Department of Business & Management

BACHELOR'S DEGREE IN MANAGEMENT & COMPUTER SCIENCE

Self-Sovereign Identity and the blockchain enhancing a metaverse of trust

Supervisor:

Prof.

Massimo Bernaschi

Candidate:

Edoardo D'Onghia

246961

ACADEMIC YEAR 2021/2022

Contents

Chapter 1

Abstract

We are living the years of change, where our society is about to change forever due to the upcoming Metaverse, a digital space where users can reinvent themselves with a digital identity built upon avatars and digital assets. Digital identity is key to the Metaverse and a way to protect it properly has to be found. Of the multiple issues associated with this concept, blockchain could be the best solution as it will afford users the potential to assume greater ownership rights over their data, giving them more control over the information they share with others, and enabling transparency and trust.

Chapter 2

Introduction

In October 2021 when Facebook announced the metaverse vision and changed the name to Meta something changed forever. Actually, what is *really* intended with that name is still not so clear, but some major organizations started investing in it while Meta is trying to create a VR social platform. This upcoming technology has generated lots of different opinions. Some people are skeptical whereas others see the potential of this innovation. The most reasonable question that people ask is, how in the metaverse our identity and personal information will be protected and secured? This is a crucial question. Internet is an essential part of everyday life, we depend on our electronic devices, and now we are about to make a step further, into virtual reality, and it's clear that if our social media life it's already so connected with our real one, let's imagine how much a virtual reality would be. A way to protect our digital identity is needed. This concept is strengthened by the fact that personal identifiable information is the most targeted data for breaches, comprising 97% of all breaches in recent years. Considering that we still have difficulties dealing with a 2D digital identity, even a call from your bank or a friend's email could not be what it seems, an environment like the metaverse could set the basis for even more sophisticated identity frauds. If the Metaverse will be successful depends strongly on the chance that identity protection is guaranteed and, in this thesis, we will talk about a possible great candidate to ensure privacy and identity protection while enhancing trust and discouraging malevolous users. The world is taking a big step in the future and whether or not we want to embrace this change, it's happening, and we need to exploit its potential in the best way possible, because every innovation has the power of change, it's our choice how to use it. In the next section I'm going to expose the major issues related to digital identity that need to be solved and I will propose a valuable candidate for the aim.

Chapter 3

Problems and issues

Trying to enhance digital identity protection brings along other issues strictly connected to it. It's not enough to just guarantee safety for our data, it has to be defined a system where trust between customers can be established making possible the development of interactions, and it's crucial to enhance privacy while at the same time be able to find the identity behind who commits a certain crime. In the next session, before proposing a solution I will try to give a brief description of the most important issues regarding this topic.

Digital identity

It's clear that protecting digital identity is crucial, but we need to understand what is a digital identity and what makes it a good one.

A digital identity, even if there is not an official definition, can be described as a collection of information about a person that exists online, and it has to be:

- Portable: Movable from one storage to another one, without any modification.
- Persistence: It has to be durable in time.
- Private: The access and usage to an individual's information without any consent are forbidden
- Personal: An individual has complete control and access to the composition of their own identifiers

However, all these attributes mentioned to describe what digital identity is, are textual and express different semantic meanings. To purge the semantic inconsistencies in textual definitions there is a model founded on mathematical properties, the Digital Identity Model. Without going deep into complicated mathematical formulas, simply put, according to this model, the (whole) identity of an entity is actually distributed in different partial identities which are valid within different domains (context) of different enterprises (organizations). As said, the partial identity is valid only within a domain, thus, it is important to always specify the domain. Furthermore, each partial identity is composed of a number of attributes associated with a corresponding value.

Transparency

The core of the metaverse is to heighten interactions, and in order to avoid frauds the user has to make informed decisions. The only possible way is to enhance transparency, where every interaction and transaction is entirely traceable and verifiable.

Trust

As in the real world, also in the digital world trust is of paramount importance. Even though this concept may seem a little reductive wherever there is a lack of trust there is a lack of interactions, and the world, digital or not, it's based on them. So, in the absence of trust, consumers won't feel comfortable using online tools, completely blocking the development of technology in the coming years.

Decentralization/Centralization

In order to give complete control to users and avoid that major companies could exploit personal sensible information, a complete centralized system should be excluded.
Decentralization is the process of shifting control from a centralized entity to a distributed network ensuring trust leveraging mathematics, furthermore, with respect to a centralized system is faster, cheaper, and more efficient.

Privacy

In the Merriam-Webster dictionary, privacy is described as: “The quality or state of being apart from company or observation”. In the digital world, when we talk about privacy the idea is that the aim of massive pooling of data is to enhance this right, and that without consent no one can make any use of other individuals’ personal information. In practice, however, it’s impossible to speak about consent to violations of privacy since data is processed in so many ways and for so many purposes that no one can foresee all of them.

Law enforcement

Since the metaverse is still an emerging concept there is not an appropriate regulatory framework, so if, for example, a crime is committed inside the Metaverse, what consequences should be applied? There are a lot of other interesting questions, but the trickiest one is if a crime is committed, how can you know who the guilty user is, while still maintaining privacy?

As we can see there are many different issues attached to digital identity protection, that, in order to make the metaverse possible, have to be solved in the most efficient way. In the next chapters, I’m going to present and explain why the blockchain can be a valuable solution.

Chapter 4

The blockchain

4.1 What is blockchain?

The concept of blockchain technology emerged with the publication of the paper titled: "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008 (Nakamoto, 2008). Satoshi Nakamoto is the name used by the presumed pseudonymous person or persons who developed the blockchain and the bitcoin. Nakamoto succeeded, where many others had failed, thanks to the blockchain validating system that is able to solve the double spending problem and reach the consensus. The transactions in the blockchain happen in a decentralized peer-to-peer electronic cash system where there's no need for verification by a third party. A blockchain is essentially a distributed ledger or database that is shared among the nodes of a computer network. Blockchains are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions. We refer to it as a distributed ledger because if we think about it Fiat currency exists physically, so you have tangible proof of its existence but at the same time you can't prove ownership of money. For example, if there are twenty Euros on a table in a room full of people, anyone could say that money belongs to them, and there is no way to prove to whom that banknote belongs. For cryptocurrencies, it is the exact opposite. Since they don't exist in a physical form, the only way to prove their existence is by the ledger that accounts each transaction and movement of the bitcoin. In the past, many people tried to introduce cryptocurrencies, failing, because they couldn't solve a fundamental issue, the consensus. That is why the blockchain was so a breakthrough, being able to reach the consensus thanks to the Proof of Work (PoW). The Proof of Work is the process by which each block is validated, thanks to the miners, solving the double-spending problem that consists in preventing a malicious user would spend twice the same amount of money, thanks to two key general ideas:

- (Artificially) Make it computationally costly for network users to validate transactions
- To reward them for trying to help validate transactions.

Structurally the blockchain is composed of blocks where inside each new one there is the hash of the previous block validated. When a new block is generated is broadcasted among all participants for verification, after it is validated it will be added into a growing chain of blocks.

4.2 Features of the blockchain and applicability to the Metaverse

Blockchain has become so popular and successful thanks it allowed users to make transactions in a decentralized peer-to-peer system, but what are the features that guaranteed this success?

As a good ledger it is immutable and always verifiable, this means that when a block is validated it cannot be changed and everyone can check the status of that block. Another important feature is that is distributed, gaining complete transparency and security because every participant helps maintain the ledger and participate in the validation process, discouraging malevolous users. It's fascinating how this decentralization ensures security, since malevolous users would need enormous computing power and a lot of resources to overcome the validation system, such that it would be inconvenient and extremely costly to act illicitly.

Of course, blockchain is an optimal ledger, but how can it protect our digital identity? If we take a look to the features of a "good identity" (Chapter 3, "Problems and Issues) we can see that all of them match with the features of the blockchain, as they have to be portable and always verifiable, persistence and immutable, private and immutable.

The last two features are the one trickier, it's true that privacy has to be maintained, and that is what blockchain aims to do, but if someone commits illicit acts how can we understand who's the real person responsible still ensuring privacy? This is something that still has to be generally understood also because we're in absence of a regulatory framework.

However, there exist different types of blockchain and in order to understand if this system it's optimal for the protection of digital identity we have to analyze them.

4.3 Types of Blockchain

4.3.1 Permissionless blockchain

The permissionless blockchain, called also public blockchain it's a totally decentralized peer-to-peer system where each node has the same read and write authority and a complete ledger of all the past transactions and participate in the process of mining blocks. Bitcoin's blockchain is a permissionless blockchain.

4.3.2 Permissioned blockchain

It's a system that can be considered both centralized and decentralized, depending on the role it plays. Characterized by cryptography and timestamped logs through cryptographic hash functions and blocks; but there is no decentralized network consensus and no proof-of-work (no native currency): consensus is reached in another way, a subset of nodes is the authority that controls and enforces consensus among the participants, and all the participants delegate the activity of reaching consensus to the subset of nodes.

4.4 Blockchain in the Metaverse is inevitable

For a reality like the metaverse a permissionless blockchain seems the best candidate, in this way it will be avoided that the power and all sensible information would be in the hands of only one big company. Many organizations are investing in the Metaverse that, will not be just an enormous digital space, it will be many of them all interconnected. The only tool in order to maintain these connections and making them secure is inevitably a permissionless blockchain.

How the blockchain could protect and ensure digital identity

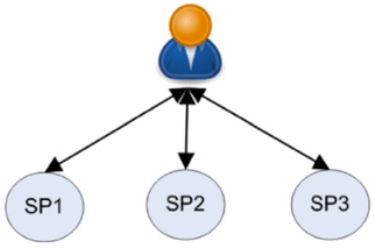
The usage of a permissionless blockchain it's crucial for the functioning of the metaverse, but there is another big pro about permissionless, sovereignty. In Nodaway's world, the platforms that we use are sovereigns, because they decide who is allowed to participate, but in a truly permissionless metaverse, there should be Self Sovereign Identity.

Chapter 5

The evolution of identity model

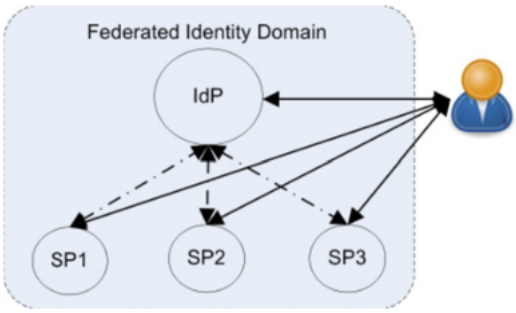
Before introducing the concept of Self Sovereign Identity is interesting to study the evolutionary path that the landscape of identity management has gone through.

Silo Model



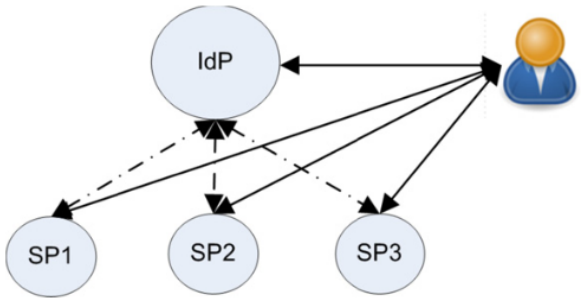
The first model to discuss is the Isolated User Identity (SILO) model which is the most common and simplest identity management model. In this model the only parties involved are two: the service provider and identity provider. The service provider provides the identifier, a username, and the corresponding credential, a password, to the users who want to access the service. However, if a user wants to access a service from a different SP, he/she needs to authenticate to each SP individually. This process results with the creation of an enormous number of specific identities that can become difficult to manage. Nowadays many online providers are trending towards new models, just to cite a few: Amazon, Yahoo, Google and eBay.

Federated Model



In a Federated model, each identity domain consists in one identity provider and one or multiple service providers. In this way the user has to authenticate himself just once to the identity provider and, when authenticated, he will be redirected to the service provider to access the service. Simply put the identity provider issues identifiers and the related credentials to the user and provides user attributes and their value to the service provider. This type of shared identity must be ensured by trust between the IdP and the corresponding SPs, by establishing a contract between them. Of course, this model results very useful in environments where identity data is shared only between trusted entities, so it's very popular in governmental services and educational institutions.

User-Centric model



The User-Centric model is very similar to the federated one, but there is no need to establish the notion of trust among the participants, so when a user wants to access a service by an SP he is redirected to the IdP in order to authenticate himself. After this process the IdP sends the identity data to the SP where the decision to grant or deny access is made. In this model there is no notion of trust, so every participant trusts each other. The model is known as the Open-trust model. Protocols like OpenID and OAuth are based on this model, which is dominant in web services provided by popular social networks like Facebook and Google

Chapter 6

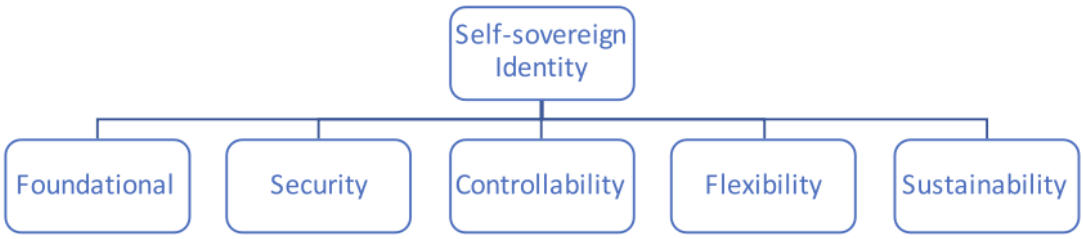
Self-Sovereign Identity

Originally, the ideological progenitor of Self Sovereign Identity was self-sovereign authority which referred to "*the actual default design parameter of Human identity, prior to the 'registration' process used to inaugurate participation in society".* This act of registration implies that identity, in order to exist, requires an administration process controlled by society, making it the 'owner' of the identity.

The concept of Self-Sovereign Identity arises with the explosion of Blockchain technology, which had a strong impact on the digital identity sector. The term was coined in 2016 by Cristopher Allen in the article "The road to Self-Sovereign Identity". In this article are explained the principles that, following Kim Cameron's Laws of Identity (2005), should guide an SSI. Surely the user must be able to control their identity and be able to access their own data. The user should be able to view, modify, hide and always have access to data of their own identity. Furthermore, in the article is stated that identities should last forever without contradicting the "right to be forgotten" while at the same time being portable, to ensure that the user's identity can be stored in multiple locations. Cristopher Allen organized the RWOT events (Rebooting Web of Trust) which were focused on creating a new identity system based on the concept of a decentralized web of trust, in 2015. Thanks to events like RWOT and IIW (Identity Internet Workshop) a basis for creating the Decentralized Identity Foundation was established (DIF, 2017). Companies such as Microsoft and initiatives like Hyperledger, among others, started participating, such that, DIF became the most relevant think tank in the field. Furthermore, in 2019 the EU, with the aim of promoting the use of blockchain technology, initiated the INATBA (International Association of Trusted Blockchain Applications).

Self-Sovereign Identity's properties

Many tried to assert the attributes that an SSI model should have, but mostly in a vague and abstract way. Even if Allen with his online article identifies several crucial properties, is completely missing the details of how to model such an identity. In the next section will be discussed the properties required by a Self Sovereign Identity, to better understand them in terms of their semantic meaning and to have a complete picture of what feature it should have.



In the taxonomy above we can see five different groups of properties that compose the SSI. For each group some properties need to be understood, which will be described in the next pages.

Foundational property:

In this group are placed all the properties that, in absence of those, self sovereign identity cannot exist. Those properties are:

- Existence : An SSI must enable a user to assert his existence in a digital domain.
- Autonomy: It must be fully autonomous in terms of management and administration.
- Ownership: The user must be the only owner of an SSI.
- Access: Unrestricted access for a user to his/her identity information.
- Single source: The user must be the single source of truth regarding his identity.

Security Property:

As the Foundational Property, also this group is crucial, because if an SSI can't ensure security there will be no point in adopt this model, since it would be useless, so it has to guarantee:

- *Protection:* An SSI should be protected properly with cryptographic mechanisms that satisfies the CIA (Confidentiality, Integrity, Authenticity) properties.
- *Availability*: Obviously it has to be accessible and available from different platforms when required by the owner.
- *Persistence:* It has to be durable in time, as long as the owner wants to.

Controllability Property:

Here there are all the properties needed in order to control identity data:

- *Choosability:* The right of the user to choose when to release an identity data and to which entity for whatever purpose.
- *Disclosure:* In order to exercise ultimate control the user must have the ability to disclose selectively particular attributes.
- *Consent:* There cannot exist some release of identity data which didn't have the user's consent.

Flexibility Property:

Since the aim of an SSI is to be interoperable within different systems, it has to satisfy some flexibility requirements:

- *Portability:* An SSI must be portable, also to ensure the persistence of identity for a longer period of time.
- *Interoperability:* As already stated, the model will need to operate in the web between different online services, so it needs to achieve the maximum level of interoperability.
- *Minimisation:* The disclosure of identity has to be minimized as much as possible.

Sustainability Property:

- *Transparency:* A user must be aware of all his partial identities and all of it's interactions, with a possible easy retrieval of such interactions in order to ensure transparency.
- *Standard:* To ensure maximum portability, interoperability and sustainability an SSI must be based on open standards.
- *Cost:* The cost to create, manage and adopt an SSI must be the lowest possible.

But why ‘self-sovereign’?

If we think about it, *self-sovereignty* is a strange terminology, the word sovereign is often used as a synonym of king or head of a state. However, today, is associated also with autonomous or independent. The definition of the word ‘sovereignty’ is: “*the quality or state of being sovereign, or of having supreme power or authority; the status, dominion, power, or authority of a sovereign; royal rank or position; royalty.”* Putting ‘self’ I front of it and already the meaning completely changes, becoming: “*a person who is neither dependent on nor subjected to any other power or state.”* However we are not dealing with just a self-sovereign, but with a self-sovereign identity, so it refers to a person’s identity that is neither dependent on nor subjected to any other person or state. But why self-sovereign identity is so important? And why can it be the solution of digital identity protection in a context like the metaverse?. First of all, SSI represents a shift in control, from the centers of the network to the edges of the network, where all the individuals interact as peers. To better understand how heavy is the need of implementing an SSI, let’s analyze the most important market drivers. These drivers fall into three major categories:

Business efficiency and customer experience: this is the primary market demand driving SSI in it’s early stages. This phenomenon is caused because corporations, governments and universities want to improve data security, cost savings, efficiency, workflows. Implementing SSI would result in a disruption of precedent modes of Identity and Access Management (IAM), but like many disruptive technologies, it will lead to new opportunities, companies and business models.

Resistance to the surveillance economy: With this expression is meant the adverse reaction to the prevailing tactics and business model of some dominant companies on the internet. Nowaday we are continuously bombed with online advertising, leading to a new industry that Harvard professor Shoshan Zuboff called ‘Surveillance capitalism’.

Sovereign individual movement: This movement originates from people who are tired of not having control over their personal data, and want to take it back. The SSI models aims to do, for decentralized identities, what bitcoin has done for decentralized money.

These three major market drivers include many other drivers in different sectors, such as E-Commerce, banking and finance and also healthcare. In the metaverse the goal that wants be achieved is to build an entire digital society, so we will find all of these mentioned drivers in there; it seems clear then, why self sovereignty is a necessary condition in order to make the metaverse possible.

Chapter 7

How does it work?

We discussed a lot of the benefits and features of the SSI model, but in practice, there's the need to understand how does SSI work and how is it built. Essentialy an SSI system is composed by seven basic building blocks, some of these concepts had been established from decades, what's interesting is how they have been put together to create this new emerging model. So let's analyze these seven building blocks:

Verifiable credentials

The term credential obviously refers to your ID, the object that proves your identity. However, the term 'credential' extends to any set of information that some authority claims to be true about the subject of the credential (ex. Passport, Diploma, Birth certificate). These examples anyway refer to a human subject, while verifiable credentials are not limited to humans, for example, issuing a vaccination for a pet can be a VC, because, simply put, every credential contains a set of claims about the subject of the credential. In order to verify the credential the claims have to be verifiable. In the digital world the verification process happen using cryptography and the Internet, in a few milliseconds. A verifiable credential is structured in four parts:

- The unique identifier for the credential
- The metadata describing the credential itself: for example an expiration date for a certain certificate
- The claims contained in the credential (name, date of birth, sex)
- The digital signature created using cryptography

Issuers, holders, and verifiers

The relation between this three figures is often referred as the trust triangle, because it is how human trust relationship are made in the digital world. The issuer is the source of the credential, so every credential has an issuer. The holders instead request VCs from issuers, and hold them in their digital wallets. Also, holders, when requested by the verifier present proof of claims from one or more credentials. Verifiers can be anyone who is seeking trust assurance about the subject of credentials, so they request proof from the holders. The critical part of this process is the verification of the digital signature, that can be resolved thanks to the DIDs.

Decentralized identifiers (DIDs)

For the past decades the technology able to create digital proof was public/private key cryptography. This model implies that the owner of the private key uses it to sign a message, and the only way to verify his signature is with the owner's public key. So for decentralized messaging, the problem was to find a solution to prove ownership of the public key. During these years as a solution to this issue the PKI model (public key infrastructure) was used. However, it is too centralized and way too expensive to meet the world demands. A new type of identifier was needed, that had to match four properties: permanent, resolvable (identifier able to retrieve public key as well as address/es), cryptographically verifiable and decentralized. DIDs are the result of these requiriments, and, as any two devices with their own IP addresses can use a TCP/IP protocol to exchange data, any two identity owners with DIDs can use an SSI protocol in order to cryptographically exchange data. In addition to this, DID-to-DID connections lead to five more properties: Permanent, private, End-to-end (no intermediaries) and extensible.

Blockchain as a data registry

Decentralized identifiers can be registered on any type of decentralized network, but why blockchain would be the most suitable? In a standard industry use of the term, a blockchain is a highly tamper-resistant transactional distributed database that no single party controls. Providing in this way an authoritative source of data, that all the peers participating can trust without any peer being in control.

The other three building blocks that contribute to the functioning of SSI technology are the digital wallets, digital agents and the governance framework. Those are still important parts but they aren't the core of this thesis, so there's not the need to study them in deep.

How blockchains can be useful for SSI in practice

Bitcoin and Ethereum are nowadays already considered "grand daddies" of the blockchain because collectively, their market value is more than four times greater than all other cryptocurrencies combined. It shouldn't be a surprise then if some of the first SSI implementations, like Learning Machine (Bitcoin) and uPort (Ethereum), targeted these blockchains. All these methods use the cryptographic address of a transaction on the ledger (a payment address) as the DID. All DIDs methods rely on a root of trust, but most of them are not self-certifying, so they require a second step: using the private key to digitally sign a transaction in a distributed ledger to record the DID and the initial associated public key.

However, payment addresses can limit interactions to a "don't call us, we'll call you" model, because they don't provide a clear way to contact the address holder, furthermore, they don't have rich metadata.

Since 2016, developers started creating the first blockchains designed specifically to support SSI, an interesting application is the Hyperledger Indy, which, In addition to DIDs, supports also the zero-knowledge proof credential format (ZKP). The ZKP format is a fundamental tool since, in early experiments in blockchain-based identity there was the notion of putting an individual's credential directly on the blockchain as encrypted data objects, but this is a bad idea. The main reason for this is that all encryption has a

limited lifespan, so writing it on an immutable public ledger could lead to the risk of being eventually cracked. ZKP represents an efficient solution because you only need to store new “proof information” on-chain, while the rest of the data can be securely stored off-chain. The goal of this tool is to reveal only the part of the message that was disclosed and that the prover knew the signature. A ZKP needs these three main properties:

- Completeness: ““If the statement is really true and both users follow the rules properly, then the verifier would be convinced without any artificial help.”
- Soundness: “In case of the statement being false, the verifier would not be convinced in any scenario.” (The method is probabilistically checked to ensure that the probability of falsehood is equal to zero.)
- Zero-knowledge: “The verifier in every case would not know any more information.”

So ZKP is able to prove information of an individual’s credential without having to fully disclose other sensitive personal information, reducing identity theft and frauds.

Chapter 8

Self-Sovereign Identity and the blockchain enhancing a metaverse of trust

In October 2021 when Facebook announced the metaverse vision and changed the name to Meta something changed forever. The metaverse is a reality that is happening right now, we still don't know how it will evolve and what the final result would be, as we didn't know for the internet. When internet started to become popular no one could possibly imagine what it would become: social networks, cryptocurrencies, online advertising and profiling. For the ones who were born later it seems normal, and maybe for the next generations hanging out with some friends in the metaverse will be a daily activity, the thing is that is happening. Even if there are risks, the benefits that we could get from an innovation like this would be countless, and as we analyzed, there are a lot of market drivers pushing towards this direction. Furthermore, identity means value, because, day by day, cryptocurrencies are becoming more used and accepted, and since the value of a currency ultimately depends on the trust that people have in that particular store of value or medium of exchange, the connection between SSI as a model for decentralized digital trust infrastructure and cryptocurrencies as decentralized, permissionless monetary systems starts to become obvious. Adopting an SSI model seems a natural and necessary progression into the future, and as we analyzed, blockchain is the ultimate candidate to support it. Let's dive into this new metaverse of trust being sovereigns of our identity.

Chapter 9

References

Alex Preukschat and Drummond Reed, (2021). Self-Sovereign Identity.

Alexandra Giannapoulou – University of Amsterdam, Fennie Wang – Dionysus Labs, (2021). Self Sovereign Identity.

MD Sadek Ferdous, Farida Chowdhury, and Madini O.Alassafi, (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology.

Rachel Wolfson, (2022). Reinventing yourself in the Metaverse through digital identity. Retrieved from: https://cointelegraph.com/news/reinventing-yourself-in-the-metaverse-through-digital-identity

David Lucatch, (2021). Digital Identity In The Metaverse. Retrieved from: https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/28/digital-identity-in-the-metaverse/?sh=2b02f8de1fb6

Shade Oladetimi, Pillsbury - Internet & Social Media Law Blog, (2022). Protecting Your Digital Identity in the Metaverse. Retrieved from: https://www.jdsupra.com/legalnews/protecting-your-digital-identity-in-the-6040663/

Alex Dzyuba, Lucid Reality Labs Founder & CEO | Anna Rohi, Lucid Reality Labs Senior Marketing & Communications Manager, (2022). 7 Challenges of The Metaverse. Retrieved from: https://lucidrealitylabs.com/blog/7-challenges-of-the-metaverse

Bernard Marr, (2022). 7 Important Problems & Disadvantages Of The Metaverse. Retrieved from: https://bernardmarr.com/7-important-problems-disadvantages-of-the-metaverse/

Consensys, (2021). Blockchain in digital identity. Retrieved from: https://consensys.net/blockchain-use-cases/digital-identity/