:

- **Mobile App:** creation of self-sovereign identity and storing of the user's keys.
- **Smart Contracts:** are the core functionalities and provided by Ethereum. It contains the logic that is required to recover the user's identity if the mobile phone is lost or broken.
- **Developer Libraries:** provide a number of open protocols for signed messages and message flow.

An identity can be cryptographically linked to off-chain data stores. Each identity is capable of storing the hash of an attributed data blob, whether on IPFS, Azure, AWS, Dropbox, etc., which is where all data associated with that identity is securely stored. Identities are capable of updating this file themselves, such as adding a profile photo or a friend, or they can also grant others temporary permission to read or write specific files [LHT⁺16].

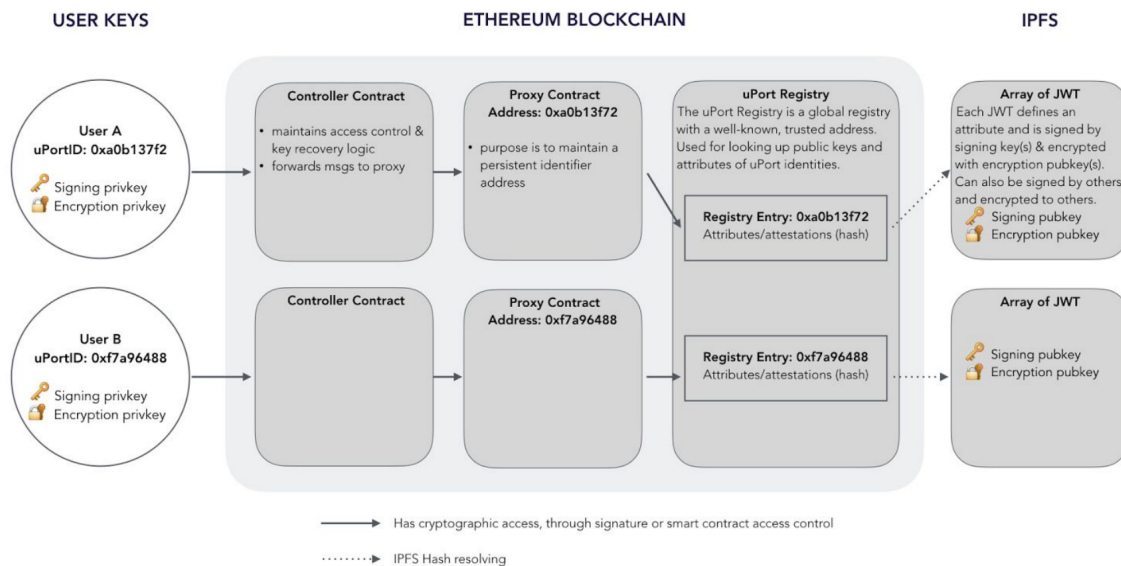


Figure 4.6.: uPort architecture with its information flow and the different contracts [LHT⁺16].

The uPort identifier is a 20-byte hexadecimal string that acts as a globally unique and persistent identifier. When the user wants to interact with a particular application smart contract, they send a transaction through the Proxy contract, via a controller contract, which contains the main access control logic. The proxy contract then forwards this transaction to the application smart contract. This architecture allows the application to view the proxy contract address as the interacting entity.

¹⁰<http://www.ethdocs.org/en/latest/introduction/index.html>

4. Self-Sovereign Identity

The Proxy contract as the core identifier allows the user to replace their private key while maintaining a persistent identifier. If the user's uPort identifier instead was the public key corresponding to their private key, they would lose control over their identifier if they were to lose the device where the private key is stored. In the case of device loss, the controller contract maintains a list of recovery delegates that can help the uPort user recover their identity.

4.3. Comparison of SSI Systems

4.3.1. Criteria

The criteria have been derived from the functional requirements of a SSI system and are based on the assessment performed by [Abr17]. These criteria are then used to assess the SSI systems introduced in Section 4.2.

- **Deployment Type (public/private):** permissionless (public) blockchains prove the consensus of the data with the proof-of-work usually solving a cryptographic problem such that no trust relationship between the parties is required. In permissioned (private) blockchain the proof-of-work does not have to be a difficult to solve cryptographic problem, *i.e.* transactions can be confirmed within a short timeframe. The permissioned entities have to be semi trusted or at least the authority, which decides if an entity becomes an authorized entity with write-access to the ledger.
- **Consensus Algorithm:** this criterion describes the proof-of-work approach which ensures the consensus of the blockchain to prove that the new blocks are valid before they are added to the chain. Depending on the deployment type, different consensus algorithms can be used.
- **Key Management:** evaluates the key management which is used for several operations such as encryption or signature operations.
- **Identity Data Import:** describes how the technology supports the import of the user's identity attributes.
- **Selective Attribute Disclosure:** describes if the technology supports selective disclosure. Selective disclosure is increasing the user's privacy by only disclosing the necessary information to the requester.
- **Data Storage:** depending on the blockchain technologies the data is stored in the blockchain whereas others use different storage approaches.
- **Trust Level:** describes the trust situation which can differ depending on the blockchain being public/private or permissioned/permissionless.
- **Identifiers:** evaluates the used identifiers of a blockchain technology.
- **Smart Contracts:** evaluates the support of smart contracts.

4.3.2. Evaluation

Sovrin

- **Deployment Type:** *Permissioned.* Two types of nodes are defined which are responsible and authorized for read and write operations to the ledger. The observer nodes are responsible for the read operations from the ledger and the validator nodes handle the write operations. Additionally, the observer keeps the ledgers synchronized between them and the observer nodes.
- **Consensus Algorithm:** *No.* Consensus protocol is implemented by the open source protocol Plenum (Byzantine Fault Tolerant Protocol) which is optimized for security and scalability. Because the ledger is permissioned, a difficult computation to calculate the proof-of-work is not required.

4. Self-Sovereign Identity

- **Key Management:** *Decentralized Public Key Infrastructure (DPKI)*. An identity owner uses keys, which are stored in a keychain, while the keychain itself is stored in a DPKI. Approaches for key discovery, rotation, revocation and recovery are defined.
- **Identity Data Import:** *Proprietary Sovrin Data Format*. The data format is defined by the Sovrin platform. In order to enable selective disclosure, each identity attribute has to be individually signed.
- **Selective Attribute Disclosure:** *Yes*. If authenticity is required each attribute has to be individually signed.
- **Data Storage:** *on- & off-ledger storage*. The platform supports two options: on- and off-ledger storage. Depending on the type and nature of the data *e.g.*, identity data, keys, transaction proofs and links are stored on-ledger, while other digital data can be stored off-ledger.
- **Trust Level:** *Yes*. Trust in the Sovrin foundation is required because they govern the board of trustees which decides and approves who is going to be a steward. A steward is a trusted entity, which is performing operations on the ledger. They can take the role of observer and validator node.
- **Identifiers:** *Key(Decentralized Identifier, DID) / Value(DID Description Object, DDO)*. Key-value pairs are used to identify the identity owner on the ledger. The design of DID records removes the dependency on a central authority.
- **Smart Contracts:** *No*, not supported.

Blockstack

- **Deployment Type:** *Permissionless (public)*. Is built on top of Bitcoin blockchain. Therefore, public access to Blockstack core is needed, if running as a node in the Blockstack network.
- **Consensus Algorithm:** *Yes*. Mining is performed on the Bitcoin blockchain.
- **Key Management:** *Distributed Key Management (DKM)*. Distributed key management, where the public keys are stored in the virtual layer.
- **Identity Data Import:** *self-entered*
- **Selective Attribute Disclosure:** *Yes*
- **Data Storage:** *off-ledger*. Based on the storage layer which uses external infrastructure.
- **Trust Level:** *No*. No trust required, due to the underlying Bitcoin and public blockchain.
- **Identifiers:** *Files*. Identifiers are stored as zone files in the routing layer while the binding zone file to name is stored in the virtual chain layer.
- **Smart Contracts:** *No*, not supported.

Multichain

- **Deployment Type:** *Permissioned (private)*. Based on a Bitcoin fork offering the possibility to run as private blockchain.
- **Consensus Algorithm:** *Yes*. Due to the restriction of allowed entities to mine, a lightweight and less complex PoW calculation can be applied. In order to ensure a consistent PoW calculation (*e.g.*, that one miner can not monopolize the mining process), a specific mechanism "mining diversity parameter" has been implemented, which is basically a constraint on the number of blocks a miner can create.

4. Self-Sovereign Identity

- **Key Management:** *Local Wallet / External Hardware*. Multichain offers two options: (1) build-in wallet to store the encrypted private keys, or (2) off-ledger on a external hardware security module/computer.
- **Identity Data Import:** *self-entered / self-signed*
- **Selective Attribute Disclosure:** *Yes*. Supported by the stream feature¹¹ of Multichain.
- **Data Storage:** *on-ledger*. Any data is stored on the blockchain. The size of the information is restricted to 64MB per transaction.
- **Trust Level:** *No*. Each transaction includes a proof of authorization and proof of validity.
- **Identifiers:** *on the blockchain*. Identifiers are encoded and stored within each transaction.
- **Smart Contracts:** *No*, not supported

Ethereum

Ethereum is the underlying blockchain technology, which enables the realization of SSI systems. For this reason, the technology is not evaluated as an SSI system.

uPort

- **Deployment Type:** *Permissionless (public)*
- **Consensus Algorithm:** *Yes*. Based on the underlying Ethereum blockchain.
- **Key Management:** *DPKI*. Private key is stored on the mobile phone of the user and the public key on the distributed storage in order to support the decentralized public key infrastructure.
- **Identity Data Import:** *Self-entered & self-signed*. uPort supports a method to include a signature to prove the attestation. These attributes can be signed by a qualified authority or simply just self-signed.
- **Selective Attribute Disclosure:** *Yes*
- **Data Storage:** *off-ledger*. Data is stored off-ledger (*e.g.*, Azure, Dropbox, etc) while the identities are cryptographically linked to the off-chain data stores.
- **Trust Level:** *No*
- **Identifiers:** *uPort identifier*. The uPort globally unique and persistent identifier is the address of an Ethereum smart contract (proxy contract). The identity is using this proxy contract to interact with other smart contracts on the blockchain.
- **Smart Contracts:** *Yes*

Summary

Table 4.1 shows a consolidated view of the properties of interest. The summary does not give a complete view of all properties. It is limited to the technical properties and makes no statement about the suitability in the intended field of application.

Based on this technical characterization, the next step is to identify the best possible solution in the context of the requirements of the financial industry. In the next Chapter 5, the technical and functional arguments are compared with the existing solutions to be able to make a possible recommendation.

¹¹<https://www.multichain.com/developers/stream-confidentiality/>

4. Self-Sovereign Identity

Name	Sovrin	Blockstack	Multichain	uPort
OpenSource	Yes	Yes	Yes	Yes
License	Apache2 License	GPL v3 License	GPL v3 License	Apache License Version 2.0
Blockchain	DLT	Bitcoin	Fork of Bitcoin	Ethereum
Deployment Type	Permissioned (private)	Permissionless (public)	Permissioned (private)	Permissionless (public)
PoW	No	Yes	Yes	Yes
Key Management	DPKI	DKM	local wallet / HW	mobile phone/ DPKI
Identity Data Import	Sovrin Data Format	self-entered	self-entered & self-signed	Yes
Selective Disclosure	Yes	Yes	Yes	Yes
Data Persistency	on- & off-ledger	storage layer (external)	Blockchain (< 64 MB/Trx)	off-chain
Trust Required	Yes	No trust required	No trust required	No trust required
Identifier	key: DID value: DDO	files on the routing layer	on transaction	uPort identifier
Smart Contracts	No	No	No	Yes

Table 4.1.: Overview of the technical assessment.

4.4. Discussion

We can assume that SSI systems provide scalable, flexible, private interactions with consent despite the issues that distance introduces. More importantly, they support natural human activities without threatening the privacy or liberty of people who use them. There are several self-sovereign identity systems existing now in various stages of development. Each of these support decentralized, self-sovereign identity but differ in how claims are issued and information is stored. New systems are in development which seem to be promising from a technical perspective, *e.g.*, Veres One¹² or VALID¹³, but are in an early premature state to be considered.

4.4.1. Limitations

It would be naive to think that blockchain technology would solve the existing problems and issues in no time at all. Blockchain as a native technology has many interesting features, which are – when correctly implemented and applied – promising to help in finding an ideal solution for the “self-sovereign identity” concept. In the article [Hal17], five problems have been addressed which blockchain does not solve.

1. **Immutability:** The immutability of a blockchain has only limited validity. Theoretically, a “51% attack” would allow an actor who controls 51% or more of the mining power on the network, to hijack and overwrite transactions on the blockchain. Depending on the size of the network, number of miners, and deployment type, it is a valid argument. The risk of deploying and trusting a public blockchain at scale for sensitive transactions when it could be undermined by a state actor is too high a risk to make a public blockchain for identity a viable approach. Private blockchains have mechanisms that can potentially overcome this challenge but then it is a consortium control model.
2. **Synthetic Identity:** One important process step of the digital identity lifecycle is the control of the uniqueness of the claimed identity. The blockchain is the underlying ledger and does not verify nor issue identities.

¹²<https://veres.one/>

¹³<https://valid.global/>

4. Self-Sovereign Identity

As a ledger, blockchain depends upon the integrity of the inputs to the ledger, and, if the inputs are wrong, then the ledger will simply record the synthetic identity on the ledger.

3. **Identity Verification:** Once an identity is established as real and unique, the next challenge is to ensure that the user claiming the identity is in fact the rightful owner of that identity. The verification of an identity is not a technical issue, it has to be covered by the implemented business processes. Depending on the process, it can happen, that an actor gains control of a real person's identity, then blockchain cannot stop that actor from exploiting that person's identity because authentication and identity proofing happen upstream.
4. **Demographics:** Issuing strong digital credentials at scale can not be solved by the blockchain technology. Identity proofing and authenticating different groups (*e.g.*, students, seniors, welfare recipient, etc.) is difficult. Younger consumers do not typically have a financial history and may not have a significant government records trail. Seniors tend to have the opposite challenge as validating and verifying the identity is easier. However, older people tend to have less computer experience and fewer devices that would help them authenticate.
5. **Standardization:** In the public and private sector, much efforts to collaborate on identity proofing have not been successful because organizations do not trust one another. Almost all regulated entities require their customers to create a login with them directly. There are a few reasons why most organizations do not share data across, *e.g.*, large organizations view identity as a moat around their business and sharing an individual's data across organizations removes friction (*e.g.*, lowering switching cost), or many organizations do not trust other organizations to follow processes and procedures that they deem acceptable. That means, that the identity providers (*e.g.*, banks or telecoms) would need to accept a lot of risk, potential liability, and uncertainty in order to participate in an identity ecosystem.

Many of these limitations can only be ascribed to the blockchain technology to a limited extent, but have to be solved by the processes and applications implemented on it.

5. Impact and Opportunities in the Financial Industry

There are various initiatives investigating how to incorporate new technologies into existing business processes in the financial industry (*e.g.* [PBPW18]). Many approaches so far have focused primarily on the settlement of transactions and the question of how blockchain technology can be used (*c.f.* Section 2.2.1). In this context, the existence of a digital identity is fundamental but not the way it is created or the question of ownership. However, self-sovereignty has not yet been in focus of these solutions.

As mentioned briefly in the introduction (Section 1), a reliable digital identity is essential to the broader financial services industry to improve core financial services processes and delivery of financial products. The need for a digital identity is becoming increasingly important. In [For16] five key trends have been identified, which increase the need for a sustainable solution in the near future.

1. **Increasing transaction volumes:** The number of identity-dependent transactions is growing through increased use of the digital channel and increasing connectivity between entities.
2. **Increasing transaction complexity:** Transactions increasingly involve very disparate entities without previously established relationships (*e.g.*, customers and businesses transacting cross-border).
3. **Customer expectations:** They expect seamless, omni-channel service delivery and will migrate to services that offer the best customer experience.
4. **Regulatory requirements:** Regulators are demanding increased transparency around transactions, meaning that financial institutions require greater granularity and accuracy in the identity information that they capture and are increasingly being held liable for inaccurate or missing identity information.
5. **Financial/Reputational damage:** Bad actors in financial systems are increasingly sophisticated in the technology and tools they use to conduct illicit activity, increasing their ability to quickly cause financial and reputational damage by exploiting weak identity systems.

In addition to the technical requirements described in Section 4.1.1 and 4.1.2, there are also the functional, financial industry specific requirements [For16]. The critical, high-level characteristics that are required by the financial industry for strong identity systems are the following:

- **Operational Efficiency:** The system allows digital transactions to be completed conveniently and effectively.
- **Scope & Scale:** The system enables large volumes of transactions through provision of transaction-critical attributes and connecting large numbers of users with important and frequently used service providers.
- **Security:** The system prevents user information from being overexposed, lost or stolen.
- **User Control & Privacy:** The system allows users to determine where their information is held and when it is shared or exposed.
- **Viability:** The system delivers value to all stakeholders, creating broad support and uptake and making it a commercially viable system.

From a digital identity concept view, the two requirements "Security" and "User Control & Privacy" are critical. Based on the existing systems (see Section 3.2), these two requirements are difficult to fulfill. In this regard, the concept of SSI is of fundamental importance to achieve these two requirements and plays an important role. Combining technical capabilities of blockchain technology to solve the functional requirements of financial industry could lead to an interesting corporation because the financial institutions are well positioned to drive identity systems that fill the gaps left by current solutions.

5.1. Role

The financial industry plays an important role in identifying and assessing its customers. Regulatory requirements have been tightened over the last few years, with the result that investments in systems for the correct identification and classification of customers are constantly increasing.

The financial institutions already act as a store of customer information for their own commercial purposes, therefore, are positioned to act as identity providers (IdPs) without extensive incremental effort. Their infrastructure, business processes and integrated functionality allows to collect accurate user information and verify them accordingly [SDE18]. An important point is the coverage of the user population. The financial institutions have almost a near-complete scope of users as natural persons, legal entities and assets. Additionally, global institutions have interconnected operations across multiple jurisdictions, providing them a structural advantage towards cross-jurisdictional identity transactions and systems, making the systems complex. Due to this increased complexity, IT departments are used to act flexible, agile and reliable in implementing new systems and standards.

Taking all this structural advantages into consideration, the positioning of the financial institutions can be summarized as follows:

- **Trusted Partnership:** Financial institutions have a long experience in validating identities and are typically trusted by consumers beyond other institutions as safe repositories of information and assets. After public providers, in the private sector financial institutions are the most reliable and they have to take advantage of this situation.
- **Capability & Reliability:** Operations and use of customer data are rigorously regulated such that they are used to dealing with compliance standards, *e.g.* regulations are increasingly requiring banks to do due diligence tasks on their customers in an effort to trace money laundering.
- **Service Provider:** They act as established intermediaries in many transactions and are therefore well positioned to act as identity intermediaries.

In addition to all these functional and structural advantages, the question of commercial aspects arises. These questions are discussed in the Section 5.2.

5.2. Business Case

The starting position of the financial institution for active participation in the creation and verification of the digital identity is given. They could derive substantial benefit from investing in the development of digital identity solutions. In principle, the advantages can be classified into three categories [For16]:

1. **Efficiency & Cost Avoidance (existing services):** Today's client data capturing, identification and verification business processes are still primarily based on the classic paper-based approach. These are cumbersome, error-prone, leading to many manual intervention and are costly. Transformation in the direction of digitization is a good opportunity to streamline current processes, increase automation, and reduce error and human intervention (straight-through-processing)¹.

¹*c.f.*, Appendix "Business Problems in the Financial Industry" A.2

2. **New revenue opportunities (new services):** Once new digital processes have been implemented and collect reliably the required customer data, these can be used to offer new products and services based on increased knowledge of customers (*e.g.*, extended financial advisory). The most important new revenue case is the offering of the identity as a service to relying parties who cannot or do not wish to store customer information. Additionally, the offering of a digital identity is to be decoupled from existing business processes and to be offered as dedicated, fee-based services for individuals who do not transact with the financial institute. In the case of a "self-sovereign" digital identity model, the range of services could be easily extended (*c.f.*, Section 5.3).
3. **Expansion of business areas (services beyond the current business areas):** expanding current business areas will fundamentally transform the known business models. For example, the liability of incorrect client information will shift from the financial institution to other entities in the network, or shift the evaluation of the clients creditworthiness based on accurate identity data including financial history rather than relying on third parties and trying to consolidate multiple data sources. Also the partnership to the public sector will change as the financial institutions will become a trusted identity provider of the public sector.

In today's banking world, stage (1) "Efficiency & Cost Avoidance" area is the main focus. Various digitization projects have been initiated with the aim of optimizing existing front processes (customer-oriented processes) and digitizing them as far as possible. Unfortunately, there are currently no focused activities towards stage (2) nor stage (3).

The concept of "self-sovereignty" of digital identity has not yet been taken up specifically - at least not in the Swiss banking world. The current approaches rely on centralized or federated deployment models. For example:

- **SwissSign²:** is an initiative driven by the Swiss Post and the SBB with the scope to establish digital identities based on one central identity provider (SwissSign) and multiple attribute providers.
- **eID:** is initiated by UBS, Credit Suisse and Swisscom. The aim is to build a federated system where customers can choose between multiple identity providers with focus on authentication, attribute sharing, signature and payment services.
- **Identity Network Switzerland³ (IDV):** initiated by the State Secretariat for Economic Affairs (SECO) and AdNovum. The goal of this solution is to simplify electronic processes with authorities by connecting public administrations. The infrastructure is open to be used by the private sector as well.

Taking the current evolvement of the digital identity into consideration (*c.f.*, Section 4.1.1), the digital identity is inevitably moving in the direction of "self-sovereignty".

5.3. Improved and Novel Capabilities

Taking the basic technical characteristics of blockchain into consideration and putting them in relation to the requirements of the financial industry with the assumption that the digital identity is evolving towards a self-sovereign model, a comprehensive platform seems to be feasible.

5.3.1. Platform selection:

- **Sovrin:** Out of all evaluated technologies in Section 4.2, Sovrin provides most of the required functionality when developing a self-sovereign identity system. It has to be considered, that Sovrins design is made to realize SSI systems. The lack of support for smart contracts may be a long-term problem, but it is currently not a serious concern. In contrast, Blockstack, Multichain, Ethereum and uPort have significant deficiencies.

²<https://www.swissid.ch/de>

³<https://www.idv-fsi.ch/>

5. Impact and Opportunities in the Financial Industry

- **Ethereum:** offers a powerful platform to develop distributed application using smart contracts. However, the platform itself would only provide the basis.
- **uPort:** is built on Ethereum with focus on self-sovereign identity. Nevertheless, it could be a valuable candidate in the future, but has not yet reached the stage of enterprise readiness.
- **Blockstack:** focus on decentralized domain name service by combining different layers and parts of already existing infrastructure such as Bitcoin blockchain for the blockchain layer or Dropbox for the storage layer. The usage for SSI might be more difficult than using Sovrin.
- **Multichain** provides a platform that allows running several different private blockchains in parallel providing a built-in permission management system. Nevertheless, the focus here is not directly on SSI and the usage for such a system might be easier using Sovrin.

Business Model for the Financial Institutions:

With the introduction of a self-sovereign identity model, the business model will not change significantly, but there are some differences. First of all the data of the digital identity then belongs to the customer, which is the owner of the data and has the full control of them. The financial institutions will have to adapt their business processes by decoupling and encapsulating the customer data capturing and verification process to enable a seamless integration. Digital identity can then be offered as "identity-as-a-service" to the clients and non-bank clients. This is an opportunity to monetize the "identity-as-a-service" concept. Especially the more complex and expensive KYC (know-your-customer) processes are here in focus, *e.g.* client risk scoring, world-check, etc. which each bank is processing redundantly.

Due to the open model of the self-sovereign identity concept and data standards, it will reduce the barriers to users to switch institutions. This fact will change the focus of the business to a more client-centric view, offering better digital services (*c.f.*, Section 5.3.2).

5.3.2. SSI Potential

The potential of the underlying technology of SSI systems is still far from being reached. A SSI system decreases the required trust, compared to traditional identity management systems, by using the distributed ledger technology.

Beyond the obvious benefits of digital identity that financial institutions would receive as a result of participating in an identity system, some future-looking use cases illustrate additional possible capabilities that digital identity might offer:

- **International Resettlement:** transport the digital identity across jurisdictions and use to easily gain access to financial and other services in the new place of residence. This would eliminate the need for the recipient financial institution to perform the costly KYC-process. It also would reduce the time and effort needed to onboard users, and allow them to incorporate trusted, historical information.
- **Digital Tax Filing:** In collaboration with governments, taxes could be automatically completed and filings generated by customers' chosen financial institution, using their complete knowledge of customers' financial holdings, assets, income and personal circumstances.
- **Determining total Risk Exposure:** Transaction counterparties could have a consolidated view of the corporate structure of the entities with which they are transacting, allowing them to determine their total risk exposure to that entity across transactions and lines of business.
- **Linking individual identity to corporate identity:** The digital and standardized collection, storage and transfer of attributes for both individuals and legal entities would ensure identity information is accurate and up-to-date. Linkages between these systems would create reliable pictures of the identities of individuals affiliated with legal entities for know-your-customer and other purposes.

5. Impact and Opportunities in the Financial Industry

- **Tailored Risk Profiles:** with user's consent, financial institutions could leverage trusted user attributes, to build more effectively risk profiles for their customers and therefore tailor credit- and risk-based products. This enhanced user experience would hopefully lead to increased customer stickiness.

However, there is another interesting aspect that is (partially) solved by the SSI approach: the General Data Protection Regulation⁴ (GDPR) [Par16]. The GDPR aims to increase data protection and data privacy of each individual citizen within the EU, where an SSI system can support the GDPR compliance when dealing with digital identities. In the following a brief summary of how the SSI system can fulfill certain GDPR articles, *e.g.*:

- **Consent:** a user must give explicit consent in order to process and collect the user's data. The SSI management system can provide the required user interfaces providing fine granular control over what data are being shared together with revocation mechanisms. Depending on the blockchain type, smart contracts could be used to enforce the user's consent decisions.
- **Right to Erasure:** In a SSI system, the user fully owns the identity data, therefore the user can simply delete the whole identity and its related data. The erasure is realized by not storing any private data in a public accessible place such as the decentralized ledger itself. Instead, only identifiers, linked to identity data, are stored in the ledger. The access relies on the user's consent and is enforced by SSI consent mechanisms. The consent mechanism also enables the revocation of previously granted data access.
- **Data Portability:** This possibility is enabled because the SSI system combines different technologies that enable the data portability such as the distributed ledger with standardized data exchange formats.
- **Data Protection by Design and by Default:** The SSI system implements state-of-the-art techniques for both to preserve the user's privacy as well as to protect the processed data. One of these state-of-the-art techniques are Zero-Knowledge Proofs (ZKP), which allow an identity owner to prove the correctness of identity specific elements without revealing any unnecessary additional information. For instance, by proving the possession of a driving license without disclosing the complete driving license.

5.4. Discussion

The impact of the SSI-based digital identity on the existing business areas of the financial industry should not be underestimated. As shown in Section 5.1, the financial industry is in an attractive situation to play a dominant role in shaping the design of the digital identity and also to expand their own business fields.

Sovrin as an underlying technology cannot meet all the expectation right from the start, but in the future it may have to be adapted to the new circumstances and developed further. The concept of self-sovereign identity is relatively new, and the development of SSI systems is in a early stage. It will certainly change in the near future, but at the moment Sovrin meets many technical and functional requirements as a platform. The fact, that Sovrin is of a private/permissioned blockchain deployment type helps to establish the technology and the concept, because a trusted network is a more reliable model nowadays. Once the trust of the users and the technical stability of the platform have been proven, the next logical step will be towards open systems.

⁴On 25th May 2018 the regulation entered into force in all European Union member states

6. Final Considerations

”Blockchain technology” and ”Digital Identity” are currently trending topics in the IT world, and it is not only technically interesting but is also attractive from a business perspective. The combination of blockchain and self-sovereign digital identity introduces a new system for preserving client’s credentials for their public & financial services. 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.

As shown in Section 4 and 5, self-sovereign identity based on blockchain offers a full range of new functional capabilities for less operational costs, increased efficiency leading to higher customer satisfaction. The selection of Sovrin as the underlying blockchain technology may not be the most technically sophisticated option, but it is a pragmatic decision and it meets the requirements as far as possible. Independent of all that, there are still some remaining challenges to be solved in the near future.

6.1. Remaining Challenges

The blockchain technology as it is used today in this form is still young, as well as the concept of self-sovereign identity implemented in a public deployment model. Nevertheless, some problems still remain, which will challenge the ”self-sovereign identity on blockchain” concept in the future, *e.g.*

- **Maturity level of blockchain technology:** regardless of the advantages of blockchain (decentralization, immutability, public) there are still some concerns about the maturity level. As mentioned in Section 2.3, further development is needed, especially in performance and scalability. For example, in a public deployment model and blockchain type, 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.
- **Trust:** an important, non-technical point. Even if the technology is excellent and provides new capabilities in comparison to existing systems, it is not yet being used to the same extent as it would be necessary in the financial industry¹. It should be noted that many larger banks are still working on legacy systems (*e.g.* PL/1 or COBOL based on overnight batches), processing reliably billions of transaction every day. Therefore, new disruptive technologies and concepts are always considered to be suspicious and are carefully evaluated. Should the ”enterprise readiness” have been proven, the technology and concept will be realized in a short time.
- **Security:** any new technical architecture also introduces new cybersecurity risks, and blockchain poses some weaknesses. The type and amount of data stored in the blockchain affects the risk profile, as well as the authorization mechanisms used, especially the smart contracts that are vulnerable to cybersecurity risks.

Apart from these more technical problems, other conceptual questions arise regarding the implementation of such a ”self-sovereign” digital identity system, *e.g.*,

- **Scope of User Group:** The more different groups (*e.g.* governments, regulators, financial institutions, etc) are involved – some of them also acting in their own interests – the more difficult it becomes to agree on a common model. Finally, any compromises usually reduce the functionality and delay the development.

¹seems to be a typical chicken-and-egg problem

6. Final Considerations

- **Governance Structure:** This is an important point, which is to be defined in an early stage. Especially, in a permissioned/private deployment model, this question has to be clarified in detail.
- **Business Model:** it is not clear if the assumptions about the business case will be sustainable. The underlying business case must be regularly re-evaluated and revised.

A. Appendix

A.1. Blockchain-based identity management and authentication solutions for cross-industry applications

- **2WAY.IO** effectively transforms public nodes into private nodes by adding a permissions layer. Private nodes can connect information silos and secure communication channels. They are user-in-control (privacy-by-design and security-by-design) and require no trade-off between security and UX. These systems are both trusted third-party- and blockchain-agnostic; they only require an intermediary or blockchain when both parties agree to add one to their interaction (<http://www.2way.io/>).
- **Atencoin** is a first-generation, identity-based compliant digital currency. It is headed up by the National Aten Coin (NAC) Foundation, an organization that supports the identification of blockchain-based technology and digital currencies ([AMLBitcoin-Whitepaper](#)).
- **BlockAuth** enables users to own and operate their own identity register that allows them to submit their information for verification (<http://blockauth.org/>).
- **Blockstack** provides a decentralized domain name system (DNS), decentralized public key distribution system, and registry for apps and user identities. Personal user APIs ship with the Blockstack app and handle everything from identity and authentication to data storage. Applications can request permissions from users and then gain read-and-write access to user resources ([[ASNFI7](#)]).
- **Bitnation** is a governance 2.0 platform that is 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 an identification solution such as blockchain passport and a marriage certificate (<https://tse.bitnation.co/>).
- **BlockVerify** provides blockchain-based anti-counterfeit solutions. It uses blockchain technology to improve anti-counterfeit measures in different industries such as pharmaceuticals, luxury items, diamonds and electronics (<http://www.blockverify.io/>).
- **Cambridge Blockchain LLC** is developing its digital identity software with several leading global financial institutions, with commercial deployments planned for late 2017. The company's distributed architecture resolves the competing challenges of transparency and privacy, resulting in faster customer onboarding, lower costs, and enhanced compliance through a single, trusted and consistent view of customer reference data. Cambridge Blockchain has won FinTech competitions including BBVA Open Talent 2016 and the Santander InnoVentures Distributed Ledger Challenge. Cambridge Blockchain graduated from the 2016 FinTech Innovation Lab run by the Partnership Fund for New York City and Accenture (<https://www.cambridge-blockchain.com/>).
- **Civic** is a blockchain-based identity management platform that allows users to register and validate their personal identity information and lock their identity in order to prevent identity theft and fraudulent activity on their credit reports. Civic aims to tackle the problem of consumer identity theft and reducing online identity fraud (<https://www.civic.com/>).
- **Credits** platform enables enterprises to quickly and easily build robust blockchains that address the challenges of establishing provenance, authentication and reconciliation faced by many industries. The platform

A. Appendix

allows to create encrypted digital identities to substitute dozens of usernames and passwords while offering greater security features would save enterprises, institutions, governments and customers, time, energy and money. A golden record for identity which would work not only at a bank level but across the globe in all electronic environments (<https://credits.com/>).

- **CredyCo** provides document verification SaaS, which uses a smart contracts and identity technology built on top of the blockchain to ensure the credibility and irrefutability of all statements (<https://www.credy.co.id/>).
- **Cryptid** eliminates the possibility of counterfeit identification by adding factors of identification and encryption. Cryptid takes the data provided in the form and package it into a compact format readable by our systems and generate your Cryptid identification data. 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 block chain and can be stored on almost anything from magnetic stripes to QR codes (<https://cryptid.xyz/>).
- **Evernym** is built on Sovrin, a private-sector, international non-profit solution 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 (<https://www.evernym.com/>).
- **ExistenceID** is a secure digital identity system for safe storage and sharing of valuable identity documents. A private identity capsule rates users total identity so they can prove that they are real. Only users choose who and when can access different parts of their identity. At the same time, ExistenceID has zero knowledge of users personal account (<https://existenceid.com/>).
- **Guardtimes BLT** – Blockchain Standard for Digital Identity is an authentication and signature protocol meant to replace RSA as the standard for digital signatures. In contrast to RSAs reliance on quantum-vulnerable asymmetric key cryptography, BLT is based on Guardtimes quantum-secure Keyless Signature Infrastructure (KSI) technology, which uses only hash function cryptography (<https://guardtime.com/technology>).
- **HYPR** biometric security suite provides enterprises a fully interoperable solution to secure users across mobile, desktop and IoT systems. HYPR enhances the user experience by allowing you to choose from voice, face, touch and eye recognition. The decentralized authentication platform allows enterprises to leverage biometrics without worrying about hackers attacking a biometric server or centralized password database (<https://www.hypr.com/biometric-bitcoin-blockchain/>).
- **Identifi** is a blockchain-based startup creating address book where users can link their personal profiles and identifiers to form a trusted identity. In addition to keeping contact details such as phone number or bitcoin address up-to-date, the user can give other users trust ratings and feedback (<http://identifi.github.io/>).
- **Open Identity Exchange (OIX)** is a non-profit, technology agnostic, collaborative cross-sector membership organization with the purpose of accelerating the adoption of digital identity services based on open standards (<http://www.openidentityexchange.org/>).
- **OIXNet** is a registry. It is an official online and publicly-accessible repository of documents and information relating to identity systems and identity system participants. Referred to as a registry, it functions as an official and centralized source of such documents and information, much like a government-operated recorder of deeds. That is, individuals and entities can register documents and information with the OIXnet Registry to provide notice of their contents to the public, and members of the public seeking access to such documents or information can go to that single authoritative location to find them (<http://www.oixnet.org/>).

A. Appendix

- **KYC-Chain** is a novel platform built over 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 (<https://kyc-chain.com/>).
- **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 (<https://netki.com/>).
- **ShoCard** is a digital identity that protects consumer privacy and is as easy to understand and use as showing ones drivers license. Its optimized for mobile and so secure that even a bank can rely on it. A users identity is encrypted, hashed and then written to the blockchain, where it can be called up when needed. Users would, in effect, give banks temporary access to the private side of this blockchain record in order to verify identity. Once that is done, the bank creates its own record that can be consulted in the future to determine that a certain Joe Smith really is Joe Smith (<https://shocard.com/>).
- **UniquID** provides secure identity management, integrated with fingerprint and other biometry on personal devices. Ready to be deployed on custom hardware, servers, personal computers or smartphones and tablets, UniquID Wallet runs also on battery and low-powered devices, providing integrity and interoperability at the edge of ones infrastructure (<http://uniquid.com/>).
- **uPort**, developed by ConsenSys, is building a secure, easy-to-use system for self-sovereign identity, built on Ethereum. The uPort technology consists of three main components: smart contracts, developer libraries, and a mobile app. The mobile app holds the users keys. Ethereum smart contracts form the core of the identity and contain logic that lets the user recover their identity if their mobile device is lost. Finally, the developer libraries are how third-party app developers would integrate support for uPort into their apps ([LHT⁺16]).

A.2. Business Problems in the Financial Industry

Business problem	Retail / small- to medium-sized enterprise banking	Corporate and investment banking
Inefficient and costly onboarding processes	✓	✓
Inefficient, costly and ineffective know-your-customer (KYC) and due diligence processes	✓	✓
Highly manual and time-consuming compliance processes	✓	✓
Difficulty aggregating information on legal entities and determining total risk exposure	✓	✓
Difficulty attaching individual identity (e.g. corporate directors) to corporate identities	✓	✓
Difficulty identifying all transaction counterparties (e.g. third parties in trading relationships)	✓	✓
Difficulty complying with regulatory standards around data handling and privacy	✓	✓
Multiple views of the customer	✓	✓
Difficulty providing effective/suitable products and services	✓	
Lack of visibility into financial history for new customers	✓	
High fraud rates	✓	
Difficulty tracking asset origination and ownership		✓
Difficulty monitoring and tracking asset rehypothecation		✓

Figure A.1.: Examples of business problems in the finanacial industry [For16].

Bibliography

- [Abr17] Andreas Abraham. Self-Sovereign Identity. White Paper, E-Government Innovationszentrum, October 2017.
- [All16] Christopher Allen. *The Path to Self-Sovereign Identity*. April 2016.
- [Ant17] Lewis Antony. *A gentle introduction to self-sovereign identity*. May 2017.
- [ASNF17] Muneeb Ali, Ryan Shea, Jude Nelson, and Michael J. Freedman. Blockstack: A New Internet for Decentralized Applications. White Paper, October 2017.
- [BB16] Jeroen Bulters and Jacob Broersma. Blockchain the benefits of smart contracts., November 2016.
- [Bou16] Philip Boucher. What if blockchain technology revolutionised voting? Article, European Parliamentary Research Service, September 2016.
- [But15] Vitalik Buterin. On Public and Private Blockchains, August 2015.
- [CDD⁺16] Julia Clark, Mariana Dahan, Vyjayanti Desai, Marta Ienco, Stephanie de Labriolle, Jean-Pierre Pellestor, Kyla Reid, and Yolanda Varuhaki. Digital Identity Towards Shared Principles for Public and Private Sector Cooperation. Discussion Paper, A joint World Bank Group GSMA Secure Identity Alliance, July 2016.
- [CNP⁺16] Michael Crosby, Nachiappan, Predhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. Blockchain Technology: Beyond Bitcoin. Technical Report, Sutardja Center for Entrepreneurship & Technology, Berkley, University of California, October 2016.
- [Del16] Deloitte. A blueprint for digital identity. Technical report, Deloitte, 2016.
- [For16] World Economic Forum. A Blueprint for Digital Identity 2016. Technical report, World Economic Forum, August 2016.
- [Gre15] Gideon Greenspan. MultiChain Private Blockchain. White Paper, 2015.
- [Hal17] Blake Hall. *5 Identity Problems Blockchain Doesnt Solve*. July 2017.
- [JL15] Kieren James-Lubin. Blockchain scalability, A look at the stumbling blocks to blockchain scalability and some high-level technical solutions., January 2015.
- [LHT⁺16] Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, and Michael Sena. uPort: a Platform for Self-Sovereign Identity. White Paper, Blockchainlab.com, October 2016.
- [noaa] Blockchain Technologies for Business.
- [noab] Blockchains & Distributed Ledger Technologies.
- [noa18] Project Stella: Securities settlement systems - Delivery versus payment in a distributed ledger environment. Article, European Central Bank and Bank of Japan, March 2018.
- [Par15] Luke Parker. Bitnation starts offering blockchain public notary service to Estonian e-Residents. Online Article, December 2015.

BIBLIOGRAPHY

- [Par16] European Parliament. Regulation of the European Parliament and of the Council on the protection of individuals with regard to processing of personal data and on the free movement of such data. REGULATIONS, THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, April 2016.
- [PBPW18] Daniel Proba, Marc Burkhalter, Ante Plazibat, and Johannes Wotzka. Innovationspark: Prototyp "Banking in a Smart City". Workshop, BEI, Business Engineering Institute St.Gallen, BEI, St.Gallen, February 2018.
- [Pla17] Ante Plazibat. Geschäftsmodell und Geschäftsmodellmuster im Kontext von Digital Identity. Technical report, BEI, Business Engineering Institute St.Gallen, BEI, St.Gallen, November 2017.
- [Sat08] Nakamoto Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical Report, bitcoin.org, 2008.
- [SDE18] Ana I. Segovia Domingo and Álvaro Martín Enríquez. Digital Identity: the current state of affairs. Working Paper, Banco Bilbao Vizcaya Argentaria, January 2018.
- [Ses17] Kikitamara Sesaria. Digital Identity Management on Blockchain for Open Model Energy System. Master's Thesis, Radboud University, Niederlande, August 2017.
- [Tho16] Collin Thompson. The difference between a Private, Public & Consortium Blockchain., October 2016.
- [TR16] Andrew Tobin and Drummond Reed. The Inevitable Rise of Self-Sovereign Identity. White Paper, Sovrin Foundation, September 2016.
- [VK16] Shermin Voshmgir and Valentin Kalinov. Blockchain Handbook: A Beginners Guide, September 2016.
- [Vos16] Shermin Voshmgir. Blockchains, Smart Contracts und das Dezentrale Web. White Paper, Technische Stiftung Berlin, Berlin, 2016.
- [Win18] Phillip Windley. How blockchain makes self-sovereign identities possible, January 2018.
- [Wol16] Stephan Wolf. Identifier Verification: Evaluation of Blockchain and Alternative Technologies. Presentation, LEI: Global Legal Identity Identifier Foundation, September 2016.
- [Woo14] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Yellow Paper, 2014.
- [WR18] Phil Windley and Drummond Reed. Sovrin: A Protocol and Token for SelfSovereign Identity and Decentralized Trust. White Paper, Sovrin Foundation, January 2018.