AALBORG UNIVERSITY
COPENHAGEN

**Semester: 4th**

**Title:** Role of Distributed Ledger Technology for the EU Digital Identity Wallet
**Project Period:** Spring 2021

Aalborg University Copenhagen
A.C. Meyers Vænge 15
2450 København SV

Semester Coordinator: Henning Olesen

Secretary: Maiken Keller

**Semester Theme:** Master Thesis

**Supervisor :**

Henning Olesen

**Member :**

Deema Lama

**Pages: 67**

**Total Pages: 76**

**Finished: 11th August, 2022**

**Abstract:**

This project looks into two core matters regarding decentralized identity management: The role of Distributed Ledger Technology (DLT) in the digital identity wallet ecosystem, ,and how DLTs can support principles of Self-Sovereign Identity.

In this study, the European Digital Identity Wallet has been taken as a reference to look into both core matters. Different available DLTs have been studied and compared to explore the viability of the DLTs in the wallet ecosystem. The research has been conducted in a qualitative way. The data were collected from secondary resources which are mainly journals, articles, white papers, and from an expert consultation.

The research findings/outcomes of this study show that there are some opportunities to use DLTS, however, the challenges prevail too. Despite the challenges, DLTs help in realizing the potential of the EU-DIDW in many ways such as the use of DLT as a data registry allowing storage of DIDs of users that provide a secure way of mutual authentication. Further, it can facilitate cross-border transactions in a simpler and less time consuming manner. It allows users to have control on different attributes of their personal information in a safe and secure manner.

*Keywords: Decentralized Identity, Distributed Ledger Technology, EU Digital Identity Wallet*

**When uploading this document to Digital Exam each group member confirms that all have participated equally in the project work and that they collectively are responsible for the content of the project report. Furthermore each group member is liable for that there is no plagiarism in the report.**

AALBORG UNIVERSITY
COPENHAGEN

## Table of Contents

# 1. Introduction

## Background

In our day-to-day life, we perform various transactions like opening a bank account, applying for universities, and purchasing tickets. As part of the transaction, officials and companies obtain pieces of our identity from documents, such as passports and identification cards. These documents like passports and driver's licenses, which we carry, and exchange are called credentials.

Before the internet, the global standard for credentials was paper-based. They were kept in the purse, in a safe, or in a drawer. When needed to prove your identity, they were presented to the requesters. This was done in physical presence, and it was easier to maintain a level of trust between the transacting parties.

After the internet, most of our interactions shifted from physical to online. While we are using online services, we create accounts for each. In time the number of accounts we use becomes more. Today, an average person has 191 online accounts [1]. At the same time, we have to fill up similar information every time we are creating online accounts for different online services. This doesn't provide a good customer experience as it is time-consuming and problematic to manage all these accounts. While we are giving more information about ourselves online, our data is fed into silos that can be misused, and sold to third parties along with data breaches [1].

With the work from home and increase in online business as a result of the COVID-19 pandemic, the useability of online services became inevitable more than ever [2]. Employees are provided a digital identity to access company resources and data, both on-premise and remotely. From a company's perspective, identity management can be done securely on-premise, but the complexity arises while tracking and validating remote data access.

According to a cybersecurity study done in 2020, "60 % of small-sized businesses that had employees working remotely experienced cyber-attack in the last year; out of these 56%

experienced identity theft, and 48% experienced phishing [3].” As remote working becomes the new norm, it is urgent to pay attention to creating a trusted digital identity.

## Analogy from real world

We can draw analogies from the physical world to address the challenges of digital identity. We can have all our credentials under our control and present them when needed in an insecure way. However, it needs to be practical, user-friendly, and secure. For instance, to prove our age, only the date of birth is necessary. An ideal digital solution should comply with our right to reveal minimum and only required data about us [4]. However, with our physical id, we are revealing not just our age but also other information about us such as our address, and social security number.

There is a need for a digital solution that allows us to store and exchange our information within our control. We should be able to do so in a trusted and secure digital space. Such a solution also needs to comply with data privacy and protection laws such as GDPR. Digital Identity Wallet can be one of the solutions.

## Digital Wallet in Context

Most of us are already using smartphones to store virtual versions of debit and credit cards. It is more convenient to carry as it can reside inside the phone and there is less risk of losing or dropping it. The idea of the digital identity wallet is similar to having a physical wallet but replacing the physical wallet with an application. The wallet can be for a person, for a thing, or for a company.

A minimum viable wallet can be used for secure storage of credentials and cryptographic keys can act as a communication agent and can be used to display social status. Its capability can include digitally identifying, authenticating – proving who you are, and storing and managing credentials in electronic format [5]. This offers us complete control over our data along with the freedom to decide what data to share, with whom, and when.

## Initiatives in Denmark and EU

In Denmark, very soon (at the time of this document being written), citizens are able to store driver's licenses on their phones along with the MitID app [7]. The driver's license is supplementary to the physical driver's license that is valid for driving in Denmark.

Similarly, an EU initiative has started to develop a Digital Identity Wallet Solution (EUID Wallet) [8]. The European Digital Wallet will be for all the citizens, residents, and businesses to identify themselves and confirm certain personal information. " With the click of a button on their device, citizens will be able to rent a flat or open a bank account outside of their home country in a secure and transparent way. Citizens will be able to decide on how much data they wish to share, with whom, and for what purpose" [9]. Apart from the EUDI Wallet, there are existing projects on digital identity wallets. To name some, Connect. me from Evernym [10], Lissi and Esatus from IDunion Project [11].

According to the European Commission, this initiative will build on the already existing cross-border legal framework for the establishment of trusted digital identities, namely eIDAS (electronic identification and trust services) [55]. The technical specifications of the wallet are part of the eIDAS toolbox. The toolbox consists of an expert group from 27 member states which are further divided into four working groups [55]. These working groups are responsible for defining format and issuance of personal identification data, APIs and protocols for communication between stakeholders, unique identification process , governance of certification bodies, business models and fees structures [55].

The current toolbox contains information about the objectives of EU Digital Identity Wallet, the roles of the actors involved, the functional and non-functional requirements of the wallet. However, information regarding technological choices from architecture, reference framework, common standards and common guidelines are yet to be defined [55]

## European DIgital Identity Wallet (EUDI Wallet)

The EUDI Wallet will allow users to identify both online and offline. It will enable storing and exchanging the information provided by governments and trusted private sources [8]. The key principles enlisted in the wallet are [8]:

- "Any EU citizen, resident, business in the EU will be able to use it"
- "It will allow identification and confirmation of certain personal attributes to access any public can private digital service across EU"
- "It will provide users full control to choose and share different aspects of their identity, data and certificate with third parties , at the same time keep track of sharing"

The following example explains the practical use of the EUDI Wallet [8].

Let us consider a general scenario of applying for a bank loan today. A customer, **X** wants to open a bank account with bank **B. X** begins by booking an appointment and having a physical meeting. On the day of the meeting, **X** is bringing all the paper documents, the documents are verified and signed. However, this process must repeat in case a single document is missing.

Now, let us try the same process of applying for a loan but this time, **X** has a EUDI Wallet. At the request of the bank, **X** only needs to select the necessary documents stored in the digital identity wallet. On receiving the verified digital documents securely, the bank verifies them and continues with the application.

## Self-Sovereign Identity and principles

One Of the key principles in the EUDI Wallet is to provide users with full control on what they share, who to share and how much to share , and keep track of such sharing.This notion of identity where users are in control is discussed by Christopher Allen and referred to as "Self-Sovereign Identity"[17]. This is a new concept of online interaction . He has defined ten principles of SSI

which are a series of guiding principles that provides a better understanding of what self-sovereign identity is [17] [21].

- ***Existence* :** Users must have an independent existence
- ***Control:*** User must control their identities
- ***Access:*** Users must have access to their own data
- ***Transparency:*** Systems and algorithms must be transparent
- ***Persistence :*** Identities must be long lived
- ***Portability:*** Information and services about identity must be transportable
- ***Interoperability:*** Identities should be as widely useable as possible
- ***Consent:*** Users must agree to the use of their identity
- ***Minimization:*** Disclosure of claims must be minimized
- ***Protection :*** The rights of users must be protected

## Digital Identity Wallet and Distributed Ledger Technology

The digital identity wallet tends to establish a trust in the digital identity space between the different actors such as Identity providers who issue claims about an entity, Relying parties who need access to those claims to provide a service, and Subjects who are the entities about whom the claims are issued [6]. When it comes to digital trust, it cannot be achieved by technology alone but rather by humans and technology working together. In the case of the digital identity wallet, there are many different technologies that have to interoperate with each other along with the governance frameworks that ensure interoperability between the technologies, standardization of communication protocols for the wallet, and network governance to facilitate a transaction, and /or operate a node in the network [47].

One of the key technologies in the digital identity wallet can be distributed ledger technology(DLT). The concept of distributed ledger technology (DLT) existed before bitcoin and blockchain technology. The recent enthusiasm and interest in cryptocurrencies and blockchain technologies have resulted in the swift evolution of DLT system types and applications. There is also ongoing research and projects about the use of distributed ledger technologies in different domains like supply chain, healthcare, identity, and access management apart from the cryptocurrencies. However, the use of DLT in digital identity wallets is a relatively new area of research.

## 1.1 Motivation

When I applied to a foreign university in Denmark from my country, it took me more than two months before I could come here to study. There was a lot of bureaucracy that I had to deal with. In order to apply, I had to verify my national identity, diplomas, and any other documents, in order to get attested. Some of these processes were physical, which ended up taking a lot of days, but fortunately went well. I also had to get some government issued certificates, bank certificates, and more, which were online processes. The online verification and attestation was also time consuming, and complex, meaning that having a digital identity wallet could have made the process easier and faster for me. This was my personal motivation to look into the EU-Digital Identity Wallet.

The EU commission has announced the digital identity solution, a digital identity wallet. With a digital wallet, users will be able to request identity documents and electronic attestation . They can have them in the wallet under their control and use as per necessary. Some of the standards are currently to be discussed such as what type of authentication, protocols are to be used, what cryptography methods to use. Similarly use of verifiable data registry such as distributed ledger technology are still open questions. This was my next motivation to look into the role of distributed ledger technology in the wallet ecosystem.

## 1.2 Problem Formulation

The obvious way to handle retrieving, storing, exchanging, and signing digital documents has been via silo and federated methods. These methods rely solely on one entity or a small group of big

techs to establish trust. Increasingly, digital trust is being built on decentralized systems. The EUDI Wallet key principles show EU's initiatives towards decentralization.

A digital identity wallet can make our daily life more convenient and more transparent as our digital documents are stored in the local wallet, and we are consenting to what we are sharing with others. With the benefits of the digital identity wallet, what prices do we need to pay? What will be the trade-off? How will we manage and safely exchange the documents that are stored in the wallet? How will we manage the keys?

These all concerns with trust, security, and privacy related to the information we store, and share come along when we start to use the digital identity wallet. The crucial factor to take into consideration is how we can enable trust and security in the digital world.

Another important aspect to consider is when the EUDI Wallet needs to communicate with national eID of the member states such as MitID in Denmark. Integration of the EUDI Wallet with MitID which is based on a centralized approach can be challenging.

Therefore, this thesis aims at answering the following main question, along with its sub-questions:

➢ ***How can DLTs play a role in realizing the potential of the EU digital identity wallet?***

- What are the opportunities and challenges of a DLT for EUDI Wallet ?
- How do DLT comply with the principles of self-sovereign identity ?
- What will be the applicability of EUDI wallet with MitId ?

In order to answer the probæem formulation, I will use the following guidelines :

- I will investigate different distributed ledger technology and make a comparison based on how information is registered, who can access the network, and how different nodes come into an agreement about transactions;
- I will investigate DLT-based solutions and digital identity wallet examples to understand different DLTs have been exploited;
- I will explore the opportunities and challenges to use DLT in the EU- Digital Identity Wallet;
- I will explore how EUDI Wallet will work with MitID;
- I will investigate how DLT supports the principles of Self-Sovereign Identity Principles.

## 1.3 Delimitation

This thesis was conducted with the intent to analyse and review a general case study. Meaning that mainly secondary sources were used in the process to reach an answer to the proposed questions. And, even though the sources are formal and official, such factors do not always ensure accuracy, especially since people perceive things differently, and are somewhat intrinsically biased or too subjective in their analysis [60].

In this particular case, I merely tried to acquire empirical information in order to reach a conclusion, but as mentioned above I could have been somewhat biased during my analysis especially since the choice of subject for this thesis relates to my own personal interest, given the issues that I was faced with, during my application process of studying in Denmark.

Either way, I still believe that this thesis adds value to the community even if implementing a solution was not an objective of this study.

# 2. Methodology

This chapter discusses the methods and techniques applied throughout the thesis to answer the problem formulation. It describes how each chapter in the thesis was planned, how data collection was done, and how data was interpreted to answer the problem statement and achieve the goal of the overall research work. Saunders's research-onion has been used as a methodological framework for this chapter [27].

**Research philosophy:** In the Saunders research onion, the first layer is the research philosophy. It describes the set of beliefs the research is built upon. Research philosophy can be built on an ontological or epistemological point of view. The former is the assumptions that we hold about reality, the contexts, and the people we engage with [27]. The latter is the area of thinking that makes us reflect on our assumptions about knowledge and the extent to which our own values and some ideologies can influence our research [27].

Ranging from this concept there are five main research philosophies in the research onion. Among the five, this research follows the interpretivism research philosophy because as a researcher I will be drawing a holistic view of what has been said or written about distributed ledger technologies throughout the secondary sources. While finding out values and challenges of distributed ledger technologies for the digital identity wallet, I will be gathering data about the topic mostly from desk research . Then I will be using my own interpretation and data gathered when assessing the case of the EU digital Identity Wallet.

**Approach to Research:** This second layer describes whether we seek to test a theory or build a theory or build a theory that is testable. In this regard, there are three approaches: deductive, inductive, and abductive respectively [27]. An inductive research approach was used to collect data about different DLT solutions to make a comparison, identify a pattern in the use of DLTS from different existing digital identity wallets, and come up with some recommendations for the EU digital identity wallet in regarding using distributed ledger technology.

**Methodological Choice:** There are three methodological choices, quantitative, qualitative, and mixed methods [27]. The quantitative method deals with data collection to prove a theory or any hypothesis built around a subject matter. It mainly deals with numerical data. On the other hand, the qualitative method involves gathering data to build a theory or to develop a richer perspective on already existing theories. In the mixed method, data collection is done using both qualitative and quantitative approaches [27].

The choice of method was qualitative as data was collected from varieties of secondary sources like journals, gray literature, news, the official website of the EU, online websites, articles, and e-books. In addition, one consultation was done to get a more insightful overview of the EU digital identity wallet in the earlier phase of the thesis.

**Strategy:** In the Saunders research onion framework, different methodological choices are associated with different research strategies [27]. Some of the fundamental strategies that are associated with the qualitative research method are action research, case study research, ethnography, grounded theory, and narrative inquiry [27]. A case study research was used as a research strategy and EU Digital Identity Wallet was taken as a case example.

**Time Horizon:** There are two options of time horizon; the longitudinal one which takes more time and is costly. The other one is the cross-section which is suitable for research that is intended for a shorter time, and it is also cheaper than longitudinal [27]. A cross-section time horizon has been chosen as the time period to complete this thesis was nine months.

**Techniques and Procedures:** From the wide techniques of data collection, data collection was primarily based on desktop research. In the beginning phase of the research, an expert consultation was carried out to get insight into the development of the EU Digital Identity Wallet.

# 3. Literature

This chapter will provide a basic introduction about distributed ledger technology, types of distributed ledger technologies and some common properties of them.

## 3.1 Distributed Ledger Technologies

The origin of the ledger in the first place can be associated with the origin of money, especially when money was used as a record [62]. When money is involved in a transaction, a series of transactions is recorded. Today, a vast amount of money in circulation is simply transactions recorded and organized in the ledger. The ledger is maintained by central banks which provide measures and tools to connect with the ledger. Similarly, ledgers are used for recording events in different sectors beyond finance.

A ledger is a book that records financial transactions for an organization [63]. A ledger has existed since the beginning of time, whether it records contracts, payments, or assets moved. The art of bookkeeping began with clay tablets, and papyrus followed by paper [62]. Over the past decades, computers have replaced the paper-based method. With computers, record-keeping is faster and more convenient. Fast forward to today, the information stored is cryptographically secured, fast and decentralized [63]. There are two types of ledger; centralized and distributed.

A centralized ledger is a general ledger. It works as a central repository where all kinds of financial and non-financial information are stored. A single entity has total control over any transactions. If a single entity has malicious intent, it can do serious damage to its clients.

A distributed ledger is a shared ledger. There is no central administrator or centralized database. All participants have identical copies of the ledger over multiple sites, and geographies [64]. Any changes to the ledger are reflected in all copies and if there is any fault in one of the ledgers, it doesn’t affect the other ledgers. Some of the prominent characteristics of a distributed ledger are its peer-to-peer nature network which implies that all the participants' networks are designed to serve or receive data [64].

In the centralized network, it is a client-server model of the network, and a central authority is in control of the network. Whereas, there is a lack of central authority in the peer-to-peer network, providing all the network participants with equal privileges. Security is achieved through cryptographic keys and signatures so distributed ledger is relatively hard to falsify [63].

Distributed ledger can be permissioned, permissionless, private, and public [64]. Depending on the requirement of permission to access, and modify the ledger there are two general categories of the distributed ledger; pemissioned and permissionless. In the former category, nodes are required permission from central entities to access and modify the ledger. On the other hand, in the latter category, all modes can access the updated copy of the entire ledger, and any changes in the ledger are communicated to all nodes in the network. However, in both categories, all the nodes are responsible to validate any modification in the ledger through a pre-defined algorithm. This process of all nodes coming into collective agreement about any modification is known as the consensus mechanism [64].

There can be variations in the consensus mechanism. Apart from permissioned and permissionless distributed ledger, can be private or public. In private permission is required to join the network whereas in the public anyone can join the network [64].

The term Distributed Ledger Technology and blockchain are used interchangeably, but there is a subtle difference between them. Blockchain is just an example of DLT where data can be stored in a particular format. There are other types of ledgers with different formats. Despite the variation in types of the ledger, DLTS has gained a lot of attention from industry, the Government, and scholars. DLTS exhibits some properties that make it a suitable technological choice for several application domains [65].

Some of the common properties are [65] :

- ***Distributed consensus on the ledger state:*** Ability of the nodes to achieve consensus on the state of the ledger without relying on third parties;

- ***Immutability and irreversibility of the ledger state:*** The process of achieving distributed consensus among a large number of nodes makes the ledger immutable and irreversible. Some of the DLTS is tamper-proof and some are tamper-apparent. Those tamper-proofs prevent any participants to alter established records on the ledger, thus providing data immutability and irreversibility;
- ***Data Provenance:*** Every transaction stored in the ledger is signed using PKI which certifies the authenticity of the source of data;
- ***Data Control:*** Data is stored and retrieved from the ledger in a distributed manner that leads to no single point of failure;
- ***Accountability and transparency:*** Every single interaction among the participants can be verified by an authorized body promoting accountability and transparency.

In the following section, three variants of distributed ledger technology are presented to get a basic overview of the types of DLTS.

## Blockchain

Blockchain is the underlying technology of Bitcoin. It became well known in 2008 when a paper was published about bitcoin [66]. Since then, a huge amount of attention has been paid to Bitcoin and other cryptocurrencies. However, since 2014, the attention began to shift toward the technology behind Bitcoin [66].

Blockchain can be permissionless which means it is public and open source [66]. Anybody can participate in this type of blockchain. The transaction can be sent to the blockchain and can be a part of the block if validated. The transactions are transparent meaning anyone can view them but they are anonymous. Anybody can validate transactions before including them as a part of a block. In a public blockchain, the consensus mechanism used is proof -of- work [66]. A group of people called miners compete with each other to complete the transaction on the network. Bitcoin and Ethereum are some examples of the public blockchain.

Blockchain can be permissioned, and private where either a single organization or a group of organizations operate the blockchain [66]. When it is operated by a single organization, the public is allowed to read the transactions or only some selected parties can read the transactions. On the other hand, when it is operated by a group of organizations, the public can read the transaction but only the selected parties can write the transactions.

With the permissioned and private blockchain, it doesn't seem to serve a true decentralization purpose [66]. However, it differs from the traditional databases based on the use of different consensus algorithms to make a common decision in a group that can benefit the majority of the group members.

## Directed Acyclic Graph (DAG)

DAG is another type of DLT, which is a non-blockchain [64]. It can also store transactions like a blockchain but instead of linking every transaction to all the previous blocks, any new transactions are required to link to one or more previous transactions only when joining the DAG[64] . A transaction in DAG is represented by a node that is linked to one or several edges.

In theory, DAG is a graph that points in one direction. It has vertices and edges where vertices represent transactions and edges represent the direction of the graph [66]. The vertices and edges together extend the database. A DAG is acyclic as the nodes are not allowed to transverse back to themselves following the vertices.

There is no mining in DAG, however, a small proof of work is done by the nodes themselves by verifying the two closest transactions for the two closest nodes [67]. Transactions are built on top of earlier ones instead of gathering into a block.

# Hashgraph

Hashgraph is another type of distributed ledger that utilizes the directed acyclic graph for storing and accessing information. It is a patented technology, so mostly designed for private use cases [13]. Hashgraph is based on DAG but uses a different consensus algorithm; gossip protocol. Signed transactions can be created by any member of the network at any time. All the participants of the network get a copy of it and reach a Consensus on the order of those transactions.

The way information is circulated is that each member chooses another random member and passes the information they have received from the other participants and adds information about new transactions. This method of information sharing is referred to as gossip [64]. One of the interesting things about Hashgraph is the "gossip about gossip" which means that not only the transaction including a timestamp is transferred, also information about the previous receivers of the information is passed on.

The gossip about gossip introduces new consensus mechanisms called "virtual voting"[64]. The idea behind virtual voting is that in the "gossip about gossip" the participants not only know about the transaction but also know who else has access to the previous transaction. This allows the participants to calculate what the other nodes' reaction to the transaction would be.

Hashggraph consists of columns and vertices where the column represents a user in the network and the vertice represents the event. A user can submit an event that contains a new transaction. After that, the user can randomly choose another user and pass the event to the selected user. It is referred to as gossip about an event [ 13].

An event contains information such as a hash of the previous event created by the user receiving the gossip, a hash of the previous event created by the user sending the gossip, a transaction created by the user sending the gossip, and a timestamp that records the time when the event was submitted [13].
The idea of ordering and fairness is a unique characteristic of hashgraph. Events can be ordered and validated based on the order of their submission in the network.

### Sub-conclusion

The overview of different types of distributed ledger technologies shows that they vary in many ways; the underlying data structure, how transactions are performed, the consensus mechanism used to reach agreement on the state of the ledger, and the types of participants in the network.

## 3.2 Background on Digital Identity

The following section will present basic concepts on identity, digital identity, its nomenclature, and how digital identity can be created. Further, it will highlight the importance of digital identity and its management, evolution of different identity models. It will also look into how trust is maintained between different actors involved in the different identity models.

### Concepts of Identity, Digital identity, and nomenclature

The term "identity" was first used in 1570 and its origin is from Middle French "identité" from Late Latin "identitat-, identitas", or probably from "identidem" which means literally "same and same" [12]. However, there is not a single and standard definition of the term, rather it has been used from different perspectives in various literature. One simple definition of "identity" is a collection of data about a subject which can be characteristics, preferences, and traits. Another definition of identity according to [12] is "identity is what makes an individual the same today as they were yesterday, at the same time it differentiates them from one another".

Similarly, digital identity has also no consensus in a definition like a term "identity". For the scope of this report, we will consider digital identity as the set of attributes and activities of a digital subject [12]. The attribute contains information about the subject and activities refer to what a subject does on the internet. A digital identity consists of a digital subject, attributes of the subject, and partial identities. A digital subject is typically a person or a thing existing in the digital world. The attribute is a piece of information like a distinct property about a subject. Partial identity is a subset of attributes of the complete identity of a subject. Digital identities, therefore, are the union of all the subject, attribute, and partial identity.

In digital identity, another important notion is claim-based identity. as Kim Cameron explains "identity should be based on claims" [14]. A claim is a set of attributes about a subject. When a subject appears online and wants to access some resources from a website a triangular relationship is established between the subject and other parties. In this scenario where a person accesses a website, the person is the user, and the website is the service provider or relying party.

In order to access any resource from this website, the user needs to present some claims about him/her, and it is done in the form of credentials. So, credentials act as a placeholder for attributes about the user. A third party is also there who is an identity provider that can provide assertion on behalf of the user. Assertions are provided to support claims made about users. In this interaction between three entities, a triangular relationship is formed which is often called a trust triangle as there should be some level of trust between all the interacting entities.

A subject has multiple identities and is created in numerous contexts. When a digital identity has been created a subject leaves traces in the form of IP address, email, username, passwords, banking data, tags, and links over the internet [15]. These traces of fragmented information about its identity are scattered all over the internet which raises questions about what happens to all this information scattered all over the internet. The internet was created without an identity layer and establishing online trust is difficult [15].

To sum up, in the physical world, usually, the users know who they are interacting with and they are in control of what and how much information to share about them. However, in the digital world, it is often the case that identity providers are in control of the user's information and data. They are aware of users' online activities allowing them to form a link and point to a particular user. In order to mitigate the concerns about users' privacy and data protection a trusted environment is necessary, where users trust the interacting parties and vice-versa, and users are in control of the information they are exchanging and sharing.

# Evolution of digital identity

The internet was created without an identity layer. It lacks a standard way to know who and what you connect to [14]. The ever-present issue regarding identification on the internet is depicted in the famous cartoon by Peter Steiner, “On the internet, nobody knows you’re a dog” [16]. So, online services started to identify subjects with a username and password in the beginning days. Since then, the model of digital identity has been evolving and according to Christopher Allen, there are four ways of digital identity [17]:

**Centralized Model:** Vast majority of identities are centralized and are owned by a single entity such as e-commercial websites or a social network [17,18]. In this model, digital identities are issued by centralized authorities. Users have to create and manage unique passwords for each different website they access. As the number of online services is expanding, it is a tedious task to remember all the passwords. Sometimes, there is a high chance to repeat those passwords or use weaker passwords which are prone to attacks. Another crucial point in this model is the accumulation of control over the user’s identity by the identity providers. The users lost control over their identities.

**Federated Model**: The Federation model addresses some of the issues in the centralized model. It enables a user to login into one service and re-uses the credentials in another service. This removes the burden of remembering a chunk of passwords for a user. Within the large business, it allows users to use a single sign-on so he/she can access multiple internal services with a single username and password. Although it allows users to utilize the same identity across multiple sites, it puts the identity provider in control. The consequences of losing a federated account are more significant than losing an account to third-party services in the centralized model.

**User-Centric Model**: The model in principle focuses on placing the user in the center of the identity process where he/she has better control over his/her digital identity [12]. It allows users to log in to multiple services with one profile created with one service [14]. The model differs from the federated model as this model allows a user to choose a site as a login for another. For example, with Google’s Single Sign-On (SSO), users can create a profile and store data with Google. This profile can be used in any online service that has integrated Google’s features for quick registration.

However, this model still suffers the same issue as the centralized model as the central provider will be in full control of the user's digital identities.

**Self-sovereign Identity Model**: The user-Centric Model is the next step toward user control of their identity but when it comes to user autonomy, Self-Sovereign Identity is the desired step as explained by Christopher Allen [17]. In this model, it is the identity owner who owns, controls, and manages their identity. With this model, users are in the center of the identity process and can reveal some or all of their data. There are no identity providers like in the centralized and federated model. Credentials are exchanged between the issuer, holder, and verifier in a peer-to-peer connection.
The dimension of identity has evolved from centralized silo to federated, followed by user-centric, and now is moving towards self-sovereign identity. So, the methods of identification and authentication have been users registering separate accounts with each entity in the centralized identity. In the federation identity, the user has to remember only the username and password of their IDP.

In the user-centric identity, users can choose a single side to log in to different other sites. However, in all these models IDPs can collect data about users about different services users are using. Not to mention, there are privacy and security risks. For example, the impact of identity theft increases from centralized to federated and user-centric models. SSI on the other hand comes with a bunch of technologies like distributed ledger technologies which are secure databases to ensure secure transactions. Similarly, in this model users exist independently. However, SSI projects still face challenges as this is immature technology without established standards, transparency versus unlikability, usability, and user experience [19].

In regard to EU Digital Identity Wallet, it is moving toward the path of a self-sovereign identity model. With the wallet solution, users will be able to choose what aspects of their data to share with third parties and, and be able to track such sharing. There are ongoing discussions on how identity management solutions based on self-sovereign identity can be benefited from the eIDAS framework [20].

## Principles of self-sovereign identity

Following are the principles of SSI which are a series of guiding principles that provides a better understanding of what self-sovereign identity is [17] [21].

**a)** ***Existence***: User's identity should not exist in wholly digital form rather they should have an independent existence. Users must be able to have independent existence without a third party. With self-sovereign identity, it makes accessible and public only some aspects of the users´ whole identity. Identity is often combined with state-issued documents such as driver's license and social security cards, and this could imply that if a state revokes credentials, a subject may lose their identity.

**b)** ***Control***: Users should be the ultimate authority over their identity. They should be able to refer, update and hide when necessary. However, this doesn't indicate that users control all the claims on their identity as other users may make claims about a user.

**c)** ***Access***: Users must be able to access their data and any related claims about them without the interference of third parties. However, this doesn't indicate that the users have control to change all aspects and claims related to their identity, but they can access records of any changes regarding their identity.

**d)** ***Transparency***: Algorithms and infrastructure must be transparent meaning the system operating the network of identities must be transparent on how they function and how they are managed and updated.

**e)** ***Persistence***: Identities of users must last as long as users wish. At least identities should last until new identity systems replace them. However, this should not contradict a right to be forgotten. Users should be able to modify or remove identity information over time if they wish.

**f)** ***Portability***: Information and services about identity must be portable. The portability of identity information puts users in control of their identity despite their move to different jurisdictions.

**g)** ***Interoperability***: The goal of the digital identity system is to make identity information as widely available, and usable as possible, across borders. The objective behind this is to create a global identity where users are in control of their identities.

**h)** ***Consent***: Users must agree on how they want to use their identity. When sharing data in an interoperable identity system, it should occur with user consent. Consent might not be interactive but it should be well understood by the users.

**i)** ***Minimization***: There should be minimal disclosure of claims. When data disclosure is required, users should be able to disclose only the minimal amount of data to complete the task at hand.

**j)** ***Protection***: Users' rights should be valued. To ensure user protection, there should be a balance between transparency, fairness, and user support within the self-sovereign identity network. There should be an independent censorship-resistant algorithm that can authenticate user identities.

## Trust model

In any kind of digital identity model, there exist relationships between the transacting parties; the issuer, the identity holder, and the verifier. Such existing relationships form the basis of trust between them. So, the formed trust model also determines the power of control among the holder, issuer, and verifier.

In the traditional identity system such as centralized and federated, trust is maintained through agreement and controls based on Public Key Infrastructure (PKI). In the PKI infrastructure, digital certificates are issued, signed, and stored by Certificate Authority (CA) [50]. In the PKI enabled model, CA is responsible for storing the public keys of users, issuing, publishing, and revocation of the digital certificate [50]. The digital certificates can be used for the identification and validation of the information contained by it. As PKI binds the subject with their public key, the recipient can verify the owner of the key by using the public key of the CA [50].

There are some concerns associated with this trust model. All parties must trust and rely on the CA for distributing and management of digital certificates for a network of users. Due to centralized control, this model is susceptible to a single point of failure [51]. In addition, the public keys can be misused by bad actors to derive private keys. The trust model built on these types of identities is not only time-consuming but the locus of power shifts towards the issuers and service providers as they can decide whether to provide the requested credentials or services to the subject.

The alternative to centralized PKI is Decentralized PKI (DPKI) based on Decentralized Identifiers and Distributed Ledgers like blockchain. In this model, distributed ledger can be used to store key values, and the power of third parties is minimized [51]. Trust among the interacting parties is achieved by sharing their DIDs which is analogous to the certificate in centralized PKI. The trust model based on DPKI concepts put the users in control and the locus of power shifts towards the holder. This is similar to the trust model based on self-sovereign identity. There is a peer-to-peer relationship between holder and issuer, and holder and verifier as the interactions are direct. Both the holder and the verifier trust the issuer [6].

To establish trust in such a trustless environment a verifiable data registry plays a crucial role in establishing trust among the interacting parties [18]. The verifiable data registry should be public so that any participants can look into, and access it in order to have confidence in the other parties that are interacting with it [18].

Similarly, the EU Digital Identity Solution aims to put the users in control of their identity. They want to provide the citizens with an identity ecosystem that is similar to the one proposed in the self-sovereign identity ecosystem.

## General data protection Regulation (GDPR)

GDPR provides guidelines on how organizations and businesses should handle information about individuals. Any systems dealing with personal information related to EU citizens need to act in accordance with guidelines of GDPR regulation [54].

The purpose of discussing some basics of GDPR regulation is to later make a reflection on any identity models or systems using distributed ledger technologies compliance with GDPR Regulation. For this purpose, not every article of GDPR will be covered but only some of the relevant data subject rights .

**GDPR Definitions**

When any transaction related to personal data occurs, the following entities are involved [54]:

- Personal data - Any information that can be used to identify an individual directly or indirectly;
- Data subject - The person whose data is processed;
- Controller - The person who decides why and how personal data will be processed;
- Processor- An entity who processes data on behalf of the controller, it can be the controller itself.

**GDPR Data Subject Rights**

When it comes to data subjects, GDPR aims to give individuals more control over their data. Any organization or system dealing with personal data should ensure GDPR compliance. Following are the data subject rights [54]:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

## Sub-Conclusion

Digital identity is the means to prove who we say who we are in the online context. It's a way to access any online services or complete any tasks that are provided by the government, organizations, and companies that mandate proof of identity.

The way of identifying ourselves and proving our identities have been evolving from the silo method to the self-sovereign method. This evolution was a result of prevailing privacy and security concerns in the former models. Nevertheless, the self-sovereign identity model we are trying to achieve is still nascent and not fully developed yet.

Trust is essential in both physical and online transactions. In the physical world, it is much easier to establish trust compared to the digital world. This is because we do not know every person or thing we are transacting within the digital world.

Trust mechanisms like digital certificates enable users to have confidence in the security and authenticity of interacting counterparties. Nevertheless, these methods use silo databases and centralized identity providers to manage users' information which is prone to the center point of failure, accumulation of control of users' data in the hands of Identity Providers, and users' identities being scattered all over the internet.

To minimize these adversities, the concept of self-sovereign identity is gaining momentum with its principles that advocate minimal disclosure of information, and users being in control when accessing and controlling their data.

# 4. State of the Art

This chapter is divided into different sections. Section **4.1,** presents different entities working to develop standards and specifications regarding digital identity. Section **4.2,** provides insights on different standards and technologies that are enlisted as an integral part of the DLT-enabled identity solution and Section. Section **4.3** explains how technical and human trust can be maintained in a digital solution. Section **4.4** gives overview about different DLT-enabled solutions. Section **4.5** presents different digital identity wallet examples .

## 4.1. Different Initiatives

Various actors are stepping to create standards and specifications, and research projects related to identity management. These are entities, foundations, government bodies, and working groups engaged in different areas of identity to enable trust in the identity ecosystem. The following section will review some of these entities, followed by the review of standards and technologies developed by them.

### World Wide Web Consortium

The World Wide Web Consortium (W3C) is an international community of full-time staff, member organizations, and the public working together to develop web standards. Its main activity is related to developing protocols and guidelines for long term growth for the web [56]. The working group in W3C have developed specifications regarding Verifiable credentials, and Decentralized Identifiers . Further details about Verifiable Credentials and Decentralized Identifiers can be found is section **4.2**.

### Trust Over IP Foundation

Trust Over IP (ToIP) is an independent project that is hosted at the Linux Foundation with a mission to provide a robust , common standard, and complete architecture for internet- scale digital trust [48]. The goal is to create safe and private space for digital interactions that occur between individuals, business, government, and things. To address this objective, it has founded two sided

stacks which are a combination of technology and governance. Further details of these stacks and reasons behind them can be found in section **4.3.**

### Decentralized Identity Foundation

Decentralized Identity Foundation (DIF) is an organization dedicated to creating an ecosystem that supports decentralized identities and enables interoperability. The members of DIF produce reference implementations for specification produced by W3C [57]. The "Identifiers and Discovery" working group under DIF is working on protocols and implementations of DIDs across decentralized systems like distributed ledgers. This includes DID creation, resolution, and discovery[57]. Another working group, " DID Authentication" focuses on format and protocols for authentication and authorization using DIDs, DID documents, and Verifiable Credentials [57].

## 4.2 Technologies and Standards

Technology and standards developed by some of the above-mentioned bodies will be presented in this section. The relevancy of this section in order to answer the research question is these standards and technologies are supporting agents to the DLTs discussed on DLT-enabled solutions for identity management and are also standards used by the wallet examples.

### Decentralized Identifiers

In the current (federated) model, we are relying on intermediaries like Facebook, Google, and email providers for most of our online interactions. We are re-using the identities that we have registered with these intermediaries. The outcomes of these are these parties gather metadata around us and data linkability is at a higher scale. This put some centralized registries in control of our identifiers making us lose control over them. Decentralized Identifiers (DIDs) however, are independent of centralized registries, authorities, or identity providers. They can be created for different contexts of digital identity, and hence can prevent data likability [39].

DIDs are defined as a new type of globally unique identifier in a document "W3C Proposed Recommendation" published by the W3C Decentralized Working Group [39]. They are intended to enable individuals and organizations to generate their own identifiers, these identifiers allow them to prove control over them by authenticating with proof based on cryptography such as a digital signature [39].

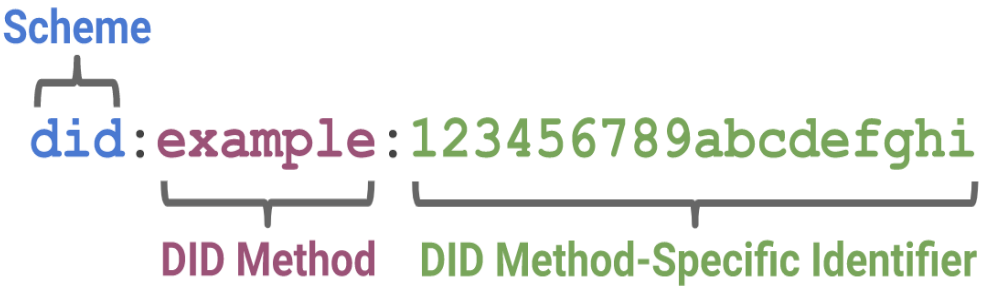



*Figure 1. DID representation [39].*

Figure **1** is a generic representation of a DID [39]. The first part "did"is the schema identifier. It should always begin with "did." The second part "DID Method" is the method scheme implemented. An individual DID method explains how DID is created, updated, resolved and deactivated within a particular system. The third part is the method specific identifier.

DID is functionally equivalent to URN for something but it is resolvable into one or more URLs.It contains DID scheme, DID method, and DID Method-specific identifier. DID is just a URI.

A DID can be resolved into a data structure called a DID document, which is needed to exchange messages and verify credentials with a subject. A subject can be a person, an organization, etc.

- **DID Document**

It is an information document that a DID revolves to. It is public so it should always contain the minimum amount of information, and enable interaction or connection with DID Subject [39].

In theory, a DID document contains any arbitrary data that describes the DID subject, this could mean even private and personal data which is why storing personal data in the DID document is discouraged.

It contains:

1. one or more public keys associated with the DID subject controlled by the DID controller.
2. One or more service endpoints for concrete interaction
3. Data such as timestamps, digital signatures, cryptographic proofs, or delegation and authorization metadata

EXAMPLE 1: A simple DID document

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

*Figure 2. DID document [39].*

Figure 2 shows a simple DID document, it contains one public key used for authentication. This figure contains the properties of DID documents such as “context” , DID subject with key “id”. “controller” who is the controller of the DID and “public key”[39].

- **DID Methods**

There is not a single technology to implement DIDs. They can be implemented in different ways, and are called DID methods. An individual DID method explains how DID is created, updated,

resolved, and deactivated within a particular system. There are many DID methods but the core functionality provided by them should be the same as specified by the W3C specification[39]
It begins with the syntax did, which is the schema identifier with a semicolon followed by the method name, and comes the method-specific identifier.

- **DID Resolution**

The process of obtaining the DID document is associated with a DID. It can be viewed as an algorithm with "did" as input and other parameters and the output is the document [39]. For example, a verifier can look into an issuer's DID, and resolve it to verify the signature of the issuer for facilitating functions such as verifying verifiable credentials. The details of verifiable credentials will be presented in a later section.

- **DID Architecture**

The overall concepts described above can be put together to show the overall architecture of DID as shown in the figure below:

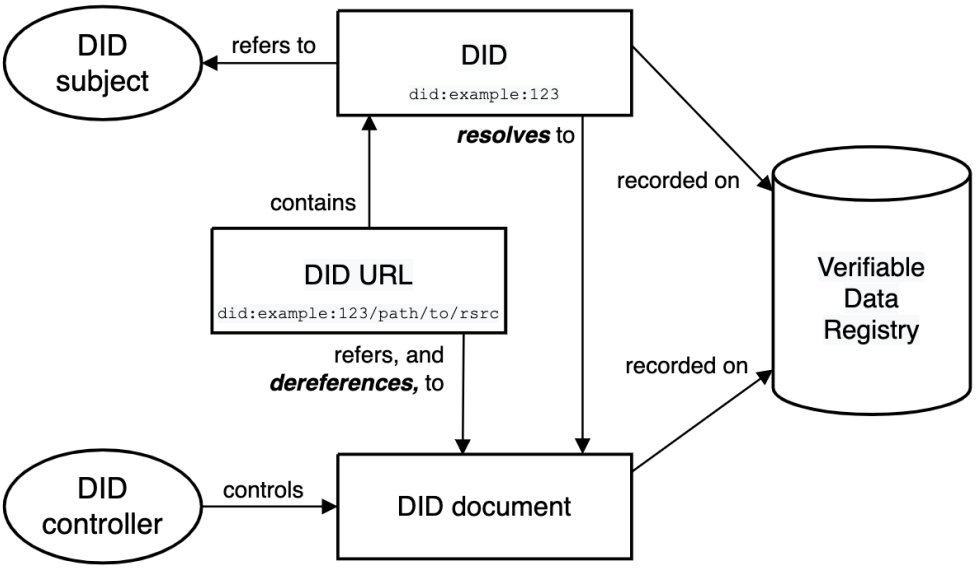



*Figure 3. Overall DID Architecture[39].*

Figure **3** shows the overview of DID architecture. The DID is related to a subject. The DID is recorded on the verifiable data registry such as distributed ledgers, decentralized file systems, or databases of any kind. Verifiable data registries support the recording of DIDs.

DID resolves into DID document, The DID document contains references and metadata about the DID subject and is controlled by the DID controller. There can be two scenarios related to DID Controller and DID subject; they can be a separate entity or the same [39].

## Verifiable Credentials

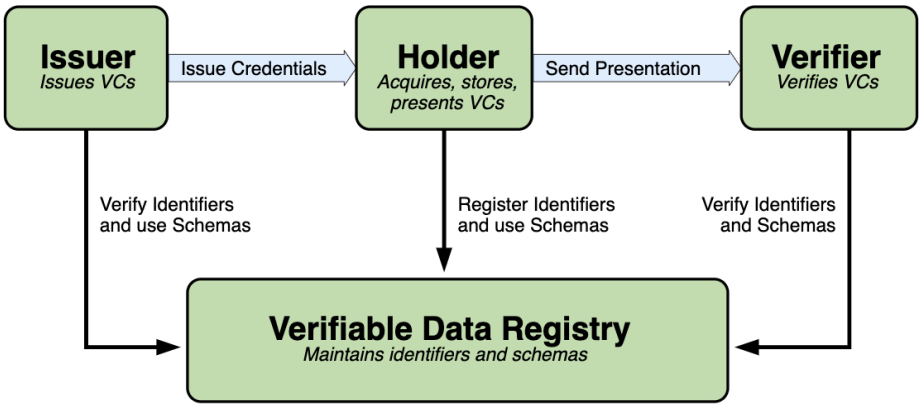
Credentials are like proofs we carry around. They can be both physical and digital. We can take them somewhere else and use them to prove something about ourselves. The problem with them is they can be forged or damaged, they are expensive to scale, and in the digital world, it is difficult to verify or we are disclosing a lot of information about ourselves.

In the digital world, it is challenging to receive the same benefits that physical credentials provide due to the difficulty to express credentials on the web [40].

Verifiable Credentials are defined by W3C specification as the digital attestation of one identity owner about another[40]. The use of technologies like digital signatures makes verifiable credentials more tamper-evident than physical credentials. The credentials expressed are able to be verified. They do not imply truth about the claims contained in them rather they contain evidence for relying parties. so, the relying parties can determine whether the provided claims are sufficient for them to trust on the provided credentials [40].

- **Verifiable Credential Ecosystem**

The ecosystem of Verifiable Credentials comprises the issuer, holder, verifier, and the verifiable data registry along with the roles and relationships between them. The roles can be implemented in different ways meaning that a holder can be an issuer or verifier depending on different scenarios[41].




F*igure 4. Different actors and their roles in the verifiable Credential Ecosystem [41].*

Figure **4** shows the different actors and their interactions with each other.The different actors are the issuers who issue credentials, the holders who request credentials, hold the credentials and present it to the verifiers. The verifiers are the one who verifies the credentials presented by the holders.

The issuer asserts claims about one or more subjects, creates verifiable credentials from claims, and transmits them to a holder. The claim contains statements about a subject. For example, it can be a statement that a subject is a graduate of a particular University. More statements can be grouped together to construct a graph of information about a subject [41].

The subject is an entity about which claims are made. They can be holders of verifiable credentials or may not be depending on cases [41]. For example, a parent can be a holder for a child, who is the subject in this case.

The holder possesses one or more verifiable credentials and generates verifiable presentations from them. Verifiable Presentations are data derived from one or more verifiable credentials that are built by the holder to satisfy the verifier's requirement [41].

The verifier receives one or more credentials or verifiable presentations as per requirement [41].

The verifiable data registry facilitates the creation and verification of relevant data such as verification credential schemas, revocation registries, issuers' public keys, and so on that may be needed for verifiable credentials [41].

- **Components of Verifiable Credentials**

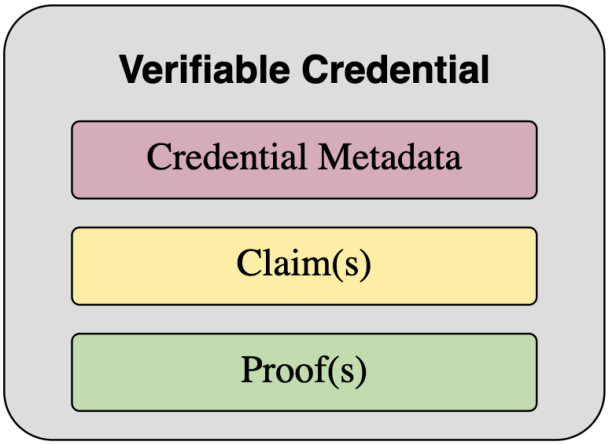



*Figure 5. Components of verifiable Credentials[43].*

The above concepts can be further illustrated in figure **5.** This figure shows Verifiable claims grouped as information graphs. The first graph is the verifiable credential that contains claims and metadata about credentials issued [43]. If Alice is a graduate of the particular university in the claim, the metadata can be who is the issuer, the issuance date, type of claim contained.

The second graph contains digital proof of the claim such as the digital signature of the university, the date of the signature created, and the creator of the signature [49]. Together these two information graphs make the verifiable credential. The verifier when required can look into the digital proof of the issuer, the verifier can decide whether to accept or reject the verifiable credential presented[43].

- **Verifiable Presentation**

A holder can have many credentials from different issuers. Some subsets of attributes from verifiable credentials about a subject can be grouped to create a verifiable presentation and present it to the verifier [43]. It is used when only minimum information is required by the verifier.

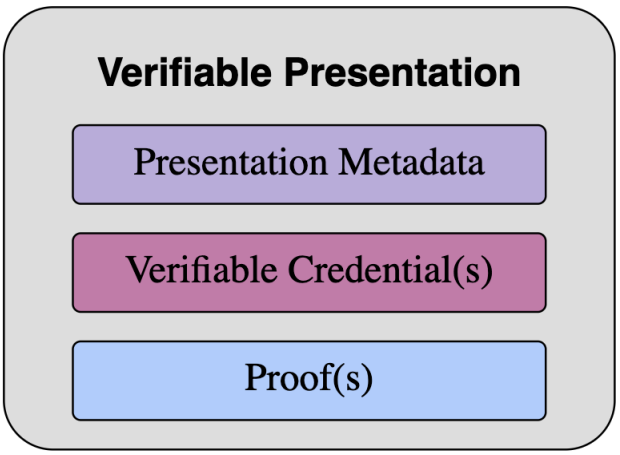



*Figure 6. Verifiable presentation and its components [43].*

Figure **6** details different components of a verifiable presentation that are created about a subject. It contains four information graphs; the first being the verifiable presentation itself, the second being the verifiable credentials with claims, the third being credentials proof which is usually the digital signature of the issuer, and the fourth is the presentation proof which is a digital signature of the presenter [43].

## 4.3 Technical and Governance Stack

When it is about trust in the digital world, it is about both trust in technology and human trust. Humans and technology should work together to achieve digital trust [47][48]. When a digital solution is developed, it should be kept in mind that interoperability should not be limited to the underlying technology but should be extended to practical governance interoperability [47]. Trust over IP has proposed a digital trust architecture combining technical and policy interoperability [48]. Thus, created architecture is divided into technology stack and governance stack that aims to maintain both humans and technology trust.

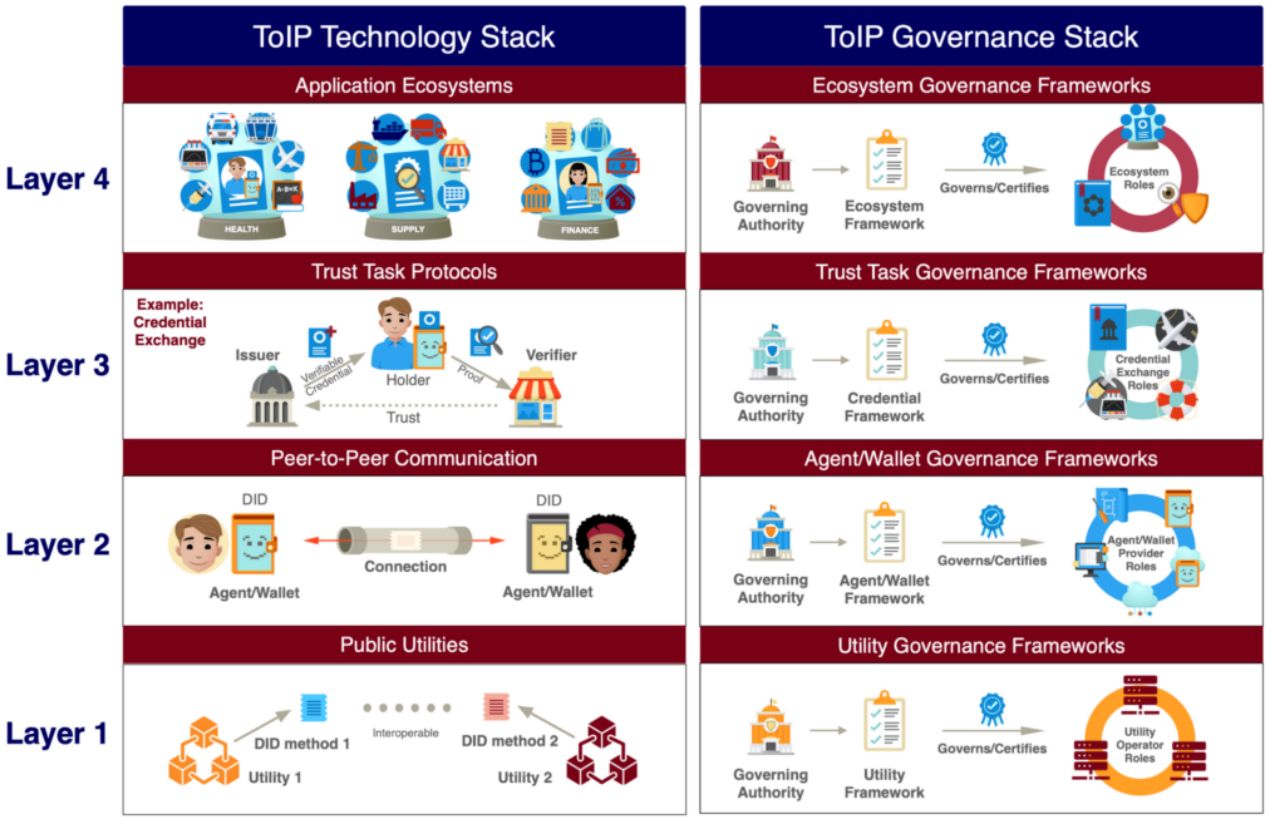



*Figure 7. An overview of two stacks proposed by ToIP[49]*

Figure **7** shows the two-sided four-layer stacks proposed by Trust Over IP. The lower two layers meet technical requirements, and the top two layers meet human requirements [48]. On the left is the technological stack which contains the technological components of different layers of a decentralized identity. On the right side is the governance stack, which shows the different governments corresponding to each technological layer.

In the technology stack, the first layer is the foundational layer- it is about the DID method and the DID registry. The DID methods and the DID registry selected for this layer are responsible and fundamental to securing the other layers. DIDs in this layer are used for verifying the public keys of the issuers of digital credentials [48]. The other layers, second and third are where the communication takes place, where credentials are issued, verified, and exchanged between the wallet or wallet agent. The fourth layer is the application ecosystem layer where the digital ecosystem is built on top of this trust infrastructure [48].

Similarly, parallel to each layer of the technology stack, four layers are in the governance stack. The purpose of the governance framework is to publish business, legal, and technical rules that the members agree to operate to achieve trust [48].

The first layer is the utility governance framework. The utility governance frameworks are to ensure trust in the policies and procedures used to operate public utilities such as blockchains, and distributed ledgers [48]. The second layer is wallet/agent governance frameworks that are needed to establish trust, privacy, data, and standards for digital wallets and agents [48]. The third layer is credential governance frameworks which set out clear and transparent policy about issuers and issuance of credentials that allow verifiers to have to make decisions on the presented verifiable credentials [48]. The fourth layer is the ecosystem governance frameworks that are needed to form rules and policies that will ensure the operation of the digital ecosystem in the three other layers [48].

## Sub-Conclusion

DIDs are new types of identifiers that are globally unique, resolvable, and cryptographically verifiable. They are associated with cryptographic keys and service endpoints that enable secure communication channels. DIDs together with verifiable credentials are the layers of decentralized identity infrastructure. Verifiable credentials can be stored by users on their local devices such as a digital wallet. When needed they can be presented to a verifier.

Verifiable Credentials contain identifiers and information to describe the properties of the credentials such as issuer, date of issue, revocation mechanism, and so on. Verifiers can look into the DID of the issuer from the Verifiable Credentials presented, the DID can be resolved further to verify the signature of the issuer, and to confirm that the credentials presented have not been revoked yet by looking at the issuer DID in the verifiable data registry.

## 4.4 DLT- based Solutions

This section will present a technical overview of different types of Distributed Ledger Technology used by organizations to deploy different decentralized applications and use cases. It will be about the functionality of the ledger, different actors that can access the nodes, and what kind of information should be stored on the ledger. Further, a brief overview of the network architecture of solutions will be discussed. This study is done to understand how distributed ledgers can be exploited to provide decentralized digital identity to users, organizations, and things.

### Sovrin Public Ledger

Sovrin Network is an open source framework for providing decentralized identity to users, managed by Sovrin Foundation [23]. The original code for Sovrin Foundation was developed by Evernym in the first place. The Sovrin Foundation contributed it to the Linux Foundation to become the Hyper Indy Project. It uses a public permissioned blockchain.

The nodes on this blockchain are called stewards. This permissioned ledger requires a governing body to approve who can act as the nodes. Stewards are responsible for operating the nodes that maintain the Sovrin Distributed Ledger. However, the user's attributes are not shared with the stewards and administrators without the consent of the identity owners [23]. Users' private data are stored on their choice of the device which means the private data about the users do not reside on the ledger itself [24].

Sovrin allows users to generate multiple identifiers which are required for separate identities of users for contextual privacy purposes. The identifiers are a pair of asymmetric key pairs that are unlinkable to each other. The identifiers are either managed by the user or appointed guardian service [25]. This service is for those who are excluded to manage their own identities, for example, a child or people with dementia.

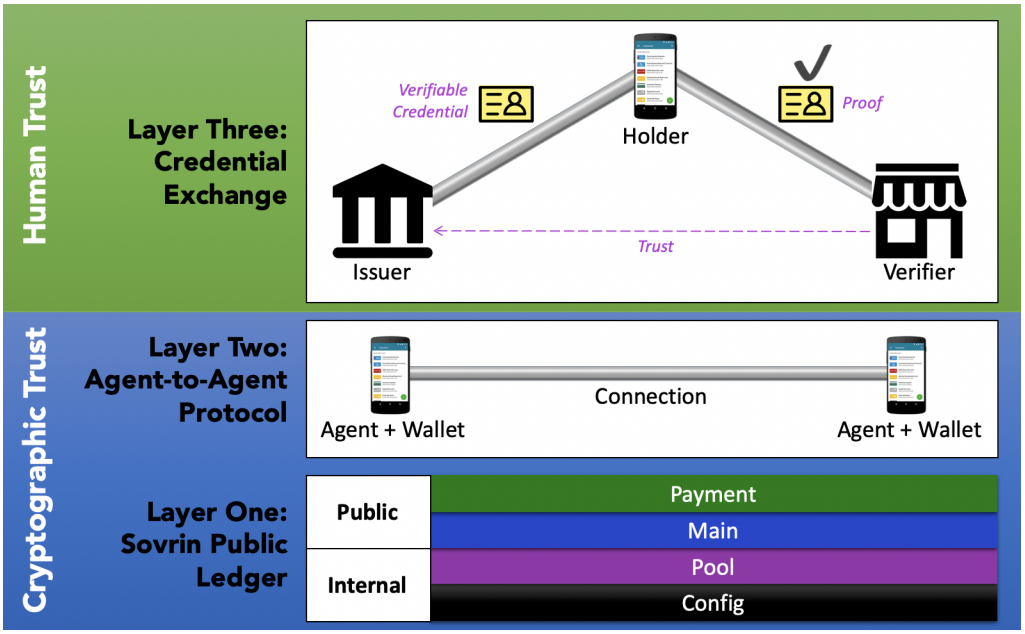



*Figure 8. Sovrin network architecture [31].*

Figure **8** shows the different actors involved in the Sovrin network architecture. The layer one is the ledger layer where information like DIDs, public keys can be stored. The layer two is where the communicating wallet forms a connection to support the credential exchange in the third layer.

The ledger is the heart of the Sovrin architecture, it contains transactions that are related to particular identifiers which are contained by the steward nodes. Two features of the ledger are no costly proof of work consensus as there is no mining like in the blockchain [26]. This reduces significant energy costs for running nodes and increases the number of transactions per second. The other feature is that trust in the network begins with a common root-of-trust formed by the globally distributed ledger, organizations and users can join the network and can form a "web of trust" [26].

A mobile application or software agent acting on behalf of users assists in the interactions with other agents on the network. The agents are network endpoints that are always addressable and accessible. Users can choose to run agents on their own servers or rely on third-party agencies. Cryptographic keys are stored and managed from the user's mobile device. The ledger is more preferable to identify the correct network endpoint to use. Otherwise, users can also use the ledger to store attribute-based credentials on the ledger, but it is not recommended to put private and sensitive data on the ledger [26].

The ledger nodes are operated by stewards categorized as validator nodes and observer nodes [23]. The validator nodes are responsible for validating new transactions. All the data that has to be written in the Sovrin Ledger must be sent to a validator node [24]. Sovrin clients write to the validator nodes and these nodes handle the write load of the network.

Another type of node is the observer node which is a read-only node of the Sovrin ledger. Validators serve three purposes [24]: first, they offload read requests and help to scale the performance of the validator nodes that run the Plenum consensus algorithm. Secondly, observer nodes can be swapped as active validator nodes in case of failure or comprising another validator node. Lastly, observer nodes send a push notification of events to subscribers without putting any load on the validator nodes.

The following goes on the Sovrin ledger [24]:

- Public DIDs and associated DID documents with verification keys and endpoints;
- Schemas and credential definition - Schemas are the data types and formats used to make claims;
- Revocation registries- for deleting or updating credentials by issuers;
- Agent authorization policies- enable an identity holder to prove to authorize their agents, which could be phone, laptop, etc.

The following does not go on the Sovrin ledger [24]:

- Private DIDs;
- Private Credentials;
- Consent receipt or records of credential exchange transactions.

The Sovrin Network is governed by the Sovrin Governance Framework (SGF) that is developed and updated by the Governance Framework Working Group(SGFWG) [52]. This Governance Framework Working Group is responsible to establish trust in the Sovrin Network. As a whole, SGF ensures that identity-related compliance and security requirements are met in terms of data security, privacy protection, portability, and individual control by preventing centralized control and central control when sharing identity data within the network.

The ledger is governed by the Board of Trustees of the Sovrin Foundation who approves the policies that select stewards. The evolution of the Sovrin open source code is also affirmed by the Board of Trustees [52].

## Hedera Public Ledger

Hedera is a public distributed ledger for building and deploying decentralized applications and microservices. The network consists of permissioned nodes run by the Hedera Governing Council, a group of enterprises that lead the path of the network. The ledger uses a hash graph algorithm as a consensus mechanism[28]. Hashgraph uses gossip protocol with virtual voting to achieve consensus on transactions. During the time of this thesis, the ledger is a permissioned type run by Hedera Governing Council but it is working to be a permissionless network node in the future.

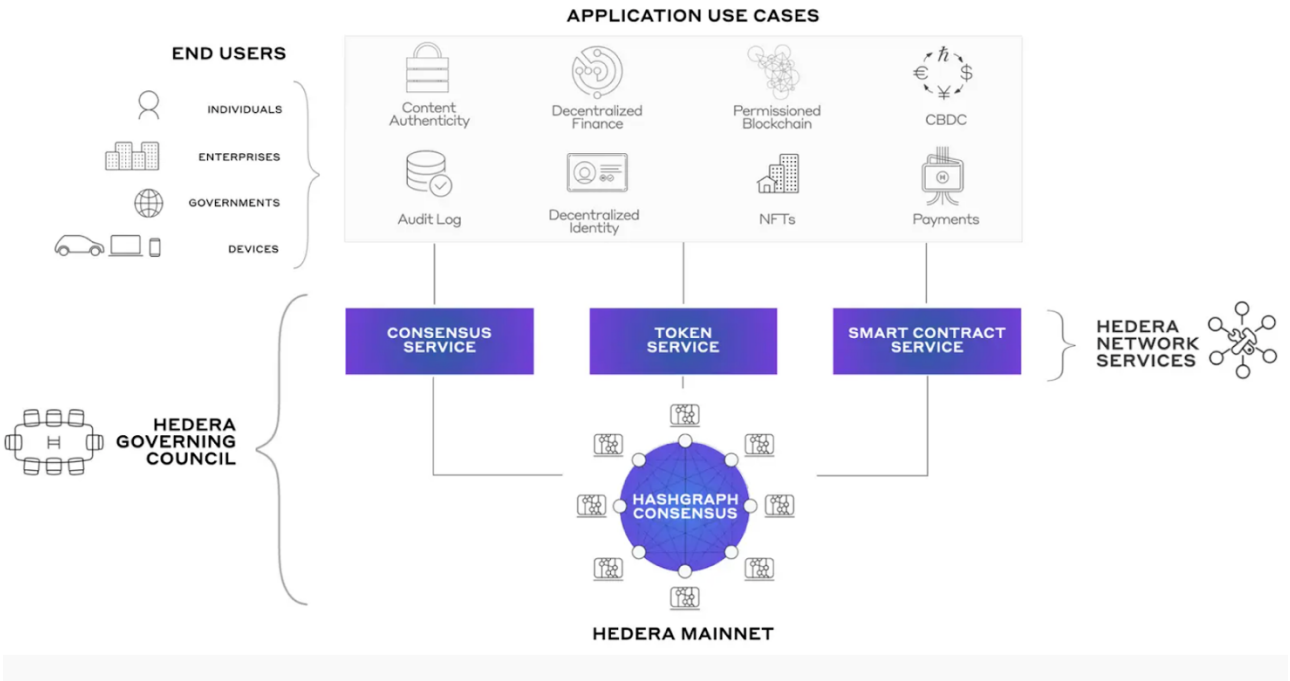



*Figure 9. Architecture of Hedera Network [32].*

The public ledger is stored on the mainnet, consisting of consensus and mirror nodes [29]. The consensus nodes participate directly in the consensus on transactions whereas the mirror nodes are value-added services that read-only properties. The whole ledger can be a single shard or subsets of multiple shards [29]. Initially, the network will be within a single shard, where a small number of nodes are operated by the governing council. In time, when the network grows, multiple shards are formed. A shard can store cryptocurrency, file, and deploy smart contracts when necessary. All sub-nodes in each shard of the ledger should maintain the exact state of the full ledger [29].

When a transaction has to be recorded in the ledger, a user begins by contacting a consensus node, the selected node then takes the transaction from the user and gossips it throughout the nodes within a given shard [29]. All the nodes run the hashgraph consensus algorithm to come up with an agreement on the time and order of that transaction. Each node then updates this consensus about the transaction to modify their shared ledger to ensure an identical consensus state [29].

Parallel to the consensus nodes are the mirror nodes. These nodes can not submit transactions for consensus and have no voting power. However, mirror nodes can be manipulated to add new services in any applications built upon the hedera network [29]. They can provide additional services such as providing audit support, access to historical data, and provide a way to get the state of the ledger to more users and applications [29].

Identity-related attributes or information should not be stored on the ledger, only the hash values [30].

In the Hedera network architecture (see Figure 9), the governing council resides to support and protect the network participants. Governance balances the interests of many different stakeholders in the network including operators of the network nodes, developers building applications on the platform, businesses reliant on the applications, and regulators [30]. It will comprise up to 39 members from a wide range of industries and geographic regions.

## IOTA Tangle

IOTA tangle is a distributed ledger technology created by the IOTA foundation mainly for IoT use-cases. The ledger is referred to as a tangle and is based on Directed Acyclic Graph. It is a public permissionless distributed ledger as anyone is allowed to participate in the network where they as nodes can initiate any new transactions and verify other transactions. Transaction validation occurs by validating previous transactions using proof of Work [33].

Any participants joining the network become nodes who can issue and can valid transactions. When transactions are issued, they are stored in a queue and two previous transactions need to be verified. The awaiting transactions are called tips. For the nodes to verify a tip, proof or work is performed [34].

The final validation is done by referencing signed transactions issued by the special node. The node is called the coordinator and thus a signed transaction is called a milestone. It is present in the tangle to ensure there are no bad actors in the network [35]. However, the presence of a coordinator in the network of IOTA Tangle makes it still centralized as validation of transactions is dependent on the central node designated by the IOTA foundation. The coordinator has been said to be a temporary solution and IOTA has announced replacement with another solution [37].

There are no miners in the network as the validation of transactions is performed by nodes and all IOTA tokens are premined [36]. The incentive for nodes to participate in the network is to process enough transactions so they are not dropped by neighboring nodes [34].

In regard to digital identity, IOTA has published a whitepaper that explains IOTA's vision for decentralized digital identity and how digital identity can be built on IOTA [38]. The proposed solution is called Unified Identity Protocol (UIP) and is built on W3C proposed standards for DID AND Verifiable Credentials. The solution allows things, organizations, and individuals to identify themselves online.

With the public and permissionless network, anyone can participate in the network on their own terms. The so-formed network claims to be neutral and trustworthy for identification as there will be no third-party incentivized by profit and the network itself doesn't have any access control [38].
Like many proposed solutions for decentralized identity, the three main roles will be issuer, holder, and verifier.

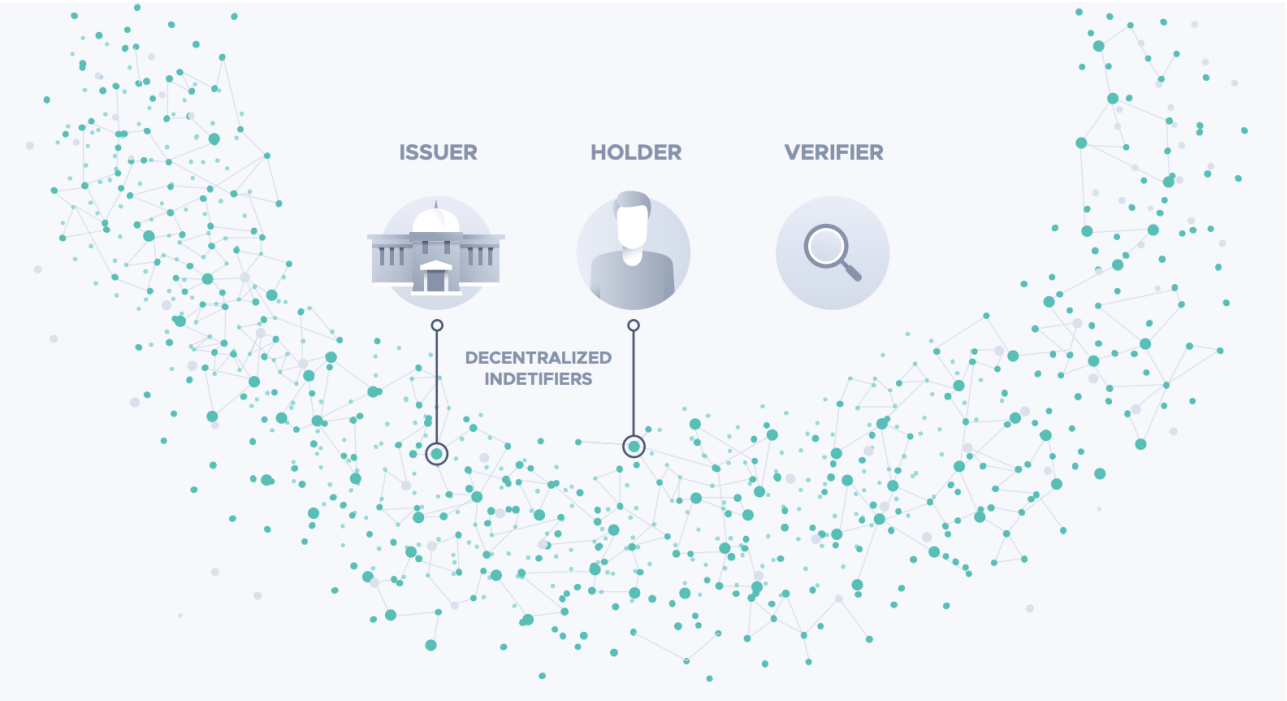



*Figure 10. Three roles in the IOTA Tangle proposed identity framework [38].*

Figure **10** shows the different participants in the IOTA Tangle identity framework. The figure shows the issuer, holder and verifier that are associated with the Tangle network.

It is not advised to store any personal data in the ledger to comply with legal requirements such as GDPR. The tangle (ledger) will be used only to store [38] :

- DID documents of the issuers and optionally of the holders
- The issuer's signature
- The issuer's public keys stored in the DID documents

A simplified interaction in this digital framework is illustrated in a scenario where a holder has to present some information to the verifier. Two interactions can happen in this course [38]:

Interaction between holder and issuer

- The credential is desired by the holder;
- Holder verifies to the issuer by logging into the issuer's environment by sharing his/her DID and requesting a credential;
- The issuer signs the credential with a cryptographic key registered in its DID document and encloses statements about the holder;
- The signed credential is sent to the holder which is stored by the holder either in a wallet or their personal repository.

Interaction between holder and verifier

- Verifier requests certain information about the holder;
- Holder sends his/her credential signed by the issuer;
- Verifier on receiving the requested credential can decide if it trusts the credential issuer, so looks into the tangle to verify the issuer's signature;
- On credential being verified meaning, it is signed by the issuer, and has not been revoked or altered at the time of signing can grant the holder access to particular resources from the verifier.

The proposed framework also claims to be used by organizations where it helps the organization to change their process to comply with new regulations [38]. Features like "Data Protection and Privacy by Design" can move the storing of personal data from an organization to individuals. For things, this framework has proposed a pay-per-use- model which means payments can be broken into chunks allowing individual payments. With the unique global identity of things, it will be convenient for people, organizations, and devices to pay for devices that can prove their ability to fulfill required tasks[38]. However, how this pay model will not be covered in this section as it is out of the scope of the thesis.

## Sub-Conclusion

Distributed Ledger technology and blockchain are used interchangeably. Blockchain is one of the types of Distributed Ledger Technology. There are other types of DLTs like DAG, and Hashgraph. They vary from the blockchain based on how information is stored, how consensus is achieved between participating nodes, and incentives to participate in the network as a node. However, they share common characteristics like the usage of public key cryptography, peer-to-peer network, and consensus mechanisms. A detailed comparison of these three variants of distributed ledger technologies will be done in the analysis chapter.

The study done on solutions based on three different DLT solutions show that distributed ledgers can be distributed data registry that allows storage of public keys and DIDs. The presented solutions use the distributed ledger as decentralized key registries for issuers using DID standards, which allows verifiers to verify signatures without relying on a centralized database.

Public ledgers allow the creation of multiple identifiers for multiple contexts for users. This allows users to have separate contextual identities. In Sovrin, the ledger is also used to store verifiable claims from different issuers, later users can select related attributes from those claims and create a verifiable presentation.

The research done on different types of wallet solutions, standards, technologies, distributed ledger, and DLT-enabled solutions showcase that distributed technology can be a technology enabler for a digital solution like EU- Digital Identity Wallet. However, the technology can not stand alone. It needs to support standards and communication protocols for data portability and interoperability. The solution should also ensure its compliance with the legal jurisdiction it is operating. In the case of the EU- the Digital Identity Wallet enabled by distributed ledger should comply with GDPR.

### 4.5 Digital Identity Wallet Examples

This section looks into different digital identity wallet solutions proposed by different companies. Different digital identity wallets will be explored to understand how the communication, and transaction of identity-related information are managed within the wallet ecosystem.

Furthermore, the underlying technology will be looked into, specifically to find out if they have made use of distributed ledger technology, if yes then what types of ledgers have been used. Looking at other wallet examples, I may be able to gain insight into what EU Digital Identity Wallet can learn.

## Connect.Me

Connect.Me is a digital wallet app created by Evernym that allows its users to hold digital credentials like passport, employee ID, and membership card in a digital form [44]. The underlying technology enabler for credential exchange in Connect.Me is hyperledger Indy, based on code contributed by the Sovrin Foundation. Users can form private connections with organizations that are in the Sovrin ecosystem., and add them as connections. They can request credentials from these connections which can be used in different contexts of use [44].

In its latest version, it states that users can connect, store credentials, exchange them privately and securely, and scan government-issued physical documents, turning them into digital credentials to store on the phone [44].

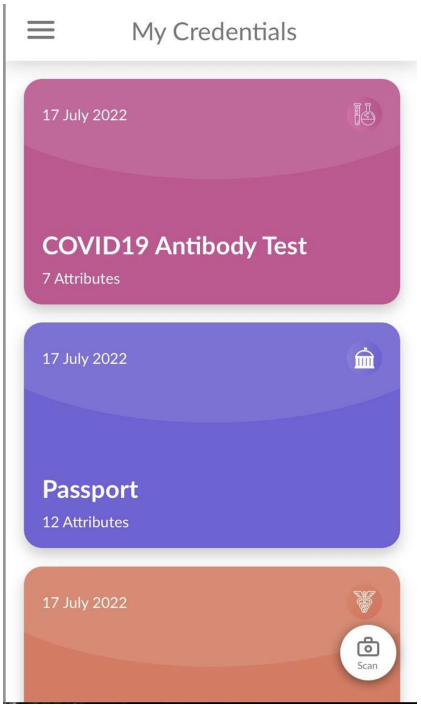



*Figure 11. Credentials examples that are retrieved by a user from his/her different connection organisation [44].*

Figure **11** shows one of the functionalities of Connect.Me. It shows a collection of credentials issued about a user by different issuers . They can be held by a user and present to access particular services from different verifiers.

One of the examples of functionalities is applying for a mortgage loan from a bank where users are required to submit some financial statements and employment IDs. With a scan of a QR code, users' credentials can be verified in a secure manner[44].

## Lissi Wallet and Esatus Wallet

Both Lissi and Esatus are digital wallets developed by the German-based organization IDunion[45]. These are applications that can receive, store, manage and share users' personal information in private connections enabled by the IDunion network. They can be downloaded both in the app store and google play[45].

IDunion network uses international standards such as Verifiable Credentials specified by World Wide Web Consortium(W3C), Decentralized identifiers(DID), proposed by W3C, and DIDcomm messaging protocol, as specified by the Decentralized Identity Foundation(DIF) to support different layers of the ToIP model [45]. As per distributed ledger, it uses blockchain-based Hyperledger Aries [45].

The wallets enable users to store and administer their personal information . This personal information is validated by public institutions and can be later presented by the users to companies and institutions when needed. When personal information is requested by verifiers, the wallets allow users to share only certain attributes that are required [45]. Users' data is stored on their local devices. The wallets enable institutions to identify users in a manner compliant with eIDAs. Furthermore, these wallets help companies and institutions to verify customers in a cost and time-effective manner [45].


*Figure 12. Collection of credentials from different issuers in lissi wallet example taken from apple store[46].*

Figure **12** shows the wallet interface of Lissi wallet.It shows different credentials that the users have acquired from different issuers. It also shows "connections' ' that can be the next page of the wallet app. The connection can be different private and public sectors that the user has added.

In order to collect these credentials, users of lissi first form connections with issuers who can be Identity Service providers like banks, Telcos, Credit bureaus, Loyalty Services, and so on [45]. These collected credentials can be later presented to relying parties in the form of self- attested documents, verified presentation as per necessary.

## Sub-Conclusions

These existing digital wallet projects share some common goals which are to use a digital identity wallet solution that allows users to receive, store, manage, and share their personal information. Another common aspect of these existing wallet solutions is that they tend to support the notion of self-sovereign identity to place users in the center of the electronic transactions where they have full control of what they share, whom they share, and how much they share.

The credentials exchange flow in all three of these solutions follows similar steps. When the holder wants to access any services from the service provider/verifier, the verifier requests certain credentials from the holder. The holder either presents it from his/her digital wallet or a request from the issuer and later provides it to the verifier. In this particular scenario the verifier, in order to trust the issuer, instead of establishing a communication with the issuer, looks into the data registry which is distributed ledger technology. From the data registry, the verifier looks into the DID of the issuer, and the public key of the issuer, and gains confidence in the validity and existence of the issuer.

Moreover, all the three wallet examples are based on W3C-based specifications such as verifiable Credentials and Verifiable presentation, and recommendations such as DID. As per the verifiable data registry, they have used a hyperledger variant of blockchain.

# 5. Analysis

This chapter takes the study and observation done on different distributed ledger technologies, different initiatives on standards and technologies in decentralized identity, digital wallet examples. It will make an analysis of the technical overview identified in the previous chapters to answer the problem formulation .

## 5.1 Comparison between different DLTs

Among different types of distributed ledger technologies are blockchain, Directed Acyclic Graph, and Hashgraph are the one explored. The basic principle and mathematical logic behind them were discussed.
DLT is simply a database that is shared across multiple distributed computer networks referred to as nodes. The nodes contain identical copies of the shared data and any changes to the ledger are replicated to all participating nodes. The variants of DLTs exhibit a common goal to establish global trust between stakeholders who do not trust each other. However they vary in many aspects; data structure, transaction, and consensus mechanism.

Along with the overview of three distributed ledger technologies, three DLT-based solutions were also reviewed. The choice of three kinds of DLTs was arbitrary but the three solutions were chosen such that they are using these three kinds of DLTs.

Another reason to review these solutions was to understand the use of different ledgers with different standards and technologies to provide decentralized identity to users. DLTs can be private, public, permissioned, and permissionless. Depending on the type, they also vary in terms of participants in the network, like who can publish transactions, and who can validate transactions in the network. The comparison between different DLTs will be done below under different properties:

### Data structure

Data structure refers to the format of the data stored on the distributed ledger. Among three types of distributed ledgers,blockchain uses an immutable and append-only linked list containing the elements' total order. System examples using this type of data structure are Bitcoin, Ethereum, etc.

On the other hand, two others; Directed acyclic Graph and Hashgraph uses directed acyclic graph as a data structure that leads to partial order of the elements.

Distributed ledgers use data structures to determine throughput - how many transactions can be processed - and latency - how long it takes for them to process a transaction time taken from the creation of a transaction to the initial confirmation that it is accepted by the network. The author of [53] has listed these two qualities as technical challenges to any DLT system.

## Transactions

Transactions are also referred to as actions [54] which are real-life activities represented digitally in a DLT system. In the blockchain, The transactions are grouped in a block. Numerous transactions are grouped together and stored in a block. A new block is connected with the previous block forming a chain to keep the blockchain transactions in chronological order.

In contrast, DAG contains a chain of individual transactions. Participants can submit many transactions as long as they confirm previous transactions. Whereas, in Hashgraph, transactions are performed via a gossip protocol meaning the participants share or gossip transactions with random participants. The transaction speed is faster in the two later DLTs than in blockchain as in the latter case, participants need to verify only two or more transactions.

## Consensus Mechanism

DLT systems rely on consensus mechanisms to establish the validity of entries on distributed ledgers. In order for a transaction to be permanently recorded in the ledger, a consensus needs to be reached. Blockchain uses proof-of-work to achieve consensus where the miners compete with each other to solve an arbitrary mathematical puzzle. This is done to prevent double-spending of tokens and prevent Sybil attacks. However, it requires a lot of computational processing power that increases as more miners join the network.

Similarly, a small amount of proof of work is required also in DAG. As there are no miners in DAG, participants perform the proof of work where they validate two closet transactions. Tangle which is based on DAG, the final validation is done by the coordinator node which is controlled by IOTA Tangle. On the contrary to these, Hashgraph relies on virtual voting consensus. The nodes do not need to take into account the entire transaction history. With a virtual voting algorithm, nodes can predict how other nodes might vote.

## Types of Ledger

The wallet examples and the DLT-based solutions I have reviewed use a public-permissioned distributed ledger except for IOTA tangle which uses public-permissionless. The ledger in public-permissioned distributed ledgers is public and anyone can use it. However, permissioned refers to the network's operation and nodes that act as validators. For instance, in Sovrin, everyone can use the Sovrin ledger to make transactions but only stewards run the validator nodes in order to achieve consensus on the transaction on the ledger.

IOTA tangle uses a public-permissionless ledger. Anyone can use the ledger not only to make transactions but can participate as validator nodes. The participants perform a small amount of proof of work by validating two previous transactions. However, the final transaction is validated by a coordinator node. All these examples presented vary from the bitcoin blockchain which is public and permissionless. Anyone is free to join the bitcoin network and act as a node and participate in achieving consensus of a transaction. The Bitcoin network is an example of a truly decentralized network whereas the examples presented here can not be perceived as a truly decentralized network.

## Participants

Participants are those who are associated in the network mainly to issue and validate transactions in the ledger. In the blockchain, there are mainly two participants; issuer and miners. The users of blockchain are transaction issuers and miners are the ones who validate transactions. In DAG-based tangle, the users are called entities, they can submit a transaction and validate two previous transactions. Apart from the entities, there is a milestone node called “co-ordinator” that is involved

to validate the submitted transaction. In Sovrin there are “sovrin clients” who write to the stewards who operate the network. Stewards responsible to write on the ledgers are validator nodes, and exhibiting read-only functionality are observer nodes.
At times of necessity, they can be validator nodes too. In the case of the Hedera Hash graph, the participants in the network are the consensus nodes operated by the Hedera Governing Council. They receive transitions from users charging transaction fees and participate in consensus. There are also mirror nodes, they store transactions and are ways to query the history of transactions from the public ledger.

Defining who can be participants in the ledger indicates how users can engage with the ledger whether to create any transactions or whether they can participate in the consensus. In addition, it also determines what kind of permission users exhibit such as reading the transaction history on the ledger, submitting transactions on the ledger through the user-agent or users directly submitting transactions on the ledger.

## Information that goes on the ledger

The overview of the wallet examples and DLT-based solutions recommend storing private data like identity-related information on users' local devices instead of storing on the ledger. When private data is stored on the ledger, any compromise on users’ keys may lead to compromise of data shared by the users with any service providers or relying parties. Further, data stored on the ledger can not be deleted or its existence can not be denied. Distributed Ledgers store data permanently.

So, storing private information can create data correlation as the data stored on the ledger are indestructible. Sovrin for example recommends to store only public DIDs, DID documents , schemas and credential definitions, revocation registries and agent authorization policy.

On Tangle, DID documents of issuers, issuers’ signature, issuers public keys are the only information that is suggested to store on the ledger. The storage of users/holders’ DID documents is left optional. In Hedera Hashgraph they recommend only storing hash values of identity related

information in the ledger. In the wallet examples, the credentials are stored all in the users' wallet. The only thing that is stored on the ledgers are the public keys of the users.

Distributed ledger technology offers immutability and transparency to data stored in the ledgers. These properties however are not favorable to store personal information. With transparency, one has to pay the price for privacy. Any data once stored in the ledger lives there permanently making the data immutable. This may result in complexity or even impossible to remove or erase data, negating compliance to data rights such as GDPR. Instead of storing private data, distributed ledgers can be used to store transactions, hash values of data, and public keys, DIDs of the issuers.

## 5.2 Consultation

A consultation was taken in the earlier stage of the thesis. It was conducted under controlled conditions, where a list of questions was prepared in advance and mailed to the participant by my supervisor.

The participant was Mogens Rom Andersen, Public Sector Lead Architect, mitID, Agency for Digital Government. My supervisor and I made a zoom call with him and asked the prepared questions.

The objective of this consultation was to get some updates on the development of the EU Digital Identity Wallet and to know how it can integrate with the Danish eId, which was in the process of replacing NemID during that time.

At the time of this consultation, the wallet interface has not been defined, and the working group is focused on specifications. There are current discussions being made about different standards that are to be used by the wallet for various purposes like personal data identification, choice of authentication protocols, and choice of cryptography.

When asked about the necessity of the EUDIW wallet, he explained that many member states have multiple eIDs for different use cases. The issue with such fragmented eIDS is that they do not work

to satisfy the cross-border use of eIDS. So, EU digital solutions aim to solve this interoperability through international standards.

One of the interesting findings from this meeting was that there is no binding in the choice of technologies. There is still uncertainty about what kind of technical implementation may come. What is certain is that the wallet development and implementation will abide by the revised eIDAS framework.

When we asked about the need and choice of a data registry like blockchain for the wallet, he said that it is needed for selective disclosure but it should not necessarily be Distributed Ledger Technologies. It could be anything such as a server hosted by the state. It is also still an open question whether to use data registries like blockchain in the wallet ecosystem of credentials.

About the wallet being integrated with Danish infrastructure, he mentioned in the future they may co-exist but it might take a long time to replace the mitID with the EU Digital Identity Wallet as it depends on how the adoption will go. There is a possibility for service providers to have a dual connection with mitID or the wallet or just choose one of the solutions.

## 5.3 Use of DLT, DID, VSCs in the digital identity wallet

While considering the use of distributed ledger in digital identity wallet, it can be a public permissioned ledger like Sovrin with a condition that the interacting parties are in the same network. The standards used for the discovery of issuers, issuance and exchange of credential can be based on standards like Verifiable Credentials and Decentralized Identifiers . A simple flow of interaction between the holder, issuer and verifier occurs in the following steps.

***Use-case Example***: Applying for a job

The first thing a user need to do is create an decentralized identifier and register in the public ledger. Users should be allowed to create multiple identifiers to establish relationships with multiple stakeholders they are interacting with. Then the user adds her university, bank, and government in

her connections. The university, government, and bank can be the issuers who on request issue verifiable credentials to the users.

Credentials issued by the government can be government ID attested by the government, a transcript issued by the university and bank details issued by the bank. These are verifiable crdentails signed by the respective issuers' public key which are contained in the DID document of them. The verifiable credentials also contain DID of each issuer. The users can hold these credentials in her wallet.

Now, when she applies for a job that in return asks her to provide required attestations. The user can now verify these credentials through cryptographic proof encoded inside the credentials. The user can also present a verifiable presentation by combining verifiable claims from different credentials in other required for minimal disclosure.

## Incentives for Verifiers

The use of DLT, DIDs, VCs should have something to offer to the verifiers to use them. Lets look into the same example of a user applying to a job. The issuers are the bank, government, and a university. The verifier is a private company. The verifier can look for issuer's DID that can be resolved into DID document. From the DID documents, verifier can find the issuer' details, the public key used to sign the credentials, and service endpoints to interact with the issuer. This helps the verifier to verify the verifiable credentials signed by the issuer and not being tampered with, Further the verifier can find information about revocation of credentials. This can enhance trust in the credentials received by the verifier.

Other incentives for the verifiers can be:

- Monetary - verifier has to spend money to do verification, for example, financial institutions do not need to do the Know Your Customer (KYC) again. They can do less KYC without relying on KYC vendors
- Minimization on the cost of GDPR Compliance:

- Stakeholders who do not trust each other can have a trusted infrastructure to share data in a secure and accountable manner. The onboarding process becomes simpler due to reusable credentials and verified data for service providers.

### Incentives for nodes

In the distributed ledger nodes play vital roles as they are the one who validate and decide the order of transactions in the ledger. They can have some privilege such as stewards, they will have direct access and can perform reading or writing transactions than sovrin clients. This seems a bit unfair to those who are not stewards. To prevent any bad actors from being a node, there should be a governing body forming framework, setting policies and rules for the nodes.

## 5.4 Stakeholder analysis

The stakeholders of the digital identity wallet are the users /holders , the issuers- they can be public authorities , public and private institutions, and the verifiers- they can be service providers, public and private institutions as the role of verifiers can be exhaustive.

The stakeholder analysis is done to see how the EU- DIgital Identity wallet works from the perspective of mit-Id. The analysis will not cover in depth how EUDI Wallet can integrate with mit-Id. It will rather focus more on the possibility of these two systems working together. The information supporting this section will be based on the consultation done and presentation [61] done on the topic of mit-ID and EU Digital Identity wallet.

When we look into the structure of the mitID , mitID lies in the core with its surrounding layers as shown in figure below. When a user wants to access any service from a service provider, the users are redirected through a broker. The broker then accesses the core, returning the result of authentication to the service provider to enable the access of the service.

When the EUDI Wallet will be introduced, there should be a mechanism for the wallet and MitId to communicate. Based on the consultation, if an non-EU citizen ( residing outside of Denmark) has

to access public service from Denmark, mitID has a feature that matches or converts the received identifier to the corresponding CPR which is the Danish Social Security Number. This hints at the co-existence of mitID and the EUDI Wallet in the future. In that case, it is crucial to find the right architecture to support the interoperability between them as EUDIW Wallet is a more decentralized approach and mitID is centralized approach.

In regard to adoption of the EUDI Wallet in Denmark, there is a possibility of using both mitId and the EUDI wallet simultaneously. The wallet might be more viable when one is traveling to other EU nations or accessing online services from other EU countries. It is more likely that to access any public or private services from Denmark, people will still choose mitID as it is developed focusing a smaller scale of users compared to the wallet focusing on a huge population. People will be skeptical about using the wallet. From the Danish perspective, it is crucial that such a solution should be implemented by complementing and integrating with the existing Danish infrastructure [61]. This could benefit citizens, public authorities, and businesses if done right.

## 5.5 Use of DLT and eIDAS Compliant

The EU Digital Identity Wallet will be built on the foundation established by eIDAS regulation.
The aim of developing the wallet is to enable trusted digital identities for all Europeand where they have control of their online interaction and presence [58]. The possible roles of the EUDI wallet ecosystem have been listed in a “Reference Framework Architecture” that is being developed along with the toolbox. In this list there are listed the potential stakeholders of the wallet ecosystem that includes the end users, wallet issuers, Personal identification Data Providers, Relying Parties, and more.

Distributed Ledgers technology that is public and permissioned has potential to be pubælic verifiable registry. In that case, the roles defined in the EU DIgital Identity Wallet can be reorganized . For example, Lissi wallet has proposed such an arrangement [59]. However, it doesn’t propose distributed ledger as verifiable data registry. However, it recommends about some providers of registries of trust source such as public key Directory to store public keys of issuers, list entries.

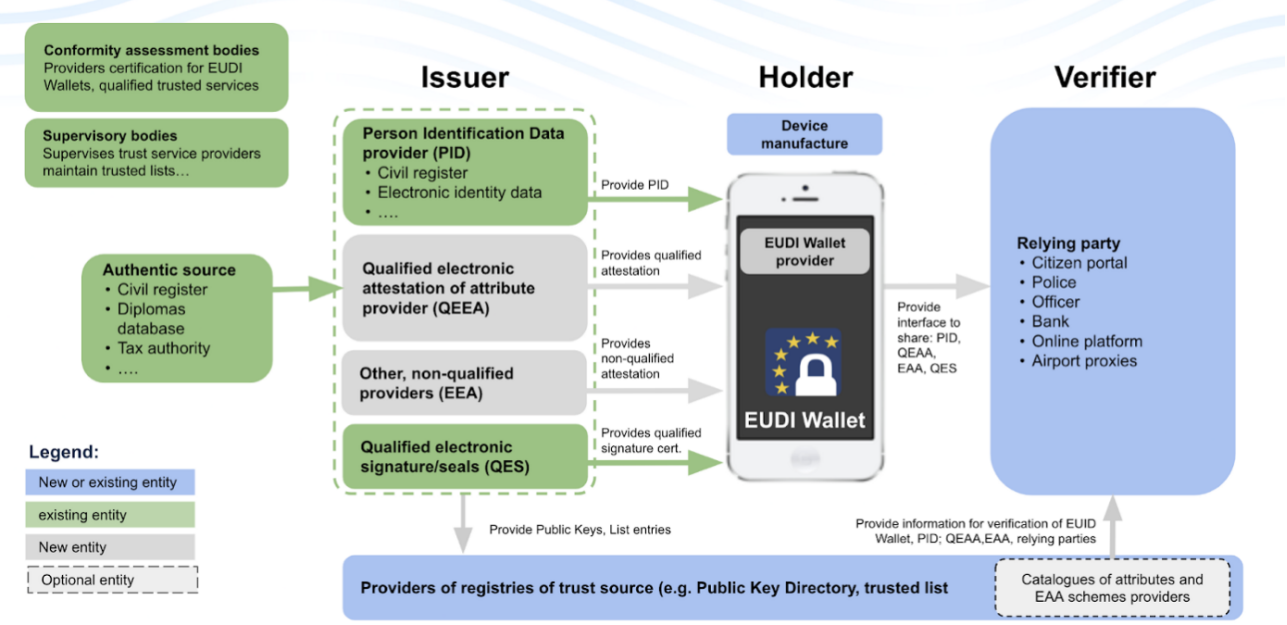



*Figure 13. The illustration of roles when interacting with the EUDI Wallet [59].*

The roles in the EU Digital Identity Wallet can be seen grouped into issuer, holder and verifier. This ecosystem will support identification, authentication, the verification of third parties, and creation of qualified electronic signatures.

Figure **13** shows the different stakeholders of the EUDI Wallet in a way that it is compliant to Self-Sovereign Identity [39]. The figure shows the wallet as the mechanism to interact with the issuer and holder. The arrow between different stakeholders shows the communication between them. The issuer needs to provide information to the registry [39]. This information can be contained in the document presented by the holder to the verifier. The verifier can take this information of the issuer and look into the trust registry.

## 5.6 SSI Principles

The distributed ledgers are seen as the architectural component in the solutions reviewed that can enable SSI . This section will look into to what extent the distributed ledgers can fulfill the SSI principles. However, these are not to be taken as strict requirements rather guiding principles.

Each transactions are signed by the original parties , written in the ledgers and are verified by consensus mechanism in the distributed ledger. The consensus mechanism prevents falsification of transactions. This enables **Persistence** on the transactions on the ledger as the transactions are immutable once written on the ledger. Revocation registries on the ledger allows modification such as update or erasure of claims but it is done vai the issuers.
The use of standards like DIDs, verifiable claims with the ledger allows users to select only required attributes for selective disclosure. This enables **minimization** on information disclosed in the form of claims.

The only easy way to get access to the user related information is through the users' private key. The nodes and administrator on the ledger can not view user attributes. This provides user **control.**

In public permissioned ledger such as Sovrin, the nodes need to have user's **consent**, in order to share users attributes with the nodes

In public ledger, the transactions can be viewed by everyone in the network so that nobody can deny it providing **transparency.** However, there should be a balance between transparency and privacy. Therefore, writing personal data on the ledgers is not advised.

The public keys, public DIDs stored on the public ledger are **accessible** by the users of the ledger residing in any jurisdiction .

Self sovereign identity is not about the technology alone but it is more about control of users' data and their personal information. It should therefore be reviewed also from a non-technology perspective.

## Self-Sovereign Identity from the perspective of technology-free definition

To exploit the opportunities of Self-Sovereign Identity, it is advisable to understand the technology-independent requirements for both subjects and observers [22]. In a review paper by Joe Andrew, the author has described sovereignty as not having to ask for permission and further

asserted that the self-sovereign identity system allows users to selectively present their own means of identification both online and offline [22].

Self Sovereign identity doesn't control how others identify a user but it allows a user to influence how other parties like companies and governments correlate a user interaction across different services and locations by putting the user in control of most uses of identity. In order to comply with One of the needs of UN Sustainable Development Goal 16.9, " identity assurance can't depend on pieces of paper, devices, or other artifacts that can be lost, destroyed and falsified", Sovereign identities must be robust enough so it is possible to recover [22]. This may be a challenge from a technical perspective to achieve.

# 6. Discussion

This chapter makes a brief discussion about the viability of distributed ledger to the EUDI Wallet. In this regard, it will focus on challenges and consideration for using the distributed ledger technologies in the implementation of EUDI Wallet.

## 6.1 Distributed Ledger Technology and viability Scope

### Use-case suitability

While considering the use of DLTs it is necessary to consider in the first place if the use-case is suited for a DLT-based solution. In the case of EU DIgital Identity Wallet, the eIDAS toolbox is working in five use-case with an objective to promote trusted digital identity and putting users in control of their online activities [58]. To name a few of the use-cases, they can be opening a bank account, applying for a university in the same as another member state, proving age, renting a car using a driver license [8].

In the wallet, distributed ledger technology allows storage of identity related references like hash value, public DIDs, and public keys for anyone in the network. Identities linked to decentralized identifiers can be created and stored on the distributed ledgers. They are immutable, transparent and secure. Furthermore, Decentralized identifiers facilitate discovery of list of issuers in the wallet ecosystem .This also eliminate the need to rely on intermediary as an identity provider.

In the DLT-enabled digital identity wallet, users can control their own data through cryptographic keys. With verifiable credentials and DIDs in the wallet, users can perform activities like opening a bank account, applying to university, proving age with fewer steps and in a shorter time period in a secure and private manner.

## Type of ledger

The next thing to consider is then what kind of ledger should it be. Public Permissionless are not suitable candidates as everyone can not only access it but will be able to write on the ledger. This will affect the privacy, security and scalability of the ledger. With the private permissioned, they are more suitable for enclosed environments.

The DLT-enabled solution and wallet examples reviewed indicate that public permissioned can be a suitable type of DLT for the wallet. This facilitates everyone access in the network but only permissioned parties can write and validate transactions on the ledger. The nodes in the public permissioned ecosystem can be public authorities, private authorities, private authorities like banks who can be the issuers and verifiers in the wallet eco-system. Since it is public utility then there should be a government trust framework defining policies and rules for the nodes and participants in the network.

## Consensus Mechanism

In regards to choosing a consensus mechanism, other consensus mechanisms other than proof of work should be used. With proof of work, it requires a lot of computation power which is not a practical approach. Other mechanisms should be considered .

## Other Factors

Moreover, there should be regulators to confirm what kind of data is coming in and going out. There should also be rules and security measures for the regulators . The DLT-enables solution should also make sure that it operates within law. In the EU it should comply with GPR and e-IDAS regulation.

The “right to be forgotten” in the GDPR, constitutes a major consideration as the information on the distributed ledgers are immutable -meaning stored permanently. However, on request of users, their information should be removed. Therefore, distributed ledgers should used only for storing hash pointers to the personal information stored off chain- meaning outside the ledger.

Apart from this there should also be some network effects of the solution meaning it should benefit one who is not using the network.

## 6.2. Viability of the ledger with the cross border

To discuss the viability of the ledger with cross-border context, I will be looking into how one can open a bank account in another member state with the Federated identity scheme used in Government, eIDAS. Then I will look into how one can open a bank account with a DLT-enabled digital wallet. The latter will be only a conceptual idea. To discuss the login with e-IDAS , I have taken this information from [60].

### User experience within eIDAS

- Context: Trying to get an account with a bank in any EU country other than yours;
- Steps: Login to eIDAS, pick your home country, from list of identity providers select one provider and login , after login with them they will confirm back to the bank.

The complexity here is multiple systems are involved in the attribute exchanged and consume more time.

### User experience with the DLT-enabled Wallet

- Context: Trying to get an account with a bank in any EU country other than yours
- Steps: Identity issuer of one country will issue credentials for a person, the person will present to the bank of another country .

Once a user has credentials within their control, it will unleash a lot of power to the user as they can use it for multiple purposes.

## 6.3. Challenges associated with DLTs

Distributed Ledger Technologies has several opportunities to offer the EU digital identity wallet, however, there are many challenges associated.

- Firstly, in the public permissioned ledgers, nodes are a predefined set of actors, that interfere with the idea of decentralization. As seen in the Tangle ledger, it is the coordinator node that validates the final transaction. This still put a central authority in control.

- As there are more and more verifiers and more users are connected scalability will be another issue. This may affect the latency and throughput of the network.

- Consensus mechanisms such as proof-of- work are slow which can take relatively longer time to validate a transaction.In addition, such consensus mechanism require more computational power.

- The Key management and private data storage is another issue . When users lose their device, they can lose their private key and all the identity related data stored in the DLT. There should be solutions like cloud storage provided by third party as a back up.

- Distributed Ledger Technologies are still immature technologies and standards developed to support DLTs too. Standard maturity is needed for interoperability between different types of DLTS.

## 6.4. Separation of technical and legal issues

Legal issues and technical issues related to EUDI Wallet should be treated separately .
For example, X, graduates from a university; it can be a public statement declared by a legal entity. In this case, the standardization will focus on how to onboard this information on the wallet, on the system of credentials and attributes, and what format and what techniques can be used to carry this information in and out of the wallet. This should be irrespective of any legal values that depend on the different legal environments; in the case of the EU, there are 26 legal environments.

# 7. Conclusion

Digital identity makes online interaction possible and with the advent of internet and technologies, online presence are increasing more than ever. On the other hand, the data the information that are shared over the internet are scattered everywhere, users are losing track of their information. Security and privacy issues such as identity theft, misuse of users data are the prices users are paying . This is obvious as internet was built without an identity layer.

To address this, identity models are evolving from silod based to decentralized with a effort to make digital identity more scure and provide users control over their data. In this regard, ther are many initiatives taking places from organisation a and governmental level. One of such initiatives is the EUDI Wallet that is moving towards more decentralized approach. With the wallet in place, its objective is to establish a digital trust and provide users to decide what to share, who to share and how much to share with any private and public service providers. However, how can the wallet solution meet the objectives and how it can be operable with other national eIDS of the other member states such as MitID.

DLTS has gained a lot of attention from industry, the Government, and scholars. DLTS exhibits some properties that make it a suitable technological choice for several application domains. They are also considered technological blocks of self-soverignn identity. Therefor, to assess this technology and investigate its usability in the EUDIW Wallet, I performed the following investigations:

- study on different distributed ledger technologies, comparison was made
- Different standards and technology enablers of the digital wallet solutions were reviewed
- Stakeholder analysis was done to see how digital wallet may fit in Denmark's context
- Viability of the DLTs was analyzed
- Challenges associated with using DLTs in the EUDI Wallet were discussed.

Therefore, I would answer the problem formulation and its sub questions as:

**"How can DLTs play a role in realizing the potential of the EU digital identity wallet?"**

Distributed ledger technology can play a role in realizing EU digital identity wallet by facilitating cross-border transactions, enabling mutual authentication of users in both private and public services, and enabling storage and sharing of users' documents and data in a way that is both secure and compliant with regulations such as GDPR. Further, it supports the principle of self-sovereign identity by placing users in control of what to share, how much to share and who to share.

Based on the study done on the subject matter, I would answer the sub questions as:

"What are the opportunities and challenges of a DLT for the EUDI Wallet?"

➢ The opportunities of DLT for the EUDI Wallet are:

- Allows immutable record of hashes of identity information , as information such as public DID, public keys, Schema definition, Revocation registry .
- Provide user control over what they share as technologies such as VCs, Decentralized Identifier along with the DLT enable user for minimal disclosure
- Removal of third party as an identity providers as issuers are the one who provides attestation of documents
- There is less chance of corelation in users identity information as users can generate multiple DIDs for multiple contexts
- The cross border transaction are efficient , and other more aas discussed in te report

➢ The challenges of DLT for the EUDI Wallet are:

- Scalability issues as the network grows
- Use of more resources and enegry to achieve consensus
- Lack of matured standarization
- Key management issues '

- Lack of regulation

“How do DLT comply with the principles of self-sovereign identity ?”

➢ Based on the analysis and discussion made, DLT complies with some of the principles of Self -Soveriegn Identity. However, depending on the type of ledger , it can be extrapolated that DLT will support the principles only partially.

“What will be the applicability of EUDI wallet with MitId ?”

➢ In regard to this question, based on the discussion made, it is found that the EUDI Wallet can bring value to Danish citizen if implemented properly. Nonetheless, if implemented properly, such a solution would benefit citizens, public authorities, and businesses if it complements and integrates with the existing Danish infrastructure.

# References

[1] J. V. Schorlemer, "SELF-DETERMINED DIGITAL IDENTITIES ARE THE BASIC BUILDING BLOCK FOR A DIGITAL ECONOMY," *bpö*, 18-Jan-2022. [Online]. Available: https://www.blog-bpoe.com/2022/01/18/schorlemer/. [Accessed: 08-Jan-2022].

[2] Cybersecurity in the Remote Work Era - A Global Risk Report. (n.d.). Keeper. Available: https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf [Accessed: 20 -Jan-2022].

[3] DATA PRIVACY, ETHICS AND PROTECTION GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA. (n.d.). United Nations Sustainable Development Group. [Online]. Available: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf [Accessed: 20 -Jan-2022].

[4] Digital ID Wallet – Your credentials at hand ( Mobile ID Services). (n.d.). Thales. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/digital-id-wallet [Accessed: 18 -Jan-2022].

[5] Towards a European digital identity wallet: competitive, business-enabling, and safe, The Paypers, 29- Sep -2021 [Online] Available: https://thepaypers.com/expert-opinion/towards-a-european-digital-identity-wallet-competitive-business-enabling-and-safe--1251804 [Accessed: 28- Jan- 2022].

[6] A. Preukschat , & D.Reed, Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials, 2021

(7) Kørekort-appen. (n.d.). Digitaliseringsstyrelsen. [Online] Availbale: https://digst.dk/it-loesninger/koerekort-app [Accessed: 20-Jan- 2022]

[8] European Digital Identity | European Commission. (n.d.). European Commission. [Online] Availbale: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en [Accessed: 20- Jan- 2022].

[9] Commission proposes a trusted and secure Digital Identity for all Europeans, European Commission, 3-June-2021. [Online] Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663 [Accessed: 20- Jan- 2022].

[10] (n.d.). Cambridge Dictionary | English Dictionary, Translations & Thesaurus.[Online] Available: http://www.evernym.com/connectme [Accessed: 20- Jan- 2022].

[11] Project – IDunion. (n.d.). IDunion. [Online] Available: https://idunion.org/projekt/?lang=en [Accessed: 20- Jan- 2022].

[12] G. Ben Ayed, "Architecting User-Centric Privacy-as-a-Set-of-Services: Digital Identity-Related Privacy Framework", Springer International Publishing, 2014

[68] S. Amarpreet, " Hashgraph vs Blockchain: Is Hashgraph the Future & What's the difference ?", *medium.com*, 5- May- 2021 [Online] Available: https://medium.com/brandlitic/hashgraph-vs-blockchain-is-hashgraph-the-future-whats-the-difference-3f2b33adb529 [Accessed: 11- Aug- 2022].

[14] K.Cameron, "THE LAWS OF IDENTITY" – Kim Cameron's Identity Weblo, Kim Cameron's Identity Weblog, 8-Jan -2006 [Online] Available: https://www.identityblog.com/?p=352 [Accessed: 22 - Jan- 2022].

[15] M. Laurent, & S.Bouzefrane, "Digital Identity Management" , Elsevier Science, 2015

[16] T. Hahn, The Evolution of Digital Identity, | by Tomas Hahn | helix id. Medium, 10- Oct- 2019. [Online] Available: https://medium.com/helix-id/the-evolution-of-digital-identity-cc54917a6a49 [Accessed: 21 - Jan- 2022].

[17] C. Allen, "The Path to Self-Sovereign Identity", Life With Alacrity, 25- Apr- 2016. [Online] Available :http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html [Accessed: 22 - Jan- 2022].

[18] P. J.Windley, "The Inevitable Rise of Self-Sovereign Identity", Sovrin, 29 - Sep - 2016. [Online]
Available:
https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf [Accessed: 22 - Jan- 2022].

[19] D.Pöhn. M. Grabatin, & W. Hommel, "eID and Self-Sovereign Identity Usage: An Overview", 16- Nov- 2021. [Online]
Available:https://www.mdpi.com/2079-9292/10/22/2811/htm [Accessed: 22 - Jan- 2022].

[20] (n.d.). EIDAS SUPPORTED SELF-SOVEREIGN IDENTITY. Available: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf [Accessed: 23 - Jan- 2022].

[21] Sesana, J. (n.d.). The 10 principles of Self-Sovereign Identity (SSI). Self Sovereign Identity. Available: https://www.selfsovereignidentity.it/the-10-principles-of-self-sovereign-identity-ssi/ self-sovereign-identity/characteristics-of-sovereign-identity.md at master [Accessed: 23 - Jan- 2022].

[22] WebOfTrustInfo/self-sovereign-identity. (n.d.). GitHub. Available: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/characteristics-of-sovereign-identity.md [Accessed: 1 -Feb- 2022].

[23] Overview. (n.d.). Sovrin. Available: https://sovrin.org/overview/ [Accessed: 2 -Feb- 2022].

[24] "What Goes on the Ledger?", Sovrin, Apr 2017. Available: https://sovrin.org/wp-content/uploads/2018/10/What-Goes-On-The-Ledger.pdf [Accessed: 2 -Feb- 2022].

[25] J. Andrieu, Guardianship Whitepaper2, Sovrin, Dec 2019. Available: https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper2.pdf [Accessed: 2 -Feb- 2022].

[26] C. Allen, "The Technical Foundations of Sovrin", Evernym, 29-Sept- 2016. Available: https://sovrin.org/wp-content/uploads/2018/03/The-Technical-Foundations-of-Sovrin.pdf [Accessed: 4 -Feb- 2022].

[27] P. Lewis, A. Thornhill, & M Saunders, *Research Methods for Business Students*. Pearson, 2019

[28] Baird, L. (n.d.). How it works. Hedera. [Online] Available: https://hedera.com/how-it-works [Accessed: 3 -Feb- 2022].

[29] L. Baird, Hedera: A Public Hashgraph Network & Governing Council. Coinpare, 29- Aug -2019. [Online] Available :https://crebaco.com/planner/admin/uploads/whitepapers/hedera-whitepaper.pdf [Accessed: 13 -Feb- 2022].

[30] Hedera Global Governing Council. (n.d.). Hedera. [Online] Available: https://hedera.com/council [Accessed: 23 -Mar- 2022].

[31] P. Windley, Decentralization in Sovrin. Phil Windley's Technometria, 23 -Oct- 2018, [Online] Available: https://www.windley.com/archives/2018/10/decentralization_in_sovrin.shtml [Accessed: 23 -Mar- 2022].

[32] What is Hedera? (n.d.). Hedera. [Online] Available: https://hedera.com/learning/hedera-hashgraph/what-is-hedera-hashgraph [Accessed: 3 -May- 2022].

[33] What is IOTA. (n.d.). IOTA. [Online] Available: https://www.iota.org/get-started/what-is-iota [Accessed: 4 -July- 2022]

[34] The Tangle, The Tangle, 30-Apr-2018. [Online] Available: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf [Accessed: 4 -July- 2022].

[35] IOTA Introduction. (n.d.). IOTA Wiki. [Online] Available: https://wiki.iota.org/learn/about-iota/an-introduction-to-iota#consensus-in-a-blockchain [Accessed: 4 -July- 2022].

[36] Agnihotri, N. (n.d.). Title: What is IOTA? How Tangle works? IOTA Vs Bitcoi. Engineers Garage. [Online] Available: https://www.engineersgarage.com/what-is-iota-and-tangle/ [Accessed: 4 -July- 2022].

[37] The Coordicide, IOTA, 20-Jan-2020. Available: https://files.iota.org/papers/20200120_Coordicide_WP.pdf [Accessed: 4 -July- 2022].

[38] Millenaar, J. F. (n.d.). The Case for a Unified Identity. IOTA. [Online] Available: https://files.iota.org/comms/IOTA_The_Case_for_a_Unified_Identity.pdf [Accessed: 5-July-2022].

[39] Decentralized Identifiers (DIDs) v1.0. (n.d.). W3C. [Online] Available: https://www.w3.org/TR/did-core/ [Accessed: 5-July- 2022].

[40] Verifiable Credentials Data Model v1.1, W3C, 3- Mar - 2022. [Online] Available: https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential [Accessed: 12 -July- 2022].

[41] Verifiable Credentials Data Model v1.1, W3C, 3- Mar- 2022. [Online] Available: https://www.w3.org/TR/vc-data-model/#ecosystem-overview [Accessed: 12 -July- 2022].

[42] Verifiable Credentials Data Model v1.1, W3C, 3- Mar- 2022. [Online] Available: https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations [Accessed: 12 -July- 2022].

[43] Verifiable Credentials Data Model v1.1, W3C, 3- Mar- 2022. [Online] Available: https://www.w3.org/TR/vc-data-model/#core-data-model [Accessed: 12 -July- 2022].

[44] Connect.Me. (n.d.). Evernym. [Online] Available: https://www.evernym.com/connectme/ [Accessed: 18 -July- 2022].

[45] Projekt – IDunion. (n.d.). IDunion. [Online] Available: https://idunion.org/projekt/ [Accessed: 20 -July- 2022].

[46] Lissi Wallet on the App Store, App Store, 17- Mar- 2022. [Online] Available: https://apps.apple.com/us/app/lissi-wallet/id1529848685 [Accessed: 20 -July- 2022].

[47] Davie, Matthew & Gisolfi, Dan & Hardman, Daniel & Jordan, John & O'Donnell, Darrell & Reed, Drummond, "The Trust over IP Stack". IEEE Communications Standards Magazine. 3. 46-51. 10.1109/MCOMSTD.001.1900029, 2019

[48] (n.d.). Trust Over IP - Defining a complete architecture for Internet-scale digital trust. from [Online] Available: https://www.trustoverip.org/ [Accessed: 20 -July- 2022].

[49] The Trust Over IP Foundation Publishes New Introduction and Design Principles, Trust Over IP, 24- Jan- 2022. [Online] Available: https://trustoverip.org/blog/2022/01/24/the-trust-over-ip-foundation-publishes-new-introduction-and-design-principles/ [Accessed: 20 -July- 2022].

[50] Public Key Infrastructure, 9- Jun- 2022, GeeksforGeeks. [Online] Available: https://www.geeksforgeeks.org/public-key-infrastructure/ [Accessed: 20 -July- 2022].

[51] Y. Huang, "Decentralized Public Key Infrastructure (DPKI): What is it and why does it matter? ", HackerNoon. 13- May- 2019 [online] Available : https://hackernoon.com/decentralized-public-key-infrastructure-dpki-what-is-it-and-why-does-it-matter-babee9d88579 [Accessed: 27 -July- 2022].

[52] Sovrin Governance Framework. (n.d.). Sovrin. [Online] Available: https://sovrin.org/library/sovrin-governance-framework/ [Accessed: 28 -July- 2022].

[53] M. C.Ballandies, , M. M. Dapp, , & E Pournaras, "Decrypting distributed ledger design—taxonomy, classification and blockchain community evaluation", 19- Apr- 2021. Available: https://link.springer.com/content/pdf/10.1007/s10586-021-03256-w.pdf [Accessed: 3 -Aug- 2022].

[54] C. Tankard, "*What the GDPR means for businesses*", 11- Jan- 2017. [Online] Available: http://www.sciencedirect.com/science/article/abs/pii/S1353485816300563 [Accessed:6 -Aug- 2022].

[55] Lissi eine Marke der Main Incubator GmbH. *eIDAS and the European Digital Identity Wallet: context, status quo and why it will change the*…. Lissi, 19 -Apr- 2021. [Online] Available: https://lissi-id.medium.com/eidas-and-the-european-digital-identity-wallet-context-status-quo-and-why-it-will-change-the-2a7527f863b3 [Accessed:6 - Aug- 2022].

[56] W3C. (n.d.). World Wide Web Consortium (W3C). [Online] Available: https://www.w3.org/ [Accessed: 7- Aug- 2022].

[57] DIF. (n.d.). Decentralized Identity Foundation: DIF. [Online] Available: https://identity.foundation/ [Accessed: 11- Aug- 2022].

[58]European Commission. *European Digital Identity Architecture and Reference Framework*, 19-Apr- 2021

[59] Lissi eine Marke der Main Incubator GmbH. (n.d.). *EU ID Wallet: Illustration of the eIDAS roles and functions*. Lissi. [Online] Available: https://lissi-id.medium.com/eu-id-wallet-illustration-of-the-eidas-roles-and-functions-6cb7bb6bca39 [Accessed: 7- Aug- 2022].

[60] E. R. Babbie, *The basics of social research* , 6th ed., Wadsworth, Cengage, 2014,

[61] Lecture- Mogens Rom Andersen, “MitID, Nemlog- In3 and EUDI Wallet” , 19 -April- 2022

[62] A. Lipton, and A. Treccani , *Blockchain and Distributed Ledgers: Mathematics, Technology ,and Economics,* World Scientific, 2021. Available: https://www.worldscientific.com/doi/pdf/10.1142/9789811221538_0001 [Accessed: 11- Aug- 2022].

[63] S. Shyam, "Centralized Ledgers Vs Distributed Ledgers", *medium.com,* 2017. [Online] Available: https://medium.com/@shyamshankar/centralized-ledgers-vs-distributed-ledgers-layman-understanding-52449264ae23 [Accessed: 11- Aug- 2022].

[64] D. Bhumika, "5 Types of Distributed Ledger Technology (DLT)", *anlyticsteps.com,* 08- Apr- 2022. [Online] Available: https://www.analyticssteps.com/blogs/5-types-distributed-ledger-technologies-dlt [Accessed:11- Aug- 2022].

[65] R. Delton, " Distributed Ledger Technology: An Overview of DLT System*",* *komodoplatform.com,* 15- Mar- 2020. [Online] Available: https://komodoplatform.com/en/academy/distributed-ledger-technology/#:~:text=Distributed%20ledger%20technology%20(DLT)%20is%20a%20popular%20method%20for%20securely,or%20small%20network%20to%20function [Accessed:11- Aug- 2022].

[66] F. Firouzi, K. Chakrabarty, and N.sani , eds., *Intelligent Internet of things*: *From device to fog and cloud,* Springer Nature, 2020

[67] D. Marcel, " What is a directed acyclic graph in cryptocurrency? How does DAG work ?", *cointelegraph.com,* 7- Nov- 2021 [Online] Available: https://cointelegraph.com/explained/what-is-a-directed-acyclic-graph-in-cryptocurrency-how-does-dag-work [Accessed:11- Aug- 2022]