Motivation, Architecture and Business Viability

of Self-Sovereign Identity Framework for a Blockchain Network

freeton.id
2021

Motivation, Architecture and Business Viability

of Self-Sovereign Identity Framework for a Blockchain Network

Authors:

Alexey Vorobey
Alexander Alekseenko
Leila Jalbot
Arthur Pinchuk

Contributors:

Vladimir Kanin
Nikita Lobushkin
Anton Kirilyuk
Alena Pinchuk

2021

Contact us:
E-mail info@freeton.id
Telegram: @JasonBrn2020

Contents

Glossary[1]

Decentralized identifier (DID) is a portable URL-based identifier (string), also known as a DID, associated with a person, organization, or device that performs one or more roles in the VC ecosystem. These identifiers are most often used in a verifiable credential and are associated with subjects.

A DID document is a document that is accessible using a verifiable data registry and contains information related to a specific decentralized identifier.

Verifiable credential (VC) is a tamper-evident digital set of claims that has authorship that can be cryptographically verified. The claims in a credential can be about different subjects.

Verifiable presentation (VP) is a set of data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier. Like a single verifiable credential, this set of data is encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Contains either original VCs or data synthesized from (see ZKP)

Issuer is an entity that asserts claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.

Subject is a person, organization or thing about which claims are made.

Holder is a role an entity might perform by possessing one or more verifiable credentials and generating presentations from them. A holder is also usually, but not always, a subject of the verifiable credentials they are holding.

Verifier is a role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing.

Selective disclosure is the ability of a holder to make fine-grained decisions about what information to share.

Derived predicate is a verifiable, boolean assertion about the value of another attribute in a verifiable credential.

URI is a globally unique string of specific format (defined in RFC3986].

[1] Sporny, M., Chadwick, D. and Longley, D., 2019. Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web. W3C.org.

Part 1

Current State of Digital Identity

The Internet as the basis for a concept of digital identity

It seems not too long ago that the phenomena of the World Wide Web have hit the globe. In 1965, two computers at MIT Lincoln Lab communicated with one another using packet-switching technology.[2] Since 1965, there has not been a year that would not be marked with another tech innovation in the telecom sphere. Humanity saw the rise of ARPANET, the connection of the National Science Foundation NSFNET to a supercomputer center at 56,000 bits per second. In 1991, CERN introduced the World Wide Web to the public. In 1993 there were more than 2 million computers connected to NSFNET.[3] It was later followed by the creation of Yahoo!, Amazon.com, eBay, and eventually the Internet transformed into the most remarkable social phenomenon of the 21st century.[4]

The digital payment market, which includes all consumer transactions made over the Internet and on mobile devices, has been on the rise for over a decade, starting from the launch of Amazon in 1995. Although digital wallets have been around for over 20 years, they have just recently matured, altering the way we search for and pay for products and services. Now, the user experience is enhanced by digital mobile applications that store bank details in a single location and permit users to make offline and online purchases with their phones. They may also be used to store IDs, digital rewards, tickets, and other documents eliminating the need to carry wallets everywhere.[5]

What followed in the next couple of years? The debut of Skype, Safari Web browser, WordPress, Facebook, and Mozilla Firefox, YouTube, and Twitter. Community has also witnessed the birth of Google. However, the multiplicity of Internet-based services could not solve the most significant problem. Personal profiles did not impose the realness of the users behind the screen at first, but as the baby, Facebook grew to become the most prominent social network, the issue of real identity had become central to their policy and concept. Now, behind screens, there are individuals, who if to be trusted had to be identified. Before such rapid development of technologies, a transition of key offline services to online mode of operation has led to millions of user interactions every day, the Internet was anonymous.

[2] Ryan,J., 2010. A History of the Internet and the Digital Future. London: Reaktion Books. 10-11.

[3] Leiner, B and C, Vinton and Clark, David & Kahn, Robert & Kleinrock, L. & Lynch, Daniel & Postel, Jonathan & Roberts, Lawrence & Wolff, Stephen. (2009). A Brief History of the Internet. Computer Communication Review. 39. 22-31. 10.1145/1629607.1629613.

[4] National Science and Media Museum. 2021. A short history of the internet | National Science and Media Museum.

[5] Rofle, A., 2020. The inevitable rise and rise of the global digital wallet. Payments Cards & Mobile.Available

There was no identity on the Internet

identity

“On the Internet, no one knows you are a dog”[6] — the most famous online proverb used to describe the anonymity feature of the Internet was born before Facebook and Google became the dolmens of the web. Anonymous posting/reply services on the Internet first appeared in 1988 and were designed specifically for newsgroups that addressed highly explosive, sensitive, and personal topics. Global anonymity servers sprung up quickly, merging the functionalities of anonymous posting and anonymous remailing into a single service. Pseudonymous email services were also implemented as part of the new worldwide services, allowing anonymous communications to be responded to.

The old web, a place where one’s identity could be kept distinct from their everyday lives, has vanished from the computer screen.[7] The majority of social media models and the current Internet landscape significantly impact how we interact with one another and our identity. Why? The answer is simple. In an environment with billions of people and multiple billions of devices on the Internet, almost all of whom are strangers. The truth is that many people want to deceive you about who they are and what you are dealing with over the Internet. Identity or the lack of it is one of the primary sources of cybercrime.[8]

Online anonymity is often difficult to defend because the absence of attribution and accountability for one’s actions can encourage immoral, repulsive, and criminal activity.[9] To respond to this anonymity trend, the global community attempts to eliminate users’ privacy.[10] By stepping on privacy, those regulators may create greater risks. On the scales, on the one hand, is the security of the user when conducting online transactions, on the other hand, the efficacy of states while performing their mandate and the success of tech-giants that provide customer-oriented services. This is why it is of utmost importance to maintain the balance with control over personal data protection and the interests of cybersecurity and global data mining stakeholders.

[6] Fleishman, G., 2000. Cartoon Captures Spirit of the Internet (Published 2000). Nytimes.com

[7] Krotoski, A., 2012. Online identity: is authenticity or anonymity more important?. the Guardian

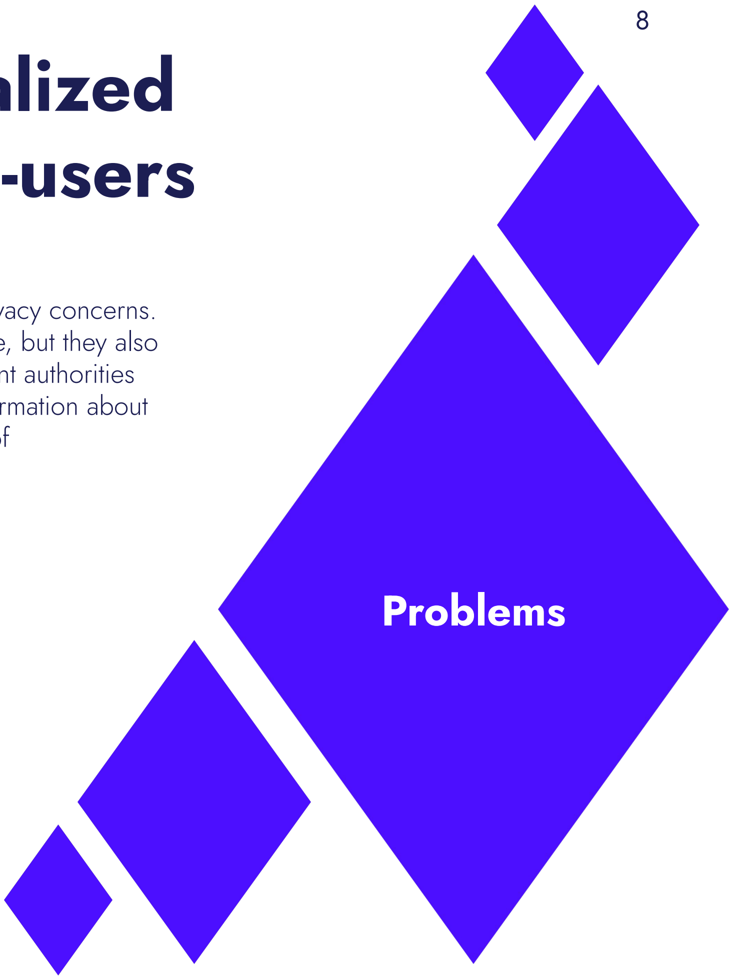
[8] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p. 14

[9] Bodle, R., 2013. THE ETHICS OF ONLINE ANONYMITY OR ZUCKERBERG VS. “MOOT”. 1st ed. [e-journal] Computers and Society, pp.Volume 43, Number 1

[10] Mirani, L., 2014. How Facebook and Google are taking over your online identity Quartz

Problems of the centralized identity model for end-users

The increasing centralization of Internet platforms raises serious privacy concerns. These linking network sites not only serve as a single point of failure, but they also serve as a rich supply of data that hackers may exploit.[11] Government authorities can also pressure centralized online operators to reveal crucial information about their user base. Depending on the architecture in use, the privacy of communications might be threatened in a variety of ways.



Loss of data control

In most centralized systems, users do not need to worry about securing their own communication channels because they are maintained by a centralized operator. Instead, they must progressively commit personal data to these operators, hoping that they would only use it for lawful purposes.[12] Nonetheless, given that all user communications are routed via these centralized operators, surveillance is nearly always a significant danger to privacy.

Centralized coordination comes at the cost of entrusting a centralized authority with the duty of administering the network in accordance with its user interests.[13] The vast majority of today's Internet platforms are built with centralized regulation and control in mind. The fact that centralized operators often rely on technological and contractual mechanisms to govern how users may (or may not) engage with their platforms makes regulation easier.

Centralized administrators may be able to intervene and penalize users who do not follow the sites' rules, To the extent that they maintain track of all online actions taking place on these platforms.[14] Nevertheless, handing control of digital identity to centralized authorities in the online world causes the same difficulties as handing control of physical identity to state authorities: users are tied in to a single authority who may refuse their identification or even affirm a fraudulent identity. Centralization inherently confers power on the centralized entities rather than the consumers.[15]

[11] de Filippi, P., 2016. The interplay between decentralization and privacy: the case of blockchain technologies. Journal of Peer Production, Alternative Internets

[12] W. Bilder, G., 2006. In Google We Trust?. The journal of electronic publishing, 9(1)

[13] Duffany, J. L. 2012. In: 10th Latin American and Caribbean Conference for Engineering and Technology.Cloud Computing Security and Privacy. Panama: Universidad Tecnológica de Panamá, pp.1-9.

[14] de Filippi, P., 2016. The interplay between decentralization and privacy: the case of blockchain technologies. Journal of Peer Production

[15] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

Identity theft

The 2021 Identity Fraud Study, published by Javelin Strategy and Research, uncovers a frightening new danger to consumers and businesses: identity fraud schemes. While overall combined fraud losses in 2020 reached a total of $56 billion, identity fraud scams accounted for $43 billion of that total. While most people are aware of data breaches in corporations, few are aware that identity theft occurs every two seconds and is the most common consumer complaint.[16]

It is estimated that the average Internet user has about 70 online identities. Most legacy systems do not even have technical capabilities to provably delete users' data.[17] Each one of those services stores the user's password and personal information in centralized databases. If they are hacked, you as a user won't even know if your personal data is stolen.

Middleman as a standardization problem

The role of a middleman is a problem that arises from the employment of centralized models. Numerous social networks perform the role of "man in the middle," where they can monitor a user's login behavior across multiple sites.[18] Hence, creating a system that securely orchestrates peer-to-peer interactions is a major goal for specific technology industries.

The increasing number of middlemen in the network fosters the development of various data standards. The competition of these standards becomes a battlefield where the customers usually lose. To scale and automate existing trust systems even further, we need a shared standard that is native to both humans and machines. As more and more document issuance and verification is happening through software, the need for machine-readable universally standardized data formats is growing. Existing digital document types like PDF or paper document scan is tough to navigate for software and can produce high levels of errors. The good news is that verifiable credentials are a natively digital semantic and cryptographically secured format.

[16] Javelin. 2021. 2021 Identity Fraud Study: Shifting Angles.

[17] Gershuni, S., 2021. Bullish Case for Self-Sovereign Identity. Medium

[18] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p.10

Problems of the centralized identity model for state authorities

Over the past decade, the global community has been periodically shaken by scandalous data leaks from major government platforms. For example, in March 2021, the voter registration and personal details of millions of Israeli citizens were leaked online, exposed information included the voter registration details of 6,528,565 Israelis and the personal details of 3,179,313 of Israel's estimated 9.3 million total population.[19] Notorious case of the Adhaar,[20] the largest state digital ID project is another sad example of data leakage. The government of India gathered biometric and demographic information on over 1.1 billion people in order to provide each person a unique 12-digit identity code known as a "Aadhaar" number. Despite the government's assurances of data protection measures such as 13-foot high walls, endless stories of leaks have prompted concerns about the security of the massive database, which is used for everything from opening a bank account to registering for a driver's license. Another, probably the largest data leak scandal of 2018[21] was caused by Facebook. Cambridge Analytica was found to have acquired the personal data of millions of Facebook users without their permission and utilized it for political advertising purposes.

These examples show how vulnerable centralized identity models are; despite their many advantages, scenarios like the ones described above show how little control individuals have over their own personal data and identity, and these aren't the only difficulties. The key drawbacks of centralized identification schemes include security problems and bureaucracy.

[19] Bar-Zik, R., 2021. Day before election, entirety of Israel's voter data leaked online — again. haaretz.com.

[20] Venkataramakrishnan, R., 2018. Scroll Explainer: What is the Aadhaar case and what is at stake for Indians? Scroll.in.

[21] Perez, S. and Whittaker, Z., 2018. Everything you need to know about Facebook's data breach affecting 50M users. Techcrunch.com

Security problems

State authorities are the primary providers of identification for people: they issue physical identity documents like passports, ID cards, birth certificates, and so on. Physical passports have the disadvantages of extensive information disclosure (for example, prior entry stamps or visas are accessible to any scrutiny) and high value for criminals, as well as being relatively easy to get.

In both street and online identity theft, the combination of a phony driver's license photograph and a real person's driver's license data (name, address, and birthdate) is effective. The destination service cannot validate the document against the issuing source in street identity use cases; hence it falls victim to the actual data, false photo document.[22] Fundamentally, centralized identity systems store sensitive personal data, resulting in honeypots of valuable information likely to be targeted in data breaches.[23]

Centralized identity models mostly operate on public key infrastructure.[24] Single points of failure and control that exist in traditional identity schemes based on PKIs and/or large-scale, international, platform-based identity providers and brokers are a major threat to privacy.[25] Reliance on centralized PKI makes it almost impossible to create complete automatization, as humans are involved.

Bureaucracy

Digital government, also known as electronic government (e-government), should make it easier to manage bureaucracy, improve the efficiency of governmental services, and save money. It should also make the government more transparent by giving individuals more access to government data and enabling more insight into and control over the state's operations.[26]

Government-issued digital identification documents are frequently electronic IDs, which are either "smart" documents/chipcards with cryptographic and electronic equipment. The applications of government-issued electronic IDs differ from country to nation, but they all serve to identify citizens in exchange for access to government services. These services could include signing documents with digital signatures, making payments (like in Estonia), and even giving the user the ability to vote.

However, even with those described facilities of the modern digital world, electronic interactions with authorities are still imperfect, especially because centralized identity models are still the core of those interactions. Centralized identity is tied to centralized PKI. That, in particular, means that the issuance of a digital signature is not a final step in authorizing somebody to act. Changes in some constitutional attributes, like company address or phone number, may cause the need to reapply for its issuance. The same is true with digital certificates. All this bureaucratic inconvenience increases the authorities' workload, at the same time creating difficulties for end users.

[22] Boysen, A., 2021. Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. Frontiers

[23] Securekey.com. 2021. A Primer and Action Guide to Decentralized Identity.

[24] Kuperberg(B), M., Kemper, S. and Durak, C., 2021. Blockchain Usage for Government-Issued Electronic IDs: A Survey. Dbsystel.de

[25] Boysen, A., 2021. Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. Frontiers

[26] Savage, N., 2018. Making digital government a better government. Nature.com

The evolution of decentralized information systems

Given the aforementioned flaws in the centralized identity paradigm, it's no surprise that the decentralized identity system is gaining popularity among developers and scientists. By definition, centralized identity systems are siloed. Organizations are incorporating federated identity models into their identity systems and researching decentralized identities in response to a growing dilemma of identity fragmentation.[27] This distributed, self-sovereign identification model, which provides both empowerment for individuals and risk mitigation for the company gathering this data, is part of the future of identity management.

The existence of decentralized systems, which do not require a central mediator to function, dates back to the development of the Web. Concepts of local systems were only ideas as long as computing was done in the data hall as a "closed shop." When minicomputers and microcomputers became affordable towards the end of the 1970s, the landscape shifted. Simultaneously, new methodologies and tools for developing tiny systems were developed (prototyping, experimental design). This movement might be interpreted as a protest against centralized systems (or at least as a way to fulfill local demands that centralized systems could not support).[28] The Internet, in particular, was gaining momentum as a vast decentralized network. Although multiple mail servers would directly exchange messages with each other, email was even more decentralized than the old postal mail service it mirrored. Time worn protocols like Network News Transfer Protocol (NNTP) enabled the decentralized exchange of news articles.

In essence, decentralization was not a radically new concept but rather the attitude of the period. Conversely, Sir Tim Berners-Lee created basic yet powerful standards for identifying, connecting, and presenting multimedia material online three decades ago. He set it free to develop and grow. However, the World Wide Web has changed drastically from what the inventor-imagined web would be —

“An open platform that would allow everyone, everywhere to share information, access opportunities and collaborate across geographic and cultural boundaries.”

Despite the fact that it has lived up to his vision, he identified serious issues with the Web's current status.[29] He feels that cyber behemoths like Google and Facebook wield far too much power and personal data — instead of referring to the firms by name, Mr. Lee prefers to refer to them as “silos”. The author claims that they have evolved into surveillance platforms and gatekeepers of innovation, fueled by massive volumes of data.[30] One of the solutions to this problem is the decentralization of the web and restoring the control over personal data to the users. Computer scientists and engineers must bear the technological burden of demonstrating that decentralized personal data networks can scale globally and offer a better user experience than centralized platforms.[31] What does the technological burden of proof rest upon?

[27] Rowe, G., Nikols, N. and Simmons, D., 2018. The Future of Identity Management (2018-2023). Techvisionresearch.com.

[28] Hugoson, MÅ., 2009.Centralized versus Decentralized Information Systems. In: Impagliazzo J., Järvi T., Paju P. (eds) History of Nordic Computing 2. HiNC 2007. IFIP Advances in Information and Communication Technology, vol 303. Springer, Berlin, Heidelberg.

[29] World Wide Web Foundation. 2017. Three challenges for the web, according to its inventor. webfoundation.org

[30] Lohr, S., 2021. He Created the Web. Now He's Out to Remake the Digital World.. Nytimes.com

[31] Verborgh, R., 2021. Power to the people: Re-decentralizing the Web, for good this time. SocietyByte

Little did humanity know about the consequences of the white paper that appeared online shortly after the domain name bitcoin.org was registered in early 2008. A mystery lies behind the genius invention by an unknown person or group of people using the name Satoshi Nakamoto, who proposed a new cryptocurrency known as Bitcoin. Bitcoin is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.[32] This invention spawned an entirely new concept and a paradigm shift in how we think about online identity and trust. The critical innovation introduced by this technology is that the network is open. Users do not need to know or trust each other to interact: electronic transactions can be automatically validated and recorded by network nodes using cryptographic methods, with no human interaction, central authority, point of control, or a third party (e.g., governments, banks, or other organizations).[33] The justification for this protocol is a decentralized trust or trust-by-computation, and its significance cannot be overstated: it symbolizes "a change from trusting humans to trusting math,"[34] with applications far beyond the development of decentralized digital currencies.[35]

Bitcoin is an excellent instrument for online value transfer, but its most valuable invention is its underlying technology, the blockchain, which enabled decentralized consensus for the first time in history.[36] The potential usefulness of blockchain technology extends beyond cryptocurrencies (which are merely applications built on top of that technology) to a wide range of other applications such as smart contracts, provenance and attribution, distributed information validation, and more.[37] Furthermore, many people consider blockchain technology as a possible game-changer that might lead to the decentralization of the web and the storage of personal data, as well as alleviate problems with the Internet's missing identity.[38]

Blockchain technology can become a game-changer in the field of identification and personal data control. This result may be achieved due to the trustworthiness of a decentralized environment in which immutability will be maintained by economic or organizational consensus. The concept of identity consists of several legal facts that can be fixated and stored in this trustless system. The influence of the blockchain ecosystem in the field of decentralized identity models will be described in detail in Part 4.

[32] Nakamoto, S., 2009. Bitcoin Whitepaper — Satoshi Nakamoto. Satoshinakamoto.me.

[33] Atzori, M., 2017. Blockchain technology and decentralized governance: Is the state still necessary?. Journal of Governance and Regulation, 6(1), pp.45-62.

[34] Antonopoulos, A., 2014. Bitcoin Security Model: Trust by Computation. O'Reilly-Radar. radar.oreilly.com

[35] Atzori, M., 2017. Blockchain technology and decentralized governance: Is the state still necessary?. Journal of Governance and Regulation, 6(1), pp.45-62.

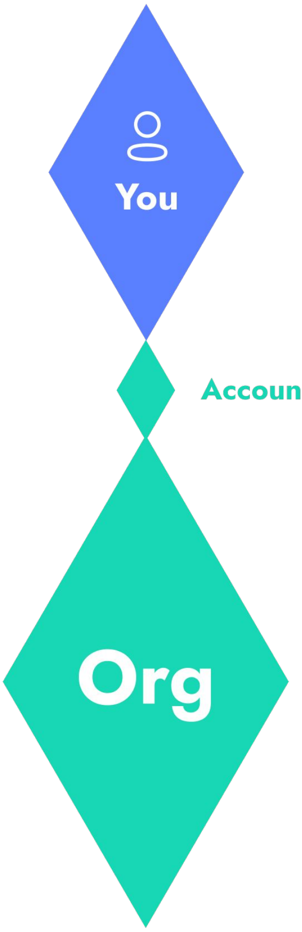
[36] Raval, S., 2021. Decentralized Applications. O'Reilly Online Learning.

[37] SBIR, 2016. Applicability of Blockchain Technology to Privacy Respecting Identity Management. sbir.gov

[38] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p.6

Types of digital identity in the Internet

Where does the concept of digital identity stand in this evolution of data storage systems? How various models apply, and what is the best to rely on? Timothy Ruff describes the evolution of the Internet identity in three models:
1) the centralized identity model;
2) the federated identity model;
3) the decentralized identity model.



Centralized identity model

In the early days of the Internet, centralized authorities were the issuers and authenticators of digital identities. IANA (1988) determined the authenticity of IP addresses, whereas ICANN (1998) arbitrated domain names.[40] In 1995, certificate authorities stepped in to assist Internet commerce sites in proving they were who they claimed to be.[41]

Users have long used the approach for practically all IDs and credentials, including government ID numbers, passports, identification cards, driver's licenses, invoices, Facebook logins, LinkedIn profiles, and so on. Central governments or service providers such as banks or telecommunications corporations grant all of these.[42] Users establish identity by registering an account (typically a username and password) with a website, service, or application. The simplest of the three models sometimes referred to as conventional, "siloed" identity: An organization provides you with (or allows you to develop) a digital credential that allows you to access its services.[43]

User's ability to access services will be terminated if they remove all of their accounts at these centralized providers. The user will be fully removed from the Internet, but all of their personal information will remain in possession of the organization, which they will have no influence over. That is only one of the many problems with centralized identity. Another issue is the difficulty of remembering and managing all of the accounts and passwords. Every website has its own set of security and privacy policies, and they are all distinct (a classic example is the wildly disparate password restrictions: minimum length, alphanumeric characters). On top of the above, these centralized databases of personal information are massive lures that have resulted in some of history's most serious data breaches.[44]

[40] Icann.org. 2020. What Does ICANN Do? – ICANN

[41] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

[42] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p.6

[43] Ruff, T., 2018. The Three Models of Digital Identity Relationships. Medium

[44] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p.7

Federated identity model

Within a federation, each organization is referred to as a relying party. Since 2005, three generations of federated identification protocols have been developed: Security Assertion Markup Language (SAML), OAuth, and OpenID Connect, with varying degrees of success. Single sign-on (SSO) is now a regular feature of most corporate intranets and extranets that use these protocols. Federated identity management (FIM) began to gain traction on the consumer Internet, where it was dubbed user-centric identity. Social login buttons from Facebook, Google, Twitter, LinkedIn, and other providers are now a typical feature on many consumer-facing websites, thanks to protocols such as OpenID Connect.[45] However, when people utilize "social log in," or the ability to sign in to a website using credentials from the big identity providers, millions of Internet users knowingly allow Facebook, Google, and others access to their online and mobile movements. Identity providers (IDPs) are unable to assist users in safely sharing some of their most valuable personal data, such as passports, government identifiers, health data, financial data, and so on, due to security and privacy constraints.[46] Preukschat and Reed identify the following problems associated with the use of IDPs:

1. There is still no single identity layer at this time. Users must utilize several IDPs and will eventually face the password nightmare that comes with a centralized identity. Users have to use multiple IDPs and sooner or later come to password hell typical for centralized identity.

2. IDPs provide "lowest common denominator" privacy policies in order to be compliant with all the services they serve.

3. Large IDPs become single failure spots, prone to crashes and attacks. For instance, in December 2020, Google experienced a global outage and was serving 5xx errors on virtually all authenticated traffic. As a result, all the services which require Google account authentication were unavailable for a duration of 50 minutes.[47]

4. IDP accounts are just like centralized identity accounts in terms of portability. All of your account logins are lost if you quit an IDP like Google, Facebook, or Twitter.) In addition, if you are banned by Google, you will lose access to third-party services as well.[48]

You
Account
IDP
Org

[45] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p.8

[46] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p.8

[47] Status.cloud.google.com. 2021. Google Cloud Status Dashboard.

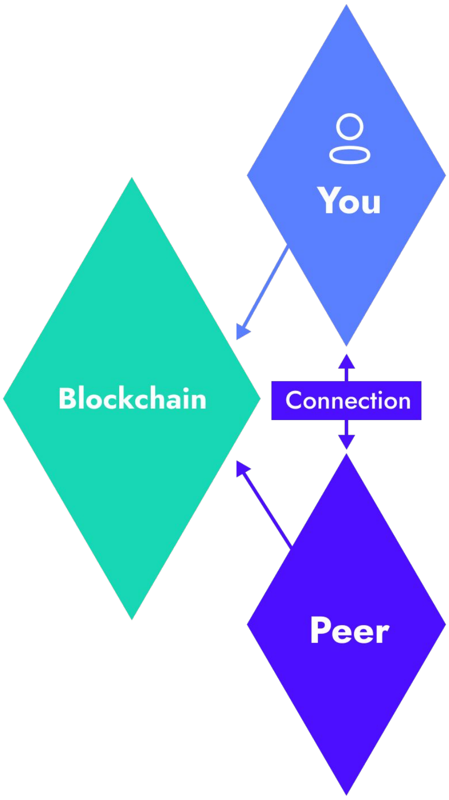
[48] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p.7

Decentralized identity model

In his blog, Christopher Allen offers another model he calls User-centric Identity, in which individual or administrative power is distributed among various authorities without the need for a federation. In its proposal to construct a next-generation Internet, the Augmented Social Network (2000) established the framework for a new type of digital identity. The distinction is that we achieve this with digital wallets, digital credentials, and digital relationships with decentralized digital identities. Their most significant breakthrough was "the idea that every individual should have the freedom to govern his or her own online identity".[49]

In 2013, a new model influenced by blockchain technology initially appeared. The FIDO Alliance was founded. It employs a hybrid model in which connections are peer-to-peer, but key management is handled centrally by the FIDO Alliance rather than through a decentralized system like blockchain. This concept was essentially decentralized and did not rely on either centralized or federated identity suppliers. It proliferated, absorbing new breakthroughs in encryption, distributed databases, and decentralized networks. It gave rise to new decentralized identification standards, including verifiable credentials and decentralized identifiers. The most significant distinction in this paradigm is that it is no longer dependent on accounts. Instead, it functions similarly to identity in the actual world in that it is founded on direct interaction between you and another party as peers. If you "provides," neither "controls," nor "owns" the other's connection. This is true regardless of whether the other party is a person, an organization, or a thing.[50] Neither of you has an "account" with the other in a peer-to-peer connection. Rather, you two share a bond. This relationship is not totally "owned" by either of you.

It's like you're both clutching a string, and if either of you lets go, the string will fall. But the relationship will last as long as you both desire it. This means that, ironically, the greatest general parallel for the decentralized identity paradigm is, in reality, it is exactly how we confirm our identity in the actual world every day: by taking our wallets out and displaying the credentials we acquired from other trustworthy sources.[51]



[49] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

[50] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p.9

[51] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 9

The preconditions for the evolution of the decentralized identity model

All major IT giants and manufacturers used to lock in users to their services,[52] e.g., Apple Inc.[53] In addition to this, until recently, it was simply impossible to ensure data portability across the apps. Partially, the problem of data portability stems from the particular features of centralized data storage.

Data storage models have evolved due to the expensive cost of the first computers and the increased need to store data. A centralized style of data storage was traditional and widely employed. In a centralized system, a single center directly supervises the functioning of separate components as well as the flow of information. Individual entities, such as municipal governments, are directly controlled by the central power in this system.

The capacity to move data between multiple applications, programs, computing environments, or cloud services based on a centralized data model is known as data portability.[54] Data portability has become standard among applications built for use on numerous vendors' personal computers and servers. Consumers may effortlessly coordinate their personal data across numerous social networking sites because of data portability. Users can share their connections, postings, images, videos, sound snippets, and personal or professional information across several platforms on social networking sites such as Facebook, LinkedIn, and Twitter.

Unfortunately, this principle is rarely abided in the field of personal account management. Vendor lock-in, unavailable data, and even data quality challenges can all come from a silted approach to data. There is no universally recognized right to data portability.[55] Hence, regular users are locked in their major services. That fact hinders the competition on the digital market and decreases the commonwealth. Switching costs can provide businesses more market power by locking in customers and lowering residual demand elasticity, which could lead to price rises in the future. Consumer lock-in can also act as a barrier to competitors' business expansion, which can help incumbent corporations to maintain their dominant market position.

The absence of data portability among various private and state-owned services leads to the lack of trust among counterparties. Independent agents tend to eliminate these hardships by creating authorized intermediaries or by using trustworthy mediums of communication in the form of paper documents. All those trust maintainers are the key reason for enormous transactional costs. When we use the Internet as a communication medium, we connect with known and unknown persons via email, social media, instant messaging, and online video conferencing. Because trust is a crucial component of meaningful social interaction, it is regularly identified as a possible obstacle to effective online communication.[56] A typical fundamental definition of trust considers it a two-way transaction between two parties:[57] if A thinks that B will behave in A's best interests and accepts vulnerability to B's actions, then A trusts B.[58] Before the Internet came along and shattered the paper paradigm, physical mediums of communication were in charge.

[52] Williams, M., 2007. Cross-border issues fracture iTunes offerings in Europe. networkworld.com

[53] News.bbc.co.uk. 2021. BBC NEWS | Technology | Itunes user sues Apple over iPod.

[54] Mullins, C., 2021. What is data portability? The right to data portability explained. SearchCloudComputing

[55] Mullins, C., 2021. What is data portability? The right to data portability explained. SearchCloudComputing

[56] Naquin, C. and Paulson, G., 2003. Online bargaining and interpersonal trust. Journal of Applied Psychology, 88(1), pp.113-120.

[57] Jacovi, A., Marasovic, A., Miller, T. and Goldberg, Y., 2021. Formalizing Trust in Artificial Intelligence | Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. Dl.acm.org

[58] Mayer, R., Davis, J. and Schoorman, F., 1995. An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), p.709.

The "Statute of Frauds," issued by England in 1677, demanded that some agreements be written down and signed.[59] The new law acted as a catalyst for the widespread adoption of document signing as a standard practice. A signature on paper, sometimes known as a wet signature, is a mark made on a paper document to indicate that the signer agrees to the terms stated in the document.[60] Furthermore, because each person's signature is distinct, it is used to identify the signer. Wet signatures can be validated, but they have a number of disadvantages. Signatures can be forged, and paper-based processes are inefficient in terms of both time and money.[61]

Electronic signatures have grown in popularity as a way to circumvent the inherent flaws of signing on paper. To preserve documents, high-trust digital signatures use public-key cryptography. A user must first be awarded a digital certificate that binds their real-life identity to a digital identity before they can digitally sign a document.[62] The user's digital certificate is incorporated into the document at the time of signing to act as irrefutable proof of the signer's identity. Multi-factor authentication, such as passwords and one-time PINS, can serve to strengthen the verification of the signer's identity. Strong encryption mechanisms prevent the papers from manipulation, and free apps like Adobe Reader can automatically check that a document has not changed since it was signed.

[59] Mayer, D., Warner, D., Siedel, G. and Lieberman, J., 2012. Law of Commercial Transactions – Open Textbook Library. Open Textbook Library.

[60] Acrobat.adobe.com. n.d. What is a wet signature | Wet vs electronic signature | Adobe Sign.

[61] Lawtrust. 2021. Wet signature vs. Electronic Signature vs. Digital Signature. lawtrust.co.za

[62] Acrobat.adobe.com. n.d. What is a digital signature | Adobe Sign.

Part 2

The Concept of Self-Sovereign Identity (SSI)

The Concept of Self-Sovereign Identity

The previous Part reminded the readers about the history of the Internet, advances of technological progress in the sphere of telecommunication, e-commerce, and the complete digitization of our lives. Now there is barely any sphere one could think of where one does not need a smartphone, tablet, or a laptop and an ID of any kind (passport, birth certificate, driving license, bank account, etc.) to perform our daily duties and tasks — starting from shopping online, calling a taxi, watching movies, signing up for a COVID-test to traveling, finding jobs, and managing our businesses and data. Governments and corporations are exchanging unprecedented amounts of data, cross-correlating everything, including viewing habits to purchases, information on the location of individuals during the day and the night, and with whom they interact.[63]

For several decades, together with the digitization of many processes, the concept of digital identity has evolved — from centralized identities to federated identities to user-centric identities to self-sovereign identities. All we did with identification sprang from the requirement for companies to save names in databases. This benefited the administrative convenience of those entities, but only to the extent that we are recognized individually by all of the entities that know us.[64] The increasingly digitized milieu wherein people interact, along with the widespread development of digital services, has resulted in an increasingly unstable and hazardous identity ecosystem. The growth of data and privacy regulations in Europe over the last decade reflects a rising awareness among legislators about the fragile status of digital infrastructure and the dubious actions of Internet corporations.[65] As a result, there is a growing need for greater control over our identities and personal information.[66]

SSI — self-sovereign identity — is a notion, or rather a philosophy, movement, that has the ability to address this demand. It is founded on a person's ability to own and govern their identity without relying on a centralized authority or the state.[67] People who seek more control over their lives and data are driving this shift. The easiest way to define this SSI market driver is that it attempts to accomplish for decentralized identity what Bitcoin aspires to accomplish for decentralized money.[68]

Why is it more than simply a fantastic approach to go further into the digitization of our lives and personal data storage? Christopher Allen, a pioneer of the SSI movement, describes SSI as a philosophy aimed at reclaiming human dignity and power in the digital age and, secondly, an evolving technological architecture designed to support that mobility.[69] Identification, identity, in essence, is a human right, despite it not being explicitly mentioned in the Universal Declaration of Human Rights. It does, however, acknowledge "the right to be recognized as a person before the law everywhere" in Article 6, the "right to a nationality" in Article 15, and the "right to hold property" in Article 17.[70] Unfortunately, when it comes to IDs and, particularly digital IDs, according to the World Bank's ID4D database, about one billion individuals worldwide lack any form of legally recognized identity. Another 3.4 billion people with some form of legally recognized identification are not participating in the digital economy, as seen by their lack of usage of social media.[71] SSI community professionals believe that the use of SSI will assist users in gaining control over their personal data while increasing individuals' access to human rights and the global economy.[72] They predict that the impact of SSI technology and the uncounted new patterns of trusted interactions will enable across all lifestyles.[73]

[63] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

[64] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p. 13

[65] Constine, J., 2018. A flaw-by-flaw guide to Facebook's new GDPR privacy changes. Techcrunch.com

[66] Simic, B., 2018. Council Post: Can Blockchain Solve Identity Fraud? Forbes

[67] Sindi, A., 2019. Adoption Factors of a Blockchain Digital Identity Management System in Higher Education: Diffusing a Disruptive Innovation - ProQuest. Proquest.com.

[68] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p. 14

[69] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

[70] López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain | Publications. Publications.iadb.org

[71] 2018. DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH. SUMMARY OF FINDINGS J. McKinsey.com

[72] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

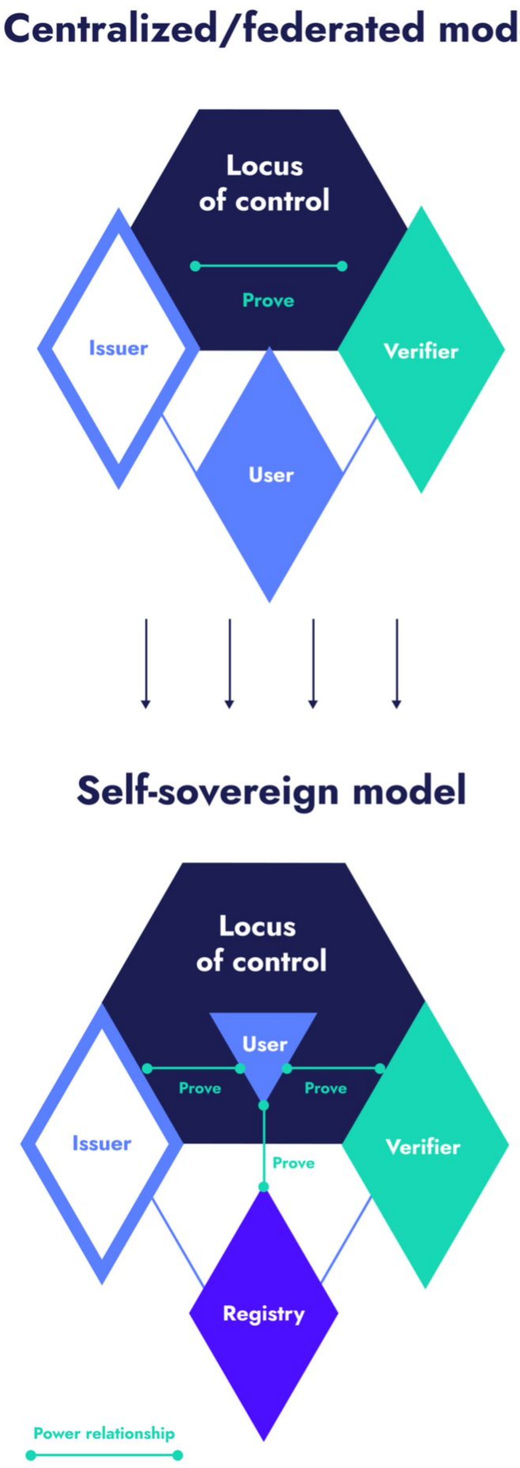
[73] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p. 12

The philosophy and principles of SSI

Self-sovereign identity represents "a shift in control."[74] The locus of control in the centralized and federated identity models is with the network's issuers and verifiers. The locus of control changes to the individual user in the decentralized SSI identity paradigm, who may now engage with everyone else as a whole peer.[75] For these reasons, SSI is much more than just tech. It also has significant commercial, legal, and societal implications.

The main point is that the user is the core administrator of their identity under the self-sovereign identity paradigm, and they have far more control over their data and information than others have, know, or disclose about them.

Decentralization is the process by which user sovereignty grows. It is applicable not just to governance but also to the construction and operation of nodes and networks. Moving toward decentralization improves user sovereignty, yet it is the most difficult thing to do since it contradicts all authoritarian instincts.[76]



The SSI method, unlike centralized and federative approaches, does not require an organization to manage people's identities. There is no requirement for an identity provider or a service provider to handle one's credentials and authenticators on their behalf. The identity provider's function has now been reduced to that of an identity issuer.[77] Christopher Allen states in his work: "*Self-Sovereign Identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale.*"[78]

In 2016, the author set 10 principles for self-sovereign identity that have become a reference in the field:

1. "Access: Users must have access to their own data.
2. Consent: Users must agree to the use of their identity.
3. Control: Users must control their identities.
4. Existence: Users must have an independent existence.
5. Interoperability: Identities should be as widely usable as possible.
6. Minimalization: Disclosure of claims must be minimized.
7. Persistence: Identities must be long-lived.
8. Protection: The rights of users must be protected.
9. Portability: Information and services about identity must be transportable.
10. Transparency: Systems and algorithms must be transparent".[79]

Everything in SSI can be split into two broad domains:

1. Authentic Data — includes passport, PCR test results, bus ticket, log-in credentials. This data is mirrored by semantic context.
2. Semantic Context — is called like this because SSI is part of the semantic web. The semantic web is an approach proposed by W3C aimed to extend the traditional so-called "web of documents".[80] The concept is that it is not only about putting data in digital format and having a cryptographic signature; it is also about providing context to people and machines about what this data means. The goal of the semantic web is to make data machine-readable by adding data descriptions (metadata) to existing content. In SSI, you may pass a piece of information (f.e, in JSON-LD format) to a programming protocol, and the machine will recognize it.

There is a number of standards that unfold the SSI concept.[81] The core two ones are under development by the World Wide Web Consortium (W3C), The Decentralized Identifiers (DID) Standard is the most significant, and it is at the heart of all others. To maintain compatibility, businesses must utilize DIDs exactly as defined in the standard. Any organization that does not use standardized DIDs will be unable to exploit the potential of interoperable standards. DID is both liberating and constricting.[82]

[74] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p. 12

[75] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications, p. 12

[76] Medium. 2020. A Unified Theory of Decentralization.

[77] López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications. Publications.iadb.org

[78] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

[79] Allen, C., 2016. The Path to Self-Sovereign Identity. Lifewithalacrity.com

[80] W3.org. 2021. Semantic Web — W3C

[81] Helmy, N., 2020. Overview of Decentralized Identity Standards. Medium.

[82] Hydraledger.io. 2021. What is SSI & DID

DIDs present a method for each person to establish their own unique identifiers in order to engage in the digital world. DIDs are designed to be "self-sovereign": that means an entity can create an identifier and prove the control over it itself, unlike traditional identifiers like passport numbers, phone numbers, etc., which are assigned by external authorities.

To genuinely be in charge of our personally identifiable information or any authenticated data, an individual must have ownership over the cryptographic keys that allow access to their own digital identity data. That's another field where DIDs, in combination with blockchain technology, may help, providing decentralized public key infrastructure. Once cryptographic keys are incorporated into a blockchain as a way of confirming credentials, new possibilities emerge; for example, any user might verify their information on the blockchain ledger rather than having point-to-point integration with an individual or organization.[83]

There is another constituent part of SSI — verifiable credentials (VCs). VCs, standardized by W3C in Verifiable Credentials Data Model 1.0, are tamper-evident digital equivalents for physical documents with cryptographically verifiable authorship. Individuals hold VCs, which include information or qualities about them (e.g., name, date of birth, location of residence, etc.). These credentials might be self-issued or issued by a third party. When the issuers are trusted authorities (e.g., a government or a financial institution), the subject might use these credentials to demonstrate such traits to others (e.g., a digital passport issued by a government). In the next Parts, a more in-depth analysis of the technology behind SSI will be presented to the reader.

[83] Lim, J., 2020. Self-Sovereign Identity: The Harmonising of Digital Identity Solutions Through Distributed Ledger Technology. Anujolt.org

What SSI brings to the table

SSI in the humanitarian context

Why is SSI technology beneficial to the humanitarian sector? For some time, there has been discussion regarding the loopholes in the current system of identification and identity. Migration crises, undocumented citizens of countries all over the world, global challenges due to the spread of COVID-19 all highlighted the necessity of dealing with the current loophole. States are continuously working to create new regulatory frameworks to regulate electronic identity and trust services for Internet access and electronic transactions.[84]

As estimated by the UNHCR, around **79.5** million individuals have been forced to leave their homes around the world. About **26** million refugees are among them, with nearly half of them being under the age of 18. There are also millions of stateless persons who have been refused citizenship and are deprived of essential rights such as education, health care, employment, and freedom of movement.[85] Within the context of UN Sustainable Development Goal 16.9, digital identification is promoted as a mean of allowing inclusive societies in which everyone has portable, long-term access to legal status and rights such as social and medical services, police protection, and economic engagement. It provides a potential answer to the problem that, in many specific circumstances, a variety of issues, such as the loss or damage of documentary proof, statelessness, and the absence of or exclusion from a national ID system, prohibit access to traditional methods of identification.[87] The rival logics involves four issues: (i) technology neutrality, (ii) refugee capacities, (iii) global governance and the nation state, and (iv) new economic models for digital identification.[88]

Blockchain technology has been used in proof-of-concepts for the World Food Programme's Building Blocks program in Syria, Jordan, and Pakistan, as well as the IFRC's 2018 digital identity and cash transfer program in Kenya and the UN's ID2020 alliance[89] — a collaboration between industry and humanitarian organizations. Mobile technology advancements have resulted in a transformation in the way humanitarian organizations offer relief to refugees. Sovrin is a permissioned blockchain that collaborates with iRespond19 to support SSI by generating a private key and authenticating users via iris scans.[90] This is an illustrative step towards keeping the data more secured by implementing two-factor authentication (private key in this case).

[84] UNHCR Blog. 2018. Bridging the identity divide — Is Portable User-Centric Identity Management the Answer? - UNHCR Blog.

[85] United Refugees. 2020. Figures at a Glance. UNHCR.

[86] Indicators.report. 2021. 16.9 by 2030 provide legal identity for all including free birth registrations — Indicators and a Monitoring Framework.

[87] Cheesman, M., 2020. Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. Geopolitics, pp.1-26.

[88] Cheesman, M., 2020. Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. Geopolitics, pp.1-26

[89] Who.int. 2018. Digital Opportunities for Displaced Women, Children and Adolescents.

[90] Who.int. 2018. Digital Opportunities for Displaced Women, Children and Adolescents.

Why is SSI a good foundation? There are still difficulties maintaining user identities, authenticating, and approving users as of today.[91] Because digital identities can be in a number of forms, technical standards for interoperability are a crucial need for a global identification system. Fortunately, many digital services now require or encourage two-factor authentication in addition to usernames and passwords. The capacity to verify yourself and manage a device or access card linked with the account ("something you have") or a biometric ("something you are") is combined with the shared secret of a username and password ("something you know"). However, using SSI, two-factor authentication may be upgraded to three, four, or even five factors, with each increase improving security: the linked device becomes a means for delivering real-time consent as well as a physical authentication element. You can prove ownership of a certain account using the cryptographic keys associated with your DIDs.The digital credentials allow you to verify information about yourself (such as your name or date of birth) using mutually trusted third parties. With a camera or fingerprint scanner, the digital wallet may provide real-time assurance that the person holding the device is the same as the person who registered or granted the credential.[92] SSI does not contradict the present authentication method; in fact, implementing SSI models can only improve the overall user experience while still ensuring privacy protection and control over personal data.

[91] Lim, S., Tankam Fotsing, P., Almasri, A., Musa, O., Mat Kiah, M., Ang, T. and Ismail, R., 2018. Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. International Journal on Advanced Science, Engineering and Information Technology, 8(4-2), p.1735.

[92] Un.org. 2021. ID2020 Summit 2016.

SSI interoperability for interstate cooperation

SSI is a novel concept, and there are still a lot of technical issues to be resolved before it can be used for its current and future planned purposes in identifying management and tackling global economic crises. However, intergovernmental groups and governmental unions, such as the ID2020 Alliance and the EU, have prioritized its development, emphasizing the importance of the provision of all invisible and vulnerable people with legal identity by 2030 to make them visible and restore them into society.[93]

The eIDAS Regulation established a trust framework at the EU level.[94] eIDAS establishes the assurance levels for electronic identification and defines the basis on which each EU Member can recognize the identification credentials of other EU Members. These categories are intended to be relevant to a wide range of identity systems. Furthermore, the Regulation authorizes the use of electronic signatures and seals by ensuring their legal effect and allowing recognized organizations to act as trust service providers.[95] Since 2018, the European Blockchain Partnership has brought together 29 countries (all EU member states, Norway, and Liechtenstein) and the European Commission (EBP) to collaborate in order to realize the full potential of blockchain-based services for the benefit of citizens, society, and the economy.[96] Recently, the European Commission[97] suggested a framework for a European Digital Identity that would be open to all EU citizens, residents, and enterprises. With the touch of a button on their phone, citizens will be able to authenticate their identity and exchange electronic documents from their European Digital Identity wallets.

The SSI eIDAS bridge, a project supported by ISA2, was created by the European Commission to promote eIDAS as a trust foundation for the SSI ecosystem. It aids the signing procedure for VC issuers and enables the verifier to automate the identification of the entity behind the issuer's DID. A Verifiable Credential may be verified trustworthy in the EU simply by "passing" the eIDAS Bridge.[98] The European Self-Sovereign Identity Framework (ESSIF), one of the European Blockchain Services Infrastructure (EBSI) basic use cases, now includes the eIDAS Bridge.

A blockchain ledger is considered a helpful technology for the purpose of the ESSIF initiative. It allows data to be securely exchanged among various parties, and parties must be granted permission to read and append data to the blockchain. A durable and portable digital identity and digital history is extremely beneficial to disadvantaged populations who are constantly on the move in terms of identity.[99]

At the same time, ID2020 Alliance has been advocating for ethical, privacy-protecting methods to digital ID since 2016. They base their manifesto on ten key points.[100] The main aim can be explained as follows: "the necessity to enable persons who face legal, political, social, and economic marginalization to achieve official identity is obvious in the context of the 2030 Agenda for Sustainable Development, which was endorsed by world leaders in 2015 with the overriding objective of leaving no one behind".[101] Supplying digital identity removes a major impediment to receiving services and exercising core human rights while also granting individuals the self-sovereign power expressed in having agency over their personal data.[102]

[93] Un.org. 2021. ID2020 Summit 2016.

[94] Shaping Europe's digital future. 2021. eIDAS Regulation.

[95] UNHCR Blog. 2018. Bridging the identity divide — Is Portable User-Centric Identity Management the Answer?.

[96] CEF Digital. 2021. EBSI.

[97] Press release. 2021. Commission proposes a trusted and secure Digital Identity for all Europeans.

[98] Joinup.ec.europa.eu. 2021. SSI eIDAS bridge.

[99] Casino, F., Dasaklis, T. and Patsakis, C., 2019. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, pp.55-81.

[100] ID2020. 2021. ID2020 | Manifesto.

[101] Un.org. 2021. ID2020 Summit 2016.

[102] Medium. 2018. Digital ID: The Power, Promise, and Challenge.

Digitization of all areas

For centuries, the only form of proof of facts was paper documents. Despite the rapid digitalization of all areas of life, a significant part of the documents and facts still remain in paper form. Paper documents do not correspond to the level of technological breakthrough that has occurred in recent years when the Internet has become a universal means of communication between people, corporations, and governments. One of the main benefits of SSI is, in fact, digitization and automation of services, meaning — reducing transaction costs of the business and making the process automatic and digital. Paper-based bureaucracy is slowly becoming history. SSI is a way of digitization that does not require is based on digital standards; one does not need to create a new connection.

Governments would need to transition to the SSI scheme for the provision of SSI-compatible national ID documents and the establishment of techno-legal frameworks.[103] Implementation of the self-sovereign identity approach has the advantage of enabling governments to issue digital IDs to persons that can be used to access any type of digital service without huge capital investments or extra responsibilities. Government offers identification credentials, the proofs of which are stored in a blockchain ledger as well as in trusted lists.

Lack of switching costs

Vendor lock-in in public IT services refers to a situation in which a user or a company is reliant (locked-in) on a single provider. A user or a company cannot simply switch vendors in the future without encountering problems such as excessive fees, legal restrictions, or technological incompatibilities. SSI is becoming more standardized and interoperable, as well as being portable and free of vendor lock-in. Because applications and agencies are modular and interchangeable, real SSI is not reliant on any one corporation or other organization.[104] It is not necessary to lose one's credentials, relationships, or history while switching from one service provider or agency to another.

When employing the SSI technique, the IDP's role may be eliminated, so the costs of maintaining a user management system and protecting against potential threats are passed to the holder and/or cryptographically secured.[105]

[103] López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications. Publications.iadb.org.

[104] Ruff, T., 2018. The Three Models of Digital Identity Relationships. Medium

[105] Laube, A. and Hassenstein, G., 2020. Self-Sovereign Identities Will the identities of Swiss university members be controlled by themselves in future?. 1st ed. Bern University of Applied Sciences Department of Engineering and Information Technology Institute for Data Applications and Security (IDAS), p.p.24.

More privacy for their citizens

In various ways, the SSI approach improves data privacy. It reduces the possibility of data aggregation violating privacy and eliminates information silos. Major attacks are also made more difficult because centralized repositories are no longer required. Ideal SSI implementations also ensure the right to be forgotten, the right to consent, the right to pseudonymization, data portability, and the minimization of PII.[106] Data maintenance necessitates a significant amount of effort in order to attain a high degree of data quality, which results in significant expenses. In addition to master data, organizations must provide certifications or other firm identity elements to consumers.

The master data in an SSI approach is based on electronic proof (e.g., excerpts from the business register or bank cards) from authorized issuers, and each legal entity may choose which data is automatically available to whom and is therefore in control of its data at all times.[107] Within a system in which trust and data security become the fundamental aspects, the person/user, as the original bearer of the data, acquires full control over his or her identity, determining if and which certified attributes to make available to external parties.[108] The user is no longer only a data subject, but also the controller of his identity, according to GDPR categorization and the use of SSI technology enables to eliminate the need for a central institution acting as intermediary, assuring instead a pattern of trusted interactions made possible by cryptography and collaboration mechanisms.

Framework for compliance

There is a growing attention to the user data privacy coming from both end users as well as regulators. Businesses need to take into account regulatory requirements such as CCPA, GDPR, FISMA, EFF and many more similar regulations in other geographies. In the European Union, for example, the GDPR (General Data Protection Regulation) is the most recent addition to a slew of new projects that already includes PSD2 (second Payment Services Directive) and eIDAS (electronic Identification Authentication and Trust Services). In the United States, the CCPA (California Consumer Privacy Act of 2018) went into effect on January 1, 2020. This regulation could serve as a model for a federal framework in the country.[109]

According to the principles of SSI, self-issued IDs might be more GDPR compliant because only minimal data has to be exchanged and retained. The identity itself can be completely controlled by the user.[110] Privacy compliance is enabled by default, so one does not have to worry about GDPR or CCPA because you will get it free if you use SSI. Transparency inside an SSI platform, according to Elizabeth Renieres, can assist with GDPR compliance. Individuals have the right under GDPR Articles 13 and 14 to be notified about the acquisition and dissemination of their personal data. With the use of an SSI platform, individuals would be able to join a network that provides transparency in line with domestic and international regulations.[111]

[106] López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications. Publications.iadb.org.

[107] Bosch Global. 2021. Digital identity – enabling secure collaboration with blockchain technology.

[108] Monokee. 2021. Trust and data protection: SSI potential regarding privacy – Monokee.

[109] Thales Group. n.d. Self-sovereign identities at work – Digital identity 2.0.

[110] Laube, A. and Hassenstein, G., 2020. Self-Sovereign Identities Will the identities of Swiss university members be controlled by themselves in future?. 1st ed. Bern University of Applied Sciences Department of Engineering and Information Technology Institute for Data Applications and Security (IDAS), p.p.24.

[111] Medium. 2020. Self-Sovereign Identity Principle #4: Transparency.

Transparency and auditability

The way in which an identity system operates is controlled and is updated must be public and sufficiently intelligible.[112] To avoid vendor lock-in, solution design should be built on open protocol standards and open-source software. In other words, it should be guided by the principle of transparency, the fourth guiding principle of SSI outlined by Christopher Allen.

Transparency must guarantee that users can monitor any possible mistreatment of identity-related claims, credentials, or connections. Individuals and users will be able to analyze how their personal information is being used. The mechanisms and procedures used to administer a network must be open, not just in terms of how they operate but also in how they are controlled and improved. As an outcome, every user will be able to examine how networks work and how their data is maintained.[113] SSI's governance model should minimize administrators' ability to access, remove, or otherwise tamper with the user's identity and personal information.[114]

Nobody expects SSI to be tied to a certain single ecosystem. In turn, entire families of applications and credentials will coexist.[115] But since those ecosystems are based on open standards and ruled by common reachable and transparent governance mechanisms, users and regulators may always check why the system behaves in one way or another.

Open provable democracy

According to the Commission, the promotion and regulation of digital identity are essential in maintaining an 'open, democratic, and sustainable society,' which is one of the main objectives of this data strategy.[116] By enacting the eIDAS legislation, Europe has just laid a solid framework for digital identity and trust services. The shift to eGovernment will result in the establishment of an open, verifiable democracy. Citizens may present/use government-grade digital attestations anywhere they choose, without worrying governments or forcing governments to commit with attestation-specific hardware and software in order to serve their citizens. A crucial organizational component in the development of a European Framework for Self-Sovereign Identity. The SSI dimension is based on human behavior and relationship concept that reflects basic European ideals such as individual emancipation and independence, human rights, and dignity. In order for European society's democratic and sovereign underpinnings to remain safe in an era of advanced technology environment, its digital identification infrastructure must be built on those same ideals.[117]

[116] Giannopoulou, A. and Wang, F., 2021. Self-sovereign identity. Internet Policy Review.

[117] CEF Digital. 2021. EBSI.

Positive effects for end-users

The SSI community identifies several benefits for SSI-users:

1. Control over one's own personal data. Users have control over the maintenance of their digital identity and the identification data linked with it. In addition, the holder of the data, the user has absolute control over what is shared with others, and most notably, by using SSI technology, users can delete their personal information at any time. SSI provides new solutions to strengthen.

2. Privacy and individual rights protection, such as granular consent management and data minimization strategies that allow individuals to contribute only the data they choose to give.

3. SSI is also promoted for its convenience. Because of standardized digital credentials that can be used for all contacts and are kept in one location, interactions and transactions are more efficient.

4. By deploying extensive encryption, SSI improves data security and aids in the prevention of identity theft and other types of fraud. Decentralized storing and management of identification attributes raise the relative cost of hacking dramatically.

5. Lock-in effects, such as those inherent in traditional Federated Identity systems, can be avoided by allowing individuals to control and maintain their identity data on their own terms. This empowerment has far-reaching consequences for identity and data portability. Individual digital identities become more robust when they get the capacity to travel between services.[118]

6. In addition to this SSI technology provides for a persistent reputation. Individuals, organizations, and objects all have a reputation, which indicates how respectable and trustworthy they are. An identity is made up of a shadow reputation, which refers to who or what is in the user's/organization's/network device and how that actor's reputation impacts the reputation. SSI can help build a reputation system that integrates with this identity system that gives the users a means to decide how much to trust each other. In the online business, online reputation management has become a necessary part. For example, the rise of fake reviews is undermining consumer confidence in reputation systems. Amazon has long tried to fight this gaming with various protection measures, including its Amazon Verifier Purchase program that is supposed to ensure the reviewer actually bought the product.[119] The SSI, on the other hand, can be a solution, and reputation systems can screen out bots by requiring verified credentials for reviewers. They can demand that a product purchase be accompanied with a verifiable credential, a verifiable receipt so that solutions like Amazon Verifier Purchase can function independently of any single merchant. Furthermore, reviewers can begin to build a reliable reputation independent of not only product vendors but also retailers; this is how an ecosystem of widely trusted independent reviewers can be built.[120]

[118] Wagner, K., Vila, X., Vandy, N., Bachenheimer, D. and Beron, D., 2020. Decentralised Identity: What's at Stake? A Position Paper by the INATBA Identity Working Group. International Association for Trusted Blockchain Applications, p.10

[119] Reed, D. and Preukschat, A., 2021. MEAP of "Decentralized Digital Identity: The advent of Self-Sovereign Identity (SSI)". Manning, pp.68-93

[120] Reed, D. and Preukschat, A., 2021. MEAP of "Decentralized Digital Identity: The advent of Self-Sovereign Identity (SSI)". Manning, pp.68-93.

7. Users see advertising tailored to their recent search at the medical office, or pet food, while they briefly complimented neighbors' puppy, and hyper-personalization has grown unsettling. Companies now offer hyper-personalization in exchange for data, but most of the time, they just need to deal with a single tiny part of our identities, such as our sizes or prior purchases. Consider how much more personalization they'll be able to provide consumers if they have (anonymous and limited) access to our private information. Because the hyperpersonalization paradox is taking place, and, e.g., in the Netherlands, according to Deloitte, In general, 58 % of Dutch residents are concerned about their privacy, and 88% want more control over the data they supply to businesses. Furthermore, due to the reputational and regulatory concerns involved, companies are becoming increasingly worried about all of the personal data they process from their clients.[121] With the use of SSI, that can be achieved because personal data will be under the user's control, and the user will decide what information will be shared.

The reader will dive deep into the pillars of the SSI idea in the next Part to understand the magic of SSI architecture.

[121] Privacy for sale — To the highest bidder, Data and ethics survey. Deloitte LLP and affiliated entities., pp.1-18.

Part 3

Deep Dive in the SSI Structure

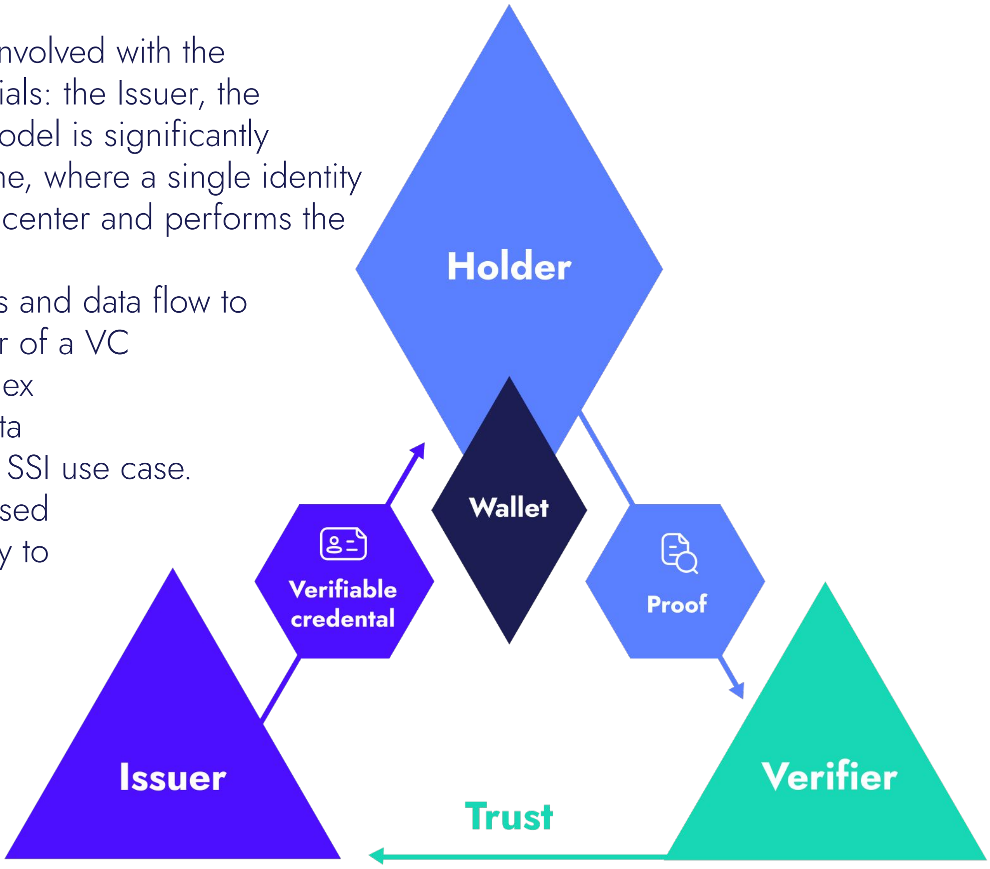
Technical aspects of SSI

SSI technology is a software architecture in which users’ data is kept in a decentralized manner (without the need for a single registry) and is completely controlled by the user. In this instance, the data is not held centrally, and instead of businesses and states, the data owner, that is, the user, is the only owner of the data.

Because of data sovereignty and portability, you may use any "digital wallet" application to keep all of your credentials in one storage, from your passport to your medical certificate, flying ticket, and diploma. Similar to paper, you determine how to keep it, who will have access to it, and how it will be protected and presented. In some cases, SSI enables you to establish any information about yourself digitally and legally relevant without sharing details: for example, to establish that you are above the age of 18 without providing your date of birth.

Trust Triangle and how it works

There are three primary roles involved with the exchange of verifiable credentials: the Issuer, the Holder, the Verifier. The SSI model is significantly different from the traditional one, where a single identity provider (the issuer) sits at the center and performs the role of a middleman while controlling the access for users and data flow to verifiers. Instead, it's the holder of a VC who sits at the center of complex relationships. The verifiable data registry is at the heart of every SSI use case. The "Trust Triangle" is a term used frequently in the SSI community to describe the SSI concept and demonstrate the relationships between the actors.



Trust triangle is a model intended to illustrate the process of credential arrangement, which is basically the following:

1. Certain entity (called the Issuer) issues a VC to the subject (an entity about which claims are made). Typically, the subject is also the holder of a credential in one person.
2. The Holder stores received a credential in his digital wallet.
3. The Holder wants to get a certain service from a Verifier.
4. Before providing a service, the Verifier asks the Holder to present a set of VCs.
5. The Holder presents VCs to the Verifier.
6. The Verifier checks the received VCs. It's not enough to validate credential proofs: the Verifier must trust the Issuer. Therefore, he checks some corresponding data publically stored in a verifiable data registry (properties confirming the authority of the issuer).

In essence, VC is a standard method for digitally expressing credentials in a cryptographically secure, privacy-preserving, and machine-verifiable manner.[122] As a standard, it signifies a remarkable transformation in emerging digital system design alternatives, transitioning from systems that offer more portable and user-centric digital identification, which is key to 'self-sovereign' or 'decentralized identity.'[123]

[122] Belchior, R., Putz, B., Pernul, G., Correia, M., Vasconcelos, A. and Guerreiro, S., 2020. SSIBAC: Self-Sovereign Identity Based Access Control. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).

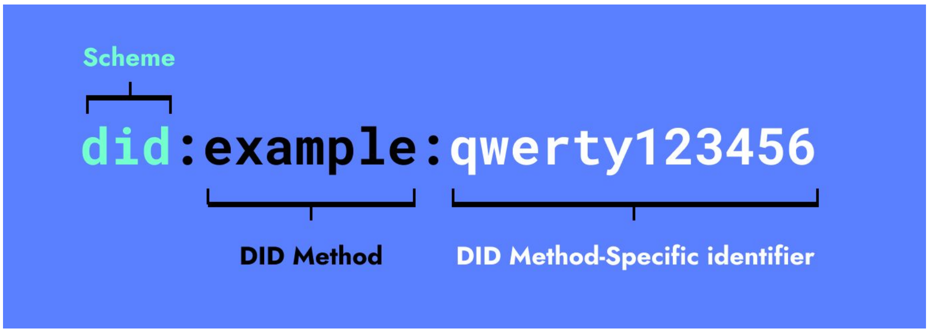
[123] Helmy, N., 2020. A solution for privacy-preserving verifiable credentials. Medium.com.

What is a decentralized identifier (DID)

As individuals and organizations, many of us use globally unique identifiers in a wide variety of contexts (telephone numbers, passports, usernames). Typically, they are issued by external parties.[124] However, for the purposes of the SSI ecosystem, there is a need for a "self-sovereign" decentralized identifier.

To meet all the SSI requirements, a DID should have the following properties.[125]

1. A permanent identifier.
2. A resolvable identifier (a standardized set of information about the DID can be discovered).
3. A cryptographically verifiable identifier (the control over DID can be proved using cryptographic mechanisms).
4. A decentralized identifier (no centralized body needed to perform CRUD operations on DID).



A DID syntax (W3C)

Any DID is a string of characters that consists of the following blocks, separated by a colon:

1. A "did" prefix.
2. A DID method identifier.
3. A unique identifier based on the DID method.

Because of the nature of a decentralized ecosystem, there is no single "true" DID method. Instead, nowadays, about a hundred DID method types have already been developed.[126] Blockchains and other distributed ledgers are used in several DID methods. Creating or changing a DID in this scenario usually entails writing a transaction to that ledger. Other DID techniques do not employ a blockchain and instead use other methods to implement the four DID actions. So, the DID method directly affects how its functionality should be implemented. Which method to use depends on the specific use case.

[124] W3c.org. 2021. DID Core..

[125] W3c.org. 2021. Use Cases and Requirements for Decentralized Identifiers.

[126] W3c.org. 2021. DID Specification Registries.

All DID Methods can be divided into the following categories:

1. Ledger-based. The most conventional method of DID implementation. A DID is rooted in blockchain and corresponding operations (creating, updating) are performed by writing a transaction to the ledger.
2. Ledger-middleware. DIDs operations are conducted at the second layer instead of requiring a base layer ledger transaction every time, as in the first technique. Instead, several transactions are combined into a single transaction, avoiding high transaction costs.[127]
3. Peer DIDs. These DIDs are not stored inside any public source of truth like a database or blockchain. Instead, a DID is created in the holder's VC wallet and shared only with the entity with which the trusted connection is established. They are free from transaction costs, extremely scalable but not resolvable and therefore not suitable for all the cases.[128.]
4. Static DIDs. This is a type of DID that can only be formed, resolved, and cannot be changed or deleted. DIDs have been simplified to the point that they don't require sophisticated protocols or storage infrastructure to function.[129]
5. Alternative DIDs. There are plenty of other DID methods even at the top of existing internet protocols (did:git, did:web, etc.).[130]

A DID itself is just a string of characters. But like a typical web address, it's only useful when it's linked with certain content. With the help of software, it can be used to get this data in the form of a so-called DID document. Public keys, services linked with this DID, authentication techniques, and other metadata indicating how to conduct trustworthy interactions are often included in a DID document.

```
{
  "@context": [
      "https://www.w3.org/ns/did/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
]

  "id": "did:example:123456789abcdefghi",
  "authentication": [{
      "id":"did:example:123456789abcdefghi#keys-1",
      "type":"Ed25519VerificationKey2020",
      "controller":"did:example:123456789abcdefghi",
      "publicKeyMultibase":"zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

A DID Document example (W3C)

A DID Document doesn't have to be a separate file stored anywhere. Instead, more complex resolution methods can be used, so that DID documents objects are generated "on the fly."[131]

[127] Reed, D. and Preukschat, A., 2021. MEAP of "Decentralized Digital Identity: The advent of Self-Sovereign Identity (SSI)". Manning, p. 171

[128] Identity.foundation. 2021. Peer DID Method Specification.

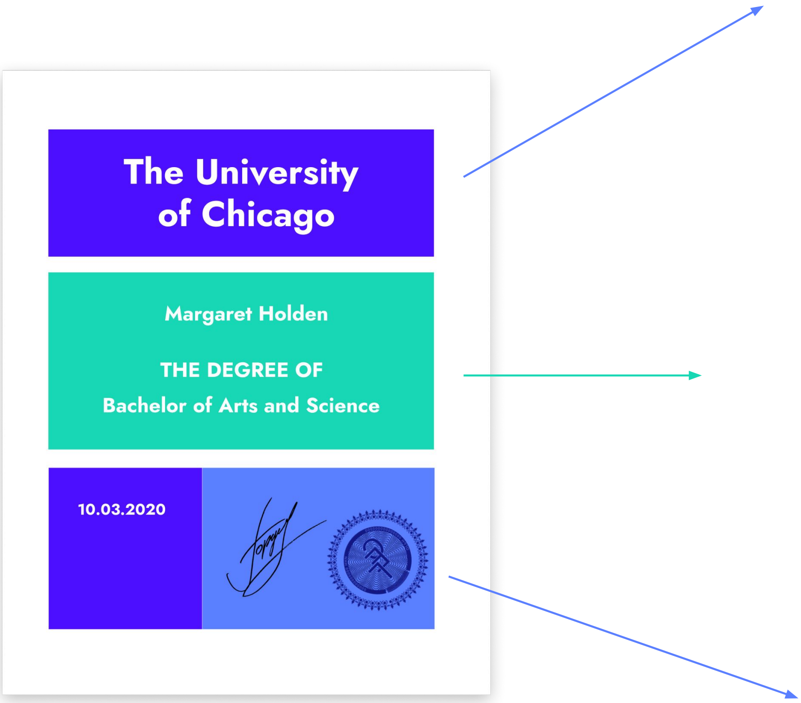
[129] Reed, D. and Preukschat, A., 2021. MEAP of "Decentralized Digital Identity: The advent of Self-Sovereign Identity (SSI)". p.171

[130] Reed, D. and Preukschat, A., 2021. MEAP of "Decentralized Digital Identity: The advent of Self-Sovereign Identity (SSI)". p.171

[131] Sabadello, M. and Zagidulin, D., 2021. Decentralized Identifier Resolution (DID Resolution) v0.2. W3c-ccg.github.io.

What is a verifiable credential (VC)

VC refers to a data structure that contains some claims about the subject. Those claims are made by a single authority, which in SSI is called an issuer of the credential. For end-users the value of this element of the SSI stack is most obvious and visible.



The University of Chicago

Margaret Holden

THE DEGREE OF

Bachelor of Arts and Science

10.03.2020

VC Metadata

```
{
"@context": [

"https://www.w3.org/2018/credentials/v1",
"https://www.w3.org/2018/credentials/examples/
v1"],

"id": "http://example.gov/credentials/3732",

"type": [
    "VerifiableCredential",
      "UniversityDegreeCredential"],

"issuer": {
    "id":
    "did:web:vc.transmute.world"
},

"issuanceDate": 2020-03-10T04:24:12.164Z",
```

VC Claims

```
"credentialSubject": {
    "id":"did:example:ebfeb1f712ebc
     6f1c276e12ec21",

     "degree": {
        "type": "BachelorDegree",
        "name": "Bachelor of
        Science and Arts"
    }
},
```

VC Proof

```
"proof": {
    "type": "JsonWebSignature2020",
    "created": "2020-03-21T17:51:48Z",
    "verificationMethod": "did:web:vc.
        transmute.world#_Qq0UL2Fq651
        Q0Fjd6TvnYE-faHiOpRlPVQcY_-t
        A4A",
    "proofPurpose":"assertionMethod",
    "jws":"eyJiNjQiOmZhbHNlLCJjcml0
        IjpbImI2NCJdLCJhbGciOiJFZERTQSJ
        9..OPxskX37SK0FhmYygDk-S4csY_
        gNhCUgSOAaXFXDTZx86CmI5nU9xkqt
        LWg-f4cqkigKDdMVdtIqWAvaYx2JBA"
    }
}
```

In terms of content, a verifiable credential does not significantly differ from a physical credential. But the mix of physical credentials and technologies, such as cryptographic mechanisms, makes verifiable credentials much more trustworthy than their physical counterparts. When based on proper asymmetric cryptographic algorithms, digital signatures are extremely forgery-resistant: actually, they are compromised not by hacking as such but by unauthorized obtaining of a private key.[132] In addition, in the case of handwritten signatures, the detection of forgery often depends on the verifier's observation, whereas in the case of digital ones, systems are designed to explicitly indicate that something is wrong. In other words, digital signatures and other methods of cryptographic protection are tamper-evident.

There are three core characteristics[133] of verifiable credentials:

1. It is machine verifiable.
2. It is secure and tamper-proof.
3. Has been issued by a competent authority.

W3C Verifiable Claims Working Group chose the JSON-LD[134]schema as a structural basis of their verifiable credentials since it already defines how to extend objects in a way that maximizes interoperability. However, other approaches already exist (f.e. JWT[135] as VC model or Blockcerts[136]).

[132] Wright, P., 2021. Can digital signatures be forged? Viafirma's Blog

[133] Medium. 2021. What are Verifiable Credentials?

[134] Json-ld.org. 2021. JSON-LD - JSON for Linking Data.

[135] Jwt.io. 2020. JWT.IO - JSON Web Tokens Introduction.

[136] Blockcerts. 2021. Blockchain Credentials.

A typical VC in the form of JSON-LD object basically contains the following properties:

1. @context. This part inherited from the JSON-LD model allows people or systems to know what JSON properties a VC may contain. The @context property contains a sequence of one or more URIs that refer to either set of properties described in structured templates called schemas or, preferably, a machine-readable document that can be downloaded and configured automatically on the verifier's side.[137] Anyone can publish a new schema and then refer to its properties in VC.

2. Type. This property allows verifiers to detect whether VC can be recognized and handled without reading whole context data. Contains a list of URIs. The first type must always be https://www.w3.org/2018/credentials/v1 which can be abbreviated to "VerifiableCredential" string using the JSON- LD @context mechanism.

3. ID. A single URI that allows entities to refer to this VC.

4. Issuer. A single URI that identifies the issuer. Depending on the type of implementation, it can be the DID of the issuer (which in turn refers to the DID Document) or just a DNS name.

5. Issuance date. Date and time in ISO 8601 [138] format.

6. Credential claim(s). That is the content part of a verifiable credential. Any fact that the issuer asserts about the subject is called a claim. Claims are organized into credentialSubject property that also optionally includes reference to the ID of the subject (may be missing in some cases). A VC can contain multiple claims, where each claim is about a different credential subject.

7. Proof(s) A proof is the cryptographic mechanism used to prove that the VC was issued by a certain issuer and was not tampered with. In simple words, this part of a VC stipulates credential verifiability. Verifiable Credentials Data Model 1.0 is designed to be flexible and does not insist on any certain type of proof, so several different types of proof can be used. Moreover, several proofs can be used simultaneously.

In this document, there was described only the basic VC structure. W3C Verifiable Claims Working Group also proposes some more useful properties, such as expirationDate, credentialStatus, and others. Visit Verifiable Credentials Data Model 1.0 web page to have a deep dive.

[137] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p.139

[138] Iso.org. 2019. ISO 8601 date and time format.

What is a verifiable presentation

Verifiable presentation (VP) is the collection of credentials that a holder may present to a verifier. A VP is one way a holder may combine several VCs to send to a verifier. VPs structure is very similar to a VC in that it contains metadata about the presentation plus a proof signed by the holder. However, there are also several differences:

1. The content part is now a set of VCs rather than a set of claims.
2. The issuer attribute is missing.
3. An id property is optional (may be included in case if the reference to this VP is needed in the future).[139]

Certain types of verifiable presentations might contain data that is synthesized but do not contain the original verifiable credentials.[140]

Communication mechanisms and DIDComm in SSI ecosystem

In the context of SSI, communication refers to establishing cryptographic trust between the parties. Three factors are necessary for this purpose:[141]

1. Each party controls its DID.
2. The connection between DIDs is secure enough.
3. A sent message is authentic and has not been unauthorizedly modified.

When building a DID communication mechanism, there are two distinct architecture approaches, which directly affect technical implementation. The chosen approach will determine how software components of the SSI ecosystem will interact at different levels.

Web-based approach. Communication is established by masking API calls and using secure TLS protocol. Systems are based on traditional RESTful service calls. However, some critical issues arise with this design. It's based on a request-response interaction with both parties being online at the same time, which sometimes is not possible in the SSI ecosystem. Privacy issues connected with TLS may also arise because of man-in-the-middle attacks.

Message-based approach (DIDComm). DIDComm is a message-oriented peer-to-peer protocol between agents identified by DIDs.[142] The purpose of DIDComm is to provide a secure, private communication methodology built atop the decentralized design o DIDs. As noted above, a traditional request-response schema is not always appropriate for the SSI ecosystem. Parties may need to be offline for an unpredictable time and then resume connection to the network. Moreover, they may need to communicate even when the internet is unavailable. That's why DIDComm is designed to be message-based and asynchronous, being much more similar to email. DIDComm is also a transport-agnostic protocol that means that it should be able to operate over HTTPS 1.x and 2.0, WebSockets, Bluetooth, SMTP, NFC, etc.[143]

[139] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p 142

[140] Sporny, M., Chadwick, D. and Longley, D., 2019. Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web. W3C.org.

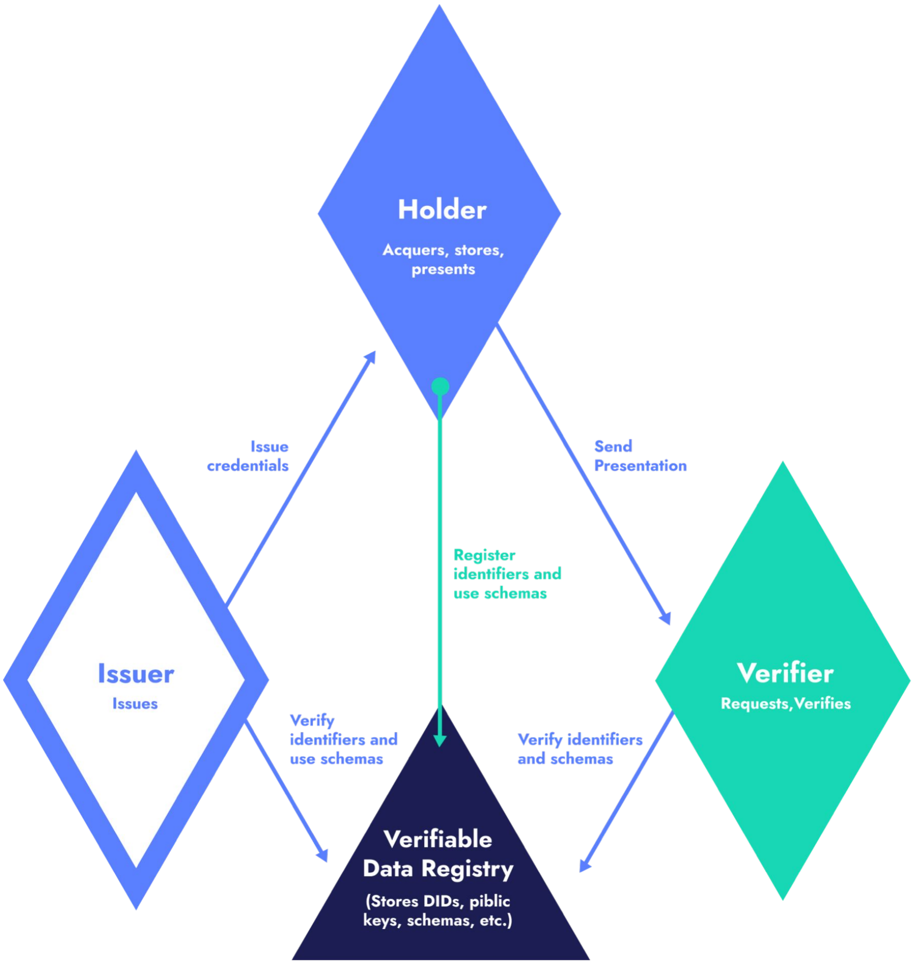
[141] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 94

[142] Hardman, D., 2021. DIDComm Messaging Specification. Identity.foundation.

[143] Hardman, D., 2021. DIDComm Messaging Specification. Identity.foundation.

What is a verifiable data registry

According to W3C, a verifiable data registry is a system mediating the creation and verification of identifiers, keys, and other relevant data.[144] All this data enables the VC ecosystem to operate.


Holder
Acquers, stores, presents
Issue credentials
Send Presentation
Register identifiers and use schemas
Issuer
Issues
Verifier
Requests, Verifies
Verify identifiers and use schemas
Verify identifiers and schemas
Verifiable Data Registry
(Stores DIDs, piblic keys, schemas, etc.)

Examples of the types of data and metadata that can be stored in this registry are the following:[145:]

1. Issuers' public keys.
2. Schemas describing possible verifiable credentials properties.
3. VC revocation registries.
4. Lists of claim types that issuers declare they are authoritative for.[146.]

Currently, there is no single standard for verifiable data registry. Being an immutable distributed tamper-resistant source of truth that no single entity controls, it's often the blockchain that is used as a verifiable data registry. However, other solutions, both centralized and decentralized, are possible: trusted databases, distributed file systems, distributed hash tables, etc. Often there is more than one type of verifiable data registry utilized in an ecosystem.[147]

[144] Sporny, M., Chadwick, D. and Longley, D., 2019. Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web. W3C.org.

[145] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p 130

[146] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 134

[147] Sporny, M., Chadwick, D. and Longley, D., 2019. Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web. W3C.org.

Selective disclosure. Zero-knowledge proofs

According to Verifiable Credentials Implementation Guidelines,[148] selective disclosure means the ability of a holder not to disclose all of the attributes contained in a VC. For example, you may need to provide only your name and registration address without showing other data from your ID document. The selective disclosure feature enables verifiers not to collect and store more data than necessary. Possible selective disclosure solutions are:

1. Issuance of a separate credential for required attributes.
2. Usage of zero-knowledge cryptography methods.

Obviously, the main disadvantage of the first method is the need to involve the issuer in most cases. Zero-knowledge proof methods may be a solution for this problem.

In cryptography, a proof refers to involving cryptographic mechanisms to demonstrate that a certain fact is true. Zero-knowledge proof is that kind that allows a prover to convince a verifier beyond a doubt that they know something without revealing what it is that they know.[149.] In the VC ecosystem, zero-knowledge proofs allow selective disclosure without involving the issuer giving two options[150]:

1. Reveal the value of a certain attribute.
2. Just prove that this attribute exists in VC without revealing it.

Another great thing that the ZKP-methods provide is predicate proofs. Predicate proof means answering a true/false question: "Are you a student? Are you 21 years old?". Using ZKP, predicate proofs can be generated on the fly by the holder.

Also, ZKPs have strong privacy-protecting advantages; there are also some ZKP drawbacks[151,] such as the complexity of technical implementation and higher hardware usage (memory, CPU) compared to traditional cryptographic methods.

[148] W3.org. 2019. Verifiable Credentials Implementation Guidelines 1.0.

[149] Expressvpn.com. 2017. What is a zero-knowledge proof and why is it useful?

[150] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 122

[151] W3.org. 2019. Verifiable Credentials Implementation Guidelines 1.0.

Governance stack of SSI

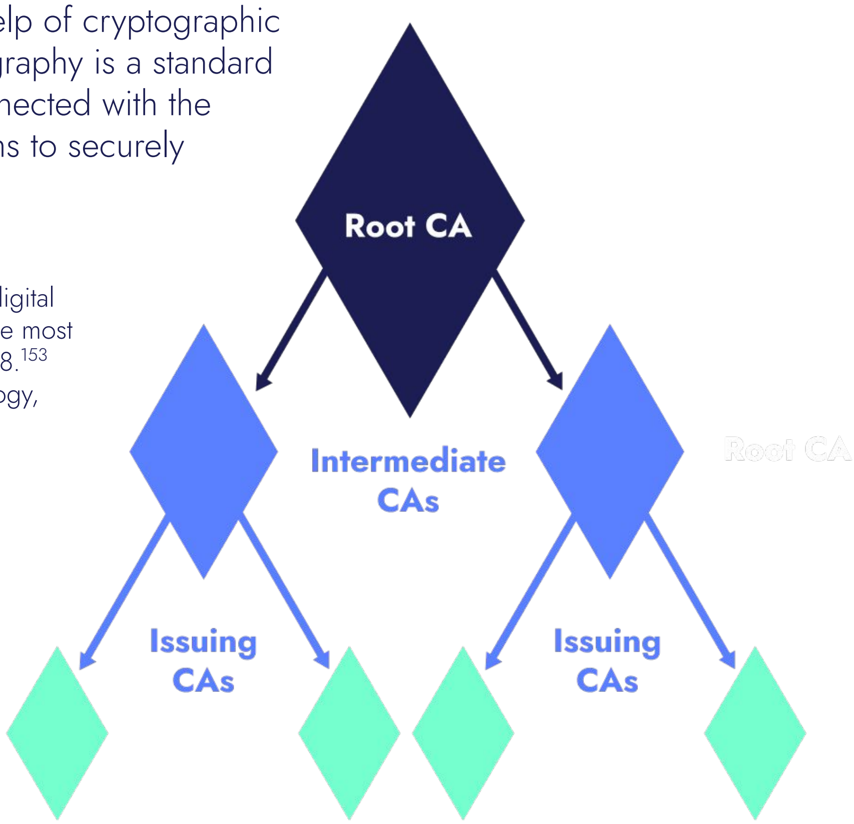
The term "Governance" can be widely described as managing, controlling, and making decisions in some system like society or state. The SSI ecosystem needs governance at all the layers to function properly. First of all, governance is needed to ensure a proper trust level between actors in SSI. Anyone can introduce themselves as the US Government and start issuing credentials, so there must be a certain root of trust. Generally, two collective governance models can be distinguished. One, centralized, is not only familiar to us for a long time, since it comes out of our real life, but has become a kind of industry-standard on the Internet. Another decentralized approach, being a relatively new model, seems more in line with the nature and needs of SSI.

Centralized governance model for SSI (PKI+CA)

One of the key governance aspects is authorizing somebody to act. In the digital environment and, especially in computer networks, that's generally done with the help of cryptographic mechanisms. Because asymmetric cryptography is a standard de-facto here, governance is strongly connected with the term "public key infrastructure," which aims to securely associate a public key with an entity.[152]

The traditional centralized model is based on issuing digital certificates that prove the ownership of public keys. The most common certificate format is X.509, defined in RFC528.[153] The advantage of X.509 certificates is that the technology, processes, and governance behind them are well-known and developed.[154]

This model is hierarchical. That means there is a chain of certificates, each of them (except the root one) is signed by a superior certification authority.



However, this approach seems not suitable for the needs of SSI for the following drawbacks:

1. It is centralized. In a typical scheme, a certificate is issued by a trusted third-party — certificate authority. Certificate authority may revoke the certificate for any reason. Only legal rulings can prevent a centralized authority from malicious acting. This model can be considered unreliable in terms of the SSI ecosystem.
2. It's segmented. It's not a trivial task to agree on the recognition of certification even between countries. So this model does not meet the needs of the fundamental principles of SSI — interoperability. Certificate authorities must be recognized by each other. This scheme is almost impossible due to the lack of intergovernmental integration mechanisms. It is highly unlikely that EU state authorities will recognize Blarizian or Chinese certificate authorities in the foreseeable future.
3. Certification is not costless because of the third parties involved. The costs of certification amendment rarely depend on market prices. Certificate authorities hold the position of natural monopoly and do not compete for the quality of certificate distribution services.
4. One entity needs to acquire a large number of certificates tied to one identity.[155]

[152] Ssh.com. n.d. (PKI) is a technology for authenticating users and devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents.

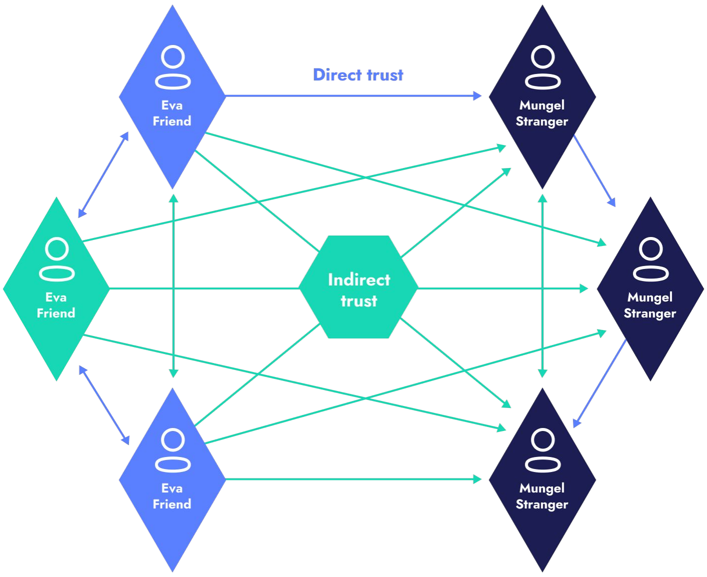
[153] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W., 2008. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Datatracker.ietf.org

[154] Windley, P., 2021. Comparing X.509 Vertificates with SSI. Windley.com

[155] Kravchenko, P., Skriabin, B. and Kurbatov, O., 2019. Engineer's Guide to Financial Internet. Distributed Lab. p 113

Decentralized governance model for SSI (web of trust, staking/slashing mechanisms)

Web of trust is an alternative way of authenticity confirmation opposite the centralized PKI+CA model. Originally the term "Web of trust" refers to a decentralized key validation system. Peer-to-peer digital certificates are created by individuals who know each other directly and therefore can sign each other's public keys.[156]



Although this model was introduced several decades ago originally and was related to OpenPGP encryption, then the scope of the model has expanded greatly over the years. As stated in Rebranding the Web of Trust whitepaper, the concept can be expanded to the whole system of peer-to-peer trusted relations, not necessarily directly related to PKI: "some use it as a term to include self-sovereign identity authentication & verification, certificate validation, and reputation assessment." [157]In other words, in a wide sense, the "Web of trust" refers to the systems that are administered in a decentralized manner.
In the context of blockchain governance, staking is a part of the consensus mechanism used by blockchain networks to achieve mutual trust. It prevents validators from inappropriate behavior. Staking requires users to stake a sum of tokens or cryptocurrency to become a validator of the network. If a validator confirms malicious blocks, he may lose his stake.[158] That mechanism of partial or full stake removal is called slashing.

Generally, the staking + slashing model with its core idea of risking a certain value may become yet another decentralized governance mechanism for certain cases in the context of the SSI ecosystem, especially at layer 1 of the technical stack based on a distributed ledger.[159] In particular, as will be shown in the Par 5, token curated registries, which use staking for assurance purposes, may serve as on-chain lists of trusted issuers or verifiers.

General scheme of the staking mechanism

Before making a decision a staker deposits a certain value

In case of improper decision the stake is lost

If the decision is proper, stake is returned with additional reward

[156] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 177

[157] Appelcline, S., Newton, J., Farmer, R. and Crocker, D., 2021. Rebranding the Web of Trust, A White Paper from Rebooting the Web of Trust. Nbviewer.jupyter.org

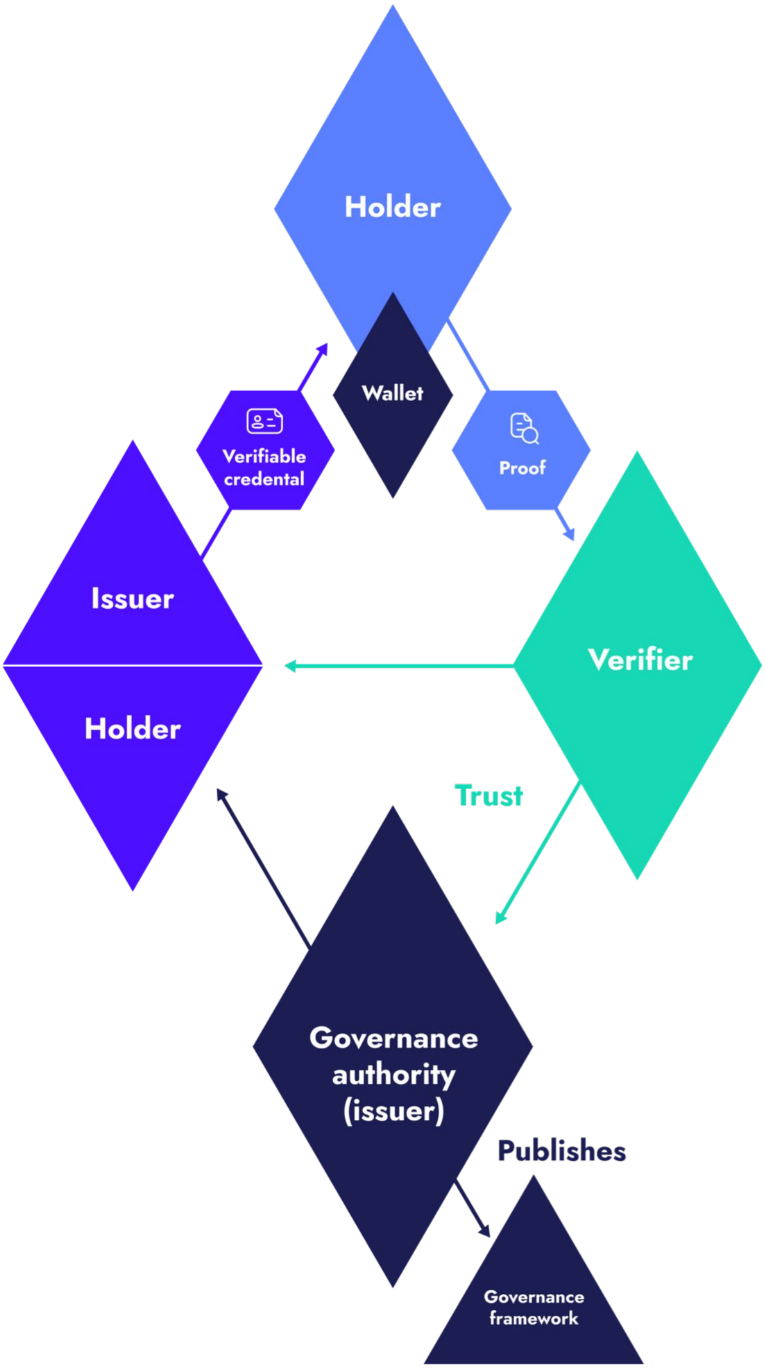
[158] Ethereum.org. 2021. Proof-of-stake (PoS)

[159] Gershuni, S., 2019. Paper: VC for decentralized assessment. Github.com.

Regulatory frameworks for SSI

Governance frameworks (also regulatory frameworks) are sets of rules, policies, and specifications designed to help solve a specific set of problems for a trust community.[160]

By establishing an appropriate regulatory ecosystem, governance frameworks enable SSI to spread widely on different scales, whether it's the level of organization, city, country, region, or even the whole Internet.[161] The relations with governance authority, issuers, and verifiers are always demonstrated using the governance trust triangle.



[160] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p 262

[161] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p 36

Regulatory frameworks for SSI

PCTF (Canada). (The Pan-Canadian Trust Framework), is a set of digital ID and authentication industry standards focused on economic benefits and designed to meet current and future Canadian innovation needs.[162] PCTF is declared to be valuable for a wide range of participants. People and organizations can feel more secure about the protection, disclosure, and use of their identity and personal information thanks to the PCTF. PCTF provides an opportunity for governments, institutions, and enterprises to deliver standardized, high-value, high-integrity services across states and the private sector.

The PCTF's mission is to allow and promote the creation of an innovative, resilient, and privacy-enhancing Canadian Digital Identity Ecosystem for all economic sectors, while also respecting fundamental human rights in the digital age. In this regard, the PCTF aims to ease the transition from conventional or sophisticated face-to-face contacts to digital interactions that position people at the center of the Digital Identity Ecosystem, while also acknowledging that analogue processes are likely to persist.[163]

ESSIF (EU). (European Self Sovereign Identity Framework). The European self-sovereign identity framework (ESSIF) is part of the European blockchain service infrastructure (EBSI) currently developed by the European Blockchain Partnership.[164] ESSIF's main intention is to build a general self-sovereign identity (SSI) system that allows people to construct and govern their own identity without depending on centralized authority across borders.[165] The goals of ESSIF are to:

1. Provide seamless cross-border services for citizens.
2. Make institutions more efficient.
3. Facilitate economic activity flow across borders.[166]

ESSIF aims to cover following issues:[167]

1. How to facilitate cross-border interaction with SSI.
2. How to make / keep national SSI projects interoperable.
3. How to integrate existing building blocks such as eIDAS, e-delivery with SSI.
4. How to conceptualize and build an identity layer in European Blockchain Services Infrastructure.
5. How to preserve European democratic values in the implementation of SSI.

[162] Diacc.ca. 2021. PCTF Overview.

[163] Diacc.ca. 2021. PCTF Overview.

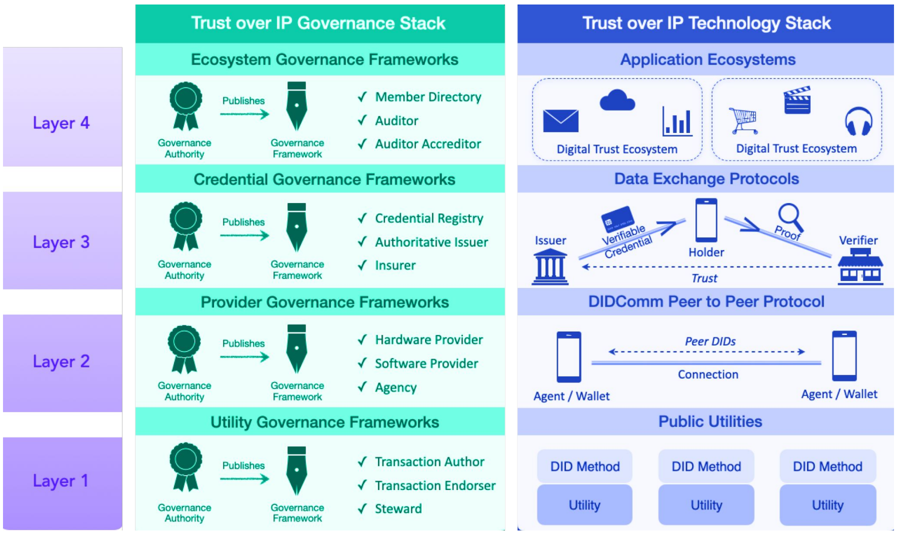
[164] Essif-lab.pages.gmet.gr. 2021. eSSIF-Lab Business Architecture.

[165] Medium.com. 2020. eSSIF: The European self-sovereign identity framework.

[166] Medium.com. 2020. eSSIF: The European self-sovereign identity framework.

[167] Du Seuil, D., 2021. European Self Sovereign identity framework. Eesc.europa.eu.

Introduction to the Trust over IP concept



Trust over IP is a complete architecture for Internet-scale digital trust that combines both cryptographic trust at the machine layer and human trust at the business, legal, and social layers.[168] This concept is currently being developed by the Trust over IP Foundation. "Trust over IP stack is aimed at key issues experienced by any entity involved in digital communications and commerce today: password fatigue, form fatigue, customer onboarding, KYC, secure messaging, data portability, business process automation, privacy management, supply chain provenance, GDPR compliance."[169]

As described in Trust over IP Foundation Whitepape[r170], the whole Trust over IP ecosystem is organized into a four-layer dual-stack model. The first two layers refer to so-called technical (or cryptographical) trust. Layer 3 and Layer 4 are those where human trust is achieved.

The core idea is based on placing governance stack in the first place in this dual-stack model: "implementing ToIP-based solutions should begin with business requirements, then move to policy requirements transparently communicated in governance frameworks. Only then should you choose the technology components required to implement those policies".[171]

Governance frameworks affect all four layers[172] of Trust over IP technical stack:

1. L4. On this layer, the governance framework regulates data exchange between apps, sites, and businesses while providing a consistent user experience of security, privacy, and data protection across the ecosystem. Governance frameworks could also replace company-specific privacy policies being openly developed uniform solutions preapproved by regulators.[173]
2. L3. Governance frameworks specify VC issuance rules, terms and conditions to which holders/verifiers must agree to obtain/verify credentials. Governance frameworks can also specify business models for credential exchange.
3. L2. Special security, privacy, portability, and auditing requirements may be established in relation to VC agents and wallets.[174]
4. L1. Governance frameworks specify design, code, test, and certification rules applied to verifiable data registries.

[168] Trustoverip.org. Trust Over IP. 2021. Trust Over IP - Defining a complete architecture for Internet-scale digital trust.

[169] Glaude, M., 2021. About Trust Over IP — A Comprehensive Resource Page. Northernblock.io.

[170] Trustoverip.org. 2020. Introducing the Trust over IP Foundation V1.

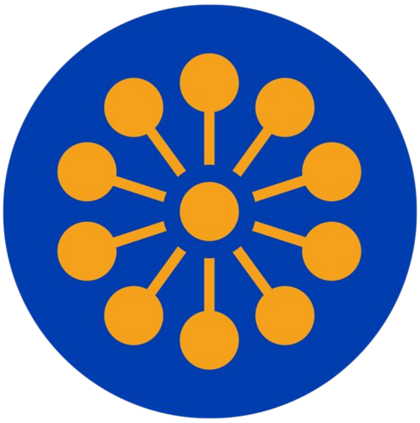
[171] Trustoverip.org. Trust Over IP. 2021. Trust Over IP - Defining a complete architecture for Internet-scale digital trust.

[172] Trustoverip.org. 2020. Introducing the Trust over IP Foundation V1. p. 19-22

[173] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p. 79

[174] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p. 213

Sovrin



The term ‘Sovrin’ most commonly refers to the Sovrin Network — a decentralized public permissioned network that enables self-sovereign identity on the Internet.[175] The purpose of the Sovrin Network is to enable a decentralized global web of trust.[176] Sovrin Network is a public blockchain available for everyone to make transactions. But unlike permissionless blockchains, Sovrin only allows trusted entities to run the network of validator nodes that achieve consensus of the transactions on the ledger.[177]

The Sovrin Governance Framework (SGF) is the legal foundation of the Sovrin Network as a global public utility for self-sovereign identity. It is developed by the Sovrin Governance Framework Working Group (SGFWG).[178] The purpose of SGF is to define the business, legal, and technical policies for the Sovrin Web of Trust, thereby providing a foundational layer upon which Domain-Specific Governance Frameworks (DSGFs) can be built.[179]

SGF principles

1. Self-Sovereignty
2. Guardianship
3. Openness and Interoperability
4. Accountability
5. Sustainability
6. Transparency
7. Collective Best Interest
8. Decentralization by Design
9. Inclusive by Design
10. Privacy by Design
11. Security by Design
12. Data Protection by Design and Default

Actually, SGF is represented by a set of documents that includes primary documents (Master document, Glossary), a number of legal agreements, and controlled documents — technical documents maintained and versioned either by the Sovrin Foundation or external standards bodies like W3C.[180]

[175] https://sovrin.org/faq/what-is-sovrin-2/

[176] Sovrin.org. 2019. Sovrin Governance Framework V2 Master Document V2. p. 4

[177] Sovrin.org. 2018. Is Sovrin ‘Permissioned’?

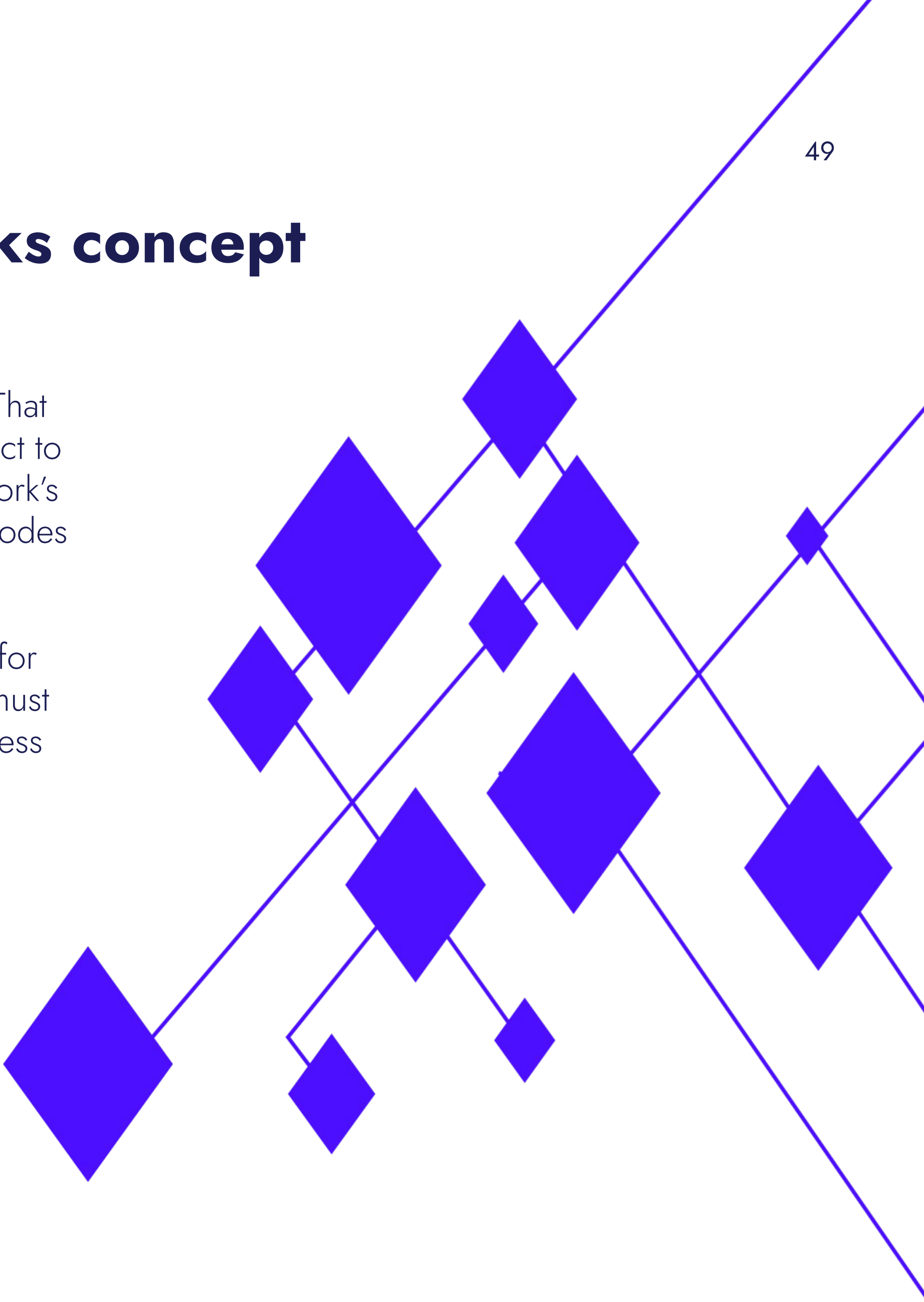
[178] Sovrin.org. 2021. Sovrin Governance Framework.

[179] Sovrin.org. 2019. Sovrin Governance Framework V2 Master Document V2. p. 6

[180] Sovrin.org. 2019. Sovrin Governance Framework V2 Master Document V2. p. 6

Network of networks concept

SSI seems to be a network technology. That means the whole SSI ecosystem is subject to Metcalfe's Law, which claims that a network's value is proportional to the number of nodes in the network. Thus, SSI value can't be realized at the level of a single small community or service. To open the way for widespread SSI adoption certain steps must be taken at both the technical and business layers.



At the technical layer emphasis should be made on increasing interoperability, Each layer of the SSI technical stack itself provides many non-trivial problems for ecosystem architects. But the bigger challenge is to make the whole ecosystem valuable via building bridges between its currently fragmented sections in order to enable credentials exchange across multiple networks and services. End-users at least should be able to:

1. Present verifiable credentials sourced from different networks in a single verifiable presentation
2. Exchange verifiable credentials data between networks

The Business layer is that which should be given even more attention at the start. Almost technically perfect system can be created, but it will have no value until somebody gives an initial boost to network effects.

To start moving towards universal dissemination SSI should propose a certain value for each kind of participant: holders, issuers, and verifiers. The latter two show mutual interest only when the identity data turnover is high enough. Only the keystone subjects have enough power to give initial bust to network effects. Thus, in particular SSI may be initially imposed by major players, like governments themselves, any weighty governance agencies as issuers and large organizations (like FAANG) as verifiers.

A typical journey for SSI users

Previous chapters of the paper introduced the reader to the philosophy and the actual algorithm of the SSI concept. In this section, the paper will guide the reader through the typical user journey from the point of view of potential use case scenarios.

Sean is a passionate cryptocurrency fan who wants to try his hand at trading on one of the major exchanges. The exchange is quite modern and cares about the security of its customers' data. Thus, all the processes which involve customers' authenticated data exchanges are built with the help of SSI. Sean still cannot imagine how fast and convenient it is. The registration flow is almost completely automated: Sean just has to press a few buttons. The process is following:

1. Sean already has a digital SSI wallet on his phone. Recently he has downloaded it and obtained his first verifiable credential — his ID, issued by the government. Sean can be sure of his data privacy and safety: during the setup, his wallet generated a pair of keys — public and private and these keys ensure that the entire data is cryptographically encrypted. The major advantage of asymmetric cryptography is increased data security: users are never obliged to divulge or exchange their private keys, reducing the likelihood of a cybercriminal finding a user's private key during data transmission.

2. When Sean starts the signup process, the exchange proposes an explanation that only traders with a particular degree of competence in order to utilize their services. Sean has two options from now on:
a) Provide a traditional economics/finance degree packaged in the form of VC, implying a certain amount of financial expertise.
b) Use a third-party service to obtain knowledge proof.

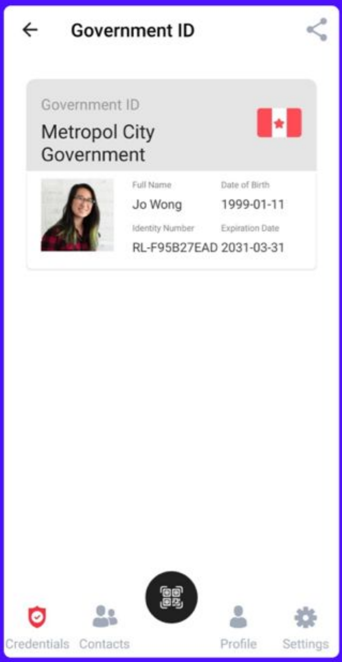
This alternative is predetermined by the exchange in a special structure called Presentation Definition, stored inside a blockchain so that Sean's wallet automatically recognizes and handles it.

3. As Sean doesn't have any special education, he chose the second variant. He discovers a third-party platform. Some identity data is required to complete the registration process. However, as SSI is based on the principle of data minimization and supports selective disclosure and derived predicate proofs, he does not have to reveal all of his personal information from his ID.

4. The platform offers a short study course. Finally, Sean completes a financial literacy test and, as a result, receives a fresh VC, confirming his competence, directly to his wallet.

5. Sean can now return to the exchange and quickly continue the registration process. As before, ID data and financial knowledge proof are required to pass the onboarding process. Sean just needs to accept or reject a share request, which his wallet received.

ID credential stored in Atala PRISM wallet

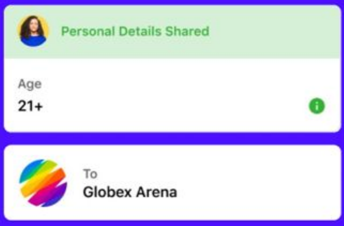


Government ID

Government ID
Metropol City Government

Full Name: Jo Wong
Date of Birth: 1999-01-11
Identity Number: RL-F95B27EAD
Expiration Date: 2031-03-31

Selective disclosure and ZKP in Civic wallet

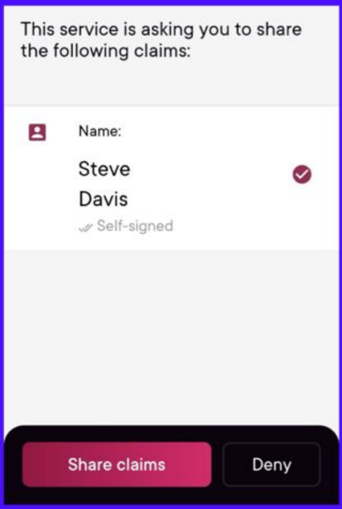


Personal Details Shared

Age
21+

To
Globex Arena

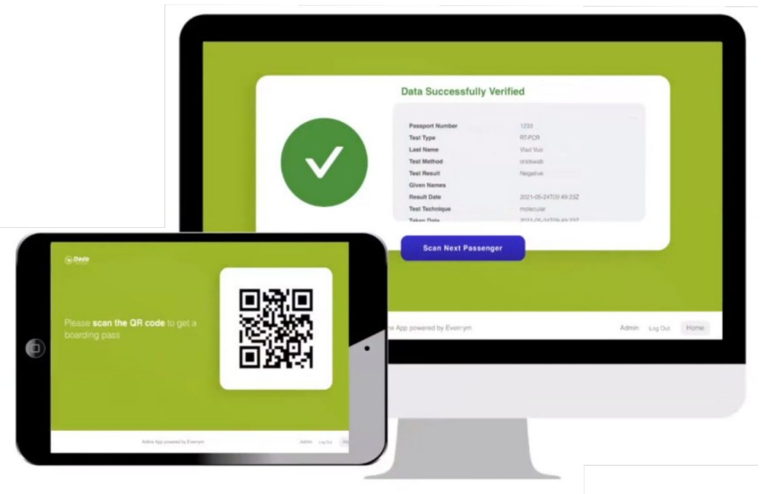
Identity data share request (Jolocom wallet)



This service is asking you to share the following claims:

Name:
Steve Davis
Self-signed

6. From the verifier's perspective, the process is not much more complicated. On that side, once Sean accepts the credentials provision, a Client Manager receives a corresponding notification in his software. The agent (the part of software responsible for SSI interactions) automatically gets the DIDs (unique identifiers) of the issuers from received credentials. Then, data needed for credentials recognition and verification (Issuers public keys, credentials schemas) is pulled up from the blockchain. The latter is performed automatically, without forcing the verifier to take unnecessary actions. And even more so, there is no need for direct contact with the issuer: without having to contact the Issuer, any Verifier confirming the validity of a digital document may rely on cryptographic verifications.



Data Successfully Verified

Passport Number	1233
Test Type	RT-PCR
Last Name	Vlad Vuo
Test Method	oralswab
Test Result	Negative
Given Names	
Result Date	2021-05-24T09:49:23Z
Test Technique	molecular

Please scan the QR code to get a boarding pass

7. As VC format is standardized in specifications and schemas, even checking its content for Sean's compliance with platform criteria (age, region, etc.) can be carried out automatically. It remains only to observe the list of green checkmarks signaling that everything is ok for the Client Manager.

8. Although the main work has already been done by the system itself, the Client Manager can still take a quick look at the results of the check to further make sure everything is alright. If everything is successful, a new investor gets access to the platform.

9. Sean from now can enjoy his trade.

As we see, each party from the considered case benefits from SSI technology. Sean obtains a fast, secure, and user-friendly onboarding process. Both verifiers gained a trusted way to check Sean's authenticated data. The process is almost completely automated: no need to request document scans and verify them manually, make video calls to verify identity, and deal with other exhausting procedures.

The next part will discuss how additional aspects of our daily life may benefit from SSI and some of the current SSI solutions on the market, including healthcare, education, job search, and finance.

Part 4

Business Opportunity for SSI

SSI value for the key actors

Being a complex phenomenon, SSI provides a certain value to its stakeholders. As we noted in Part 3, there are some specific roles in the SSI business process:

Value for the Holder

Another example holder is the one who derives the most benefit from the system. Although they may not be paid while holding the credentials or digital identities, this provides them with extra chances. Customers are already accustomed to paying for notarization services and would gladly switch to a new option that is less expensive, faster, or just easier. Self-issued credentials, such as VC-wrapped scans and PDF documents, are another but a very similar example. Sometimes the act of obtaining or acquiring credentials is less important than having a decentralized, data-rich, and portable identity.

Value for the Verifier

When the cost and speed of verifying information about the holder is a critical component of their business, the SSI system can help. The KYC process has a key role in a banking institution. SSI enables these companies to obtain verifiable and actionable information about their customers in a more timely and secure manner. That fact reduces operational costs.

Value for the Issuer

Issuers are the key data suppliers in the SSI ecosystem. Data collection, storing, and management can be costly and burdensome. In some cases, like in the field of public administration, such data does not carry a direct economic effect. This problem may be tackled by creating a system of economic incentivization for data providers. Holders or verifiers can transform their value chain and direct the money stream to the issuers. Thus issuers will be interested in providing better data packs for holders across the world. Data markets will become transparent and fair.

Value accrues to the Network

In pretty much every case where SSI is used instead of a centralized solution, there's also a network itself that benefits from the usage. We can think about accelerated network effects that will become more and more prominent once the critical mass of issuers and verifiers are connected. In this instance, the network maintenance or network owner — government or major enterprise — can subsidize the cost of running the SSI applications. To protect client privacy, Amazon may establish an SSI-enabled network among buyers and sellers.

SSI for various economic sectors

Healthcare: PCR tests, Vaccination Records, Medical Records, Insurance Claims

Healthcare data is private information, and healthcare individuals and companies seek maximum confidentiality to protect their data, and they are reluctant to allocate their data for non-clinical care purposes, and they prefer to have complete control over granting and suspending data access, as well as to be questioned before disclosing healthcare information. Electronic health (eHealth) is the use of information technologies to improve healthcare quality.[181] The goal of eHealth is to involve multiple clinics, various healthcare facilities, and departments in order to improve healthcare system management and provide efficient care services with a positive patient experience.[182]

The use of SSI in healthcare can greatly benefit the general population and vulnerable groups in particular. The COVID-19 pandemic was a catalyst that accelerated the process of boosting enterprises and governments to unite in advancing technology to solve the COVID-19 problems with traveling and carrying results of PCR tests, vaccination records, and so on. The COVID-19 pandemic highlighted the frailties of most of the world's health systems, even those of wealthy nations. These vulnerabilities heightened the possibility of restricting access to healthcare for swaths of the population and highlighted another facet of undocumented migrants' existence in the context of the health crisis.1[83] Having an identification can help illegal migrants get access to healthcare and other forms of assistance during the epidemic. It can also aid government efforts to limit the infection, such as by tracking and tracing. Blockchain-based apps can be used to give illegal migrants an identification that does not jeopardize their privacy or result in their detention. The ability to include information regarding a person's medical history increases the likelihood that these people will be able to get medical help. They may utilize an SSI to certify that they have been tested for COVID-19. This option may aid in the management of contamination and the avoidance of large-scale spreads throughout society.[184]

Persons can exercise their basic right to be remembered as a citizen and "visible" amid a calamity like the COVID-19 epidemic by using blockchain-based SSI solutions. The blockchain-based self-sovereign identification project's design is built on individuals acting as sovereign agents and the decentralization of the state system. Blockchain-based SSI can also have a positive impact on access to the services of NGOs. [185]

181

Cordeiro Domenech, M., Comunello, E. and Silva Wangham, M., 2014. Identity management in e-Health: A case study of web of things application using OpenID connect. 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom). Vigir.missouri.edu.

182

Bouras, M., Lu, Q., Zhang, F., Wan, Y., Zhang, T. and Ning, H., 2020. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors, 20(2), p.483.

183

Page, K., Venkataramani, M., Beyrer, C. and Polk, S., 2020. Undocumented U.S. Immigrants and Covid-19. New England Journal of Medicine, 382(21), Nejm.org.

184

Gans, R., Ubacht, J. and Janssen, M., 2020. Self-sovereign Identities for Fighting the Impact of COVID-19 Pandemic. Digital Government: Research and Practice, 2(2), Dl.adm.org.

185

Bouras, M., Lu, Q., Zhang, F., Wan, Y., Zhang, T. and Ning, H., 2020. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors, 20(2), p.483.

Blockchain, as publicly accessible ledgers, can improve the efficiency of all types of recordkeeping and give a solution to recordkeeping challenges in the healthcare business. Blockchain technology is being examined for the security of healthcare records, DNA data, personal information, and vital medical history data. In the healthcare system, SSI can be defined as a patient-centered framework that enhances medical information protection. A COVID-19 Credentials Initiative is one example (CCI), it is an open worldwide community founded on Verifiable Credentials (VCs), an open standard and new technology that might give a similar experience to the paper/physical credentials while providing special benefits, the most essential of which are privacy and tamper-evident.[186]

Individuals are also being granted digital certificates that allow them to show their health status and that they have recovered from the sickness. Such health passports, also known as Immunity Passports, might serve as verifiable documentation that individuals have acquired antibodies that they can provide, allowing them to return to their employment and other aspects of their lives.[187]

Mechanism: People sign up for a government-run blockchain, which will store and validate COVID 19-related data. Testing labs and hospitals must also be connected to the blockchain network so that all reports are automatically posted to the distributed ledger and cannot be changed later. When a person does the COVID-19 antibody test, the information is kept private via clever encryption. A token is created in that person's account with an expiry date based on the predicted age of antibodies. This implies that the tokens can only be confirmed for a limited period. This blockchain uses biometric authentication as a private key to prevent users from accessing each other's blockchain accounts.[188]

Contact tracing is also made easier when phone devices are linked to this blockchain via a person's account. For each person combination, the smart contract produces a unique key. When they come into touch, it adds the transaction, which is labeled with a geo-location and a timestamp. Any government/healthcare authority can only confirm whether or not the individual had contact with a COVID-19 patient. This blockchain system would reward individuals for interacting with persons who have COVID 19 immunity certificates rather than seeking infection.

It is critical to implement decentralized patient data and digital identity records in order to enable healthcare blockchain services. The initial goal driving the development of pure blockchain solutions is the elimination of intermediaries and the decentralization of power in order to achieve distributed trust.[189] Hyperchain announced the launch of its blockchain-based platform to fight against the coronavirus epidemic. It will serve as a medical supply donations portal to support hospitals in central China.[190]

[186] Covidcreds.org. 2021. COVID-19 Credentials initiative.

[187] Kumar Sharma, T., n.d. Widespread Adoption of Self-Sovereign Identity in the Wake of COVID-19. Blockchain-council.org.

[188] Bansal, A., Garg, C. and Padappayil, R., 2020. Optimizing the Implementation of COVID-19 "Immunity Certificates" Using Blockchain. Journal of Medical Systems, 44(9).

[189] Bouras, M., Lu, Q., Zhang, F., Wan, Y., Zhang, T. and Ning, H., 2020. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors, 20(2), p.483.

[190] Peng, T., 2020. Blockchain Charity Platform to Fight Against the Coronavirus Outbreak. Cointelegraph.com.

Through its identity model, Onfido creates "immunity passports." Credential providers can do this by verifying relevant information about a person or organization and issuing verifiable credentials to that person, allowing individuals to hold multiple digital credentials on their phone, and accepting or rejecting requests for information sharing with institutions.

This model is already being developed for public use; in May, Sidehide partnered with Onfido to demonstrate immunity to hotel bookings in the hopes of making people's travel safer.[191] One of the most active applications of SSI technology is the digitization of all medical documents based on an open standard. Such projects have become especially relevant against the background of the COVID-19 epidemic, but the technology makes it easier to interact not only with the results of tests but also with any other medical documents: medical books, vaccination cards, veterinary passports, any certificates, and extracts.

In addition to purely technical implementation, a sovereign digital identity requires changing an existing or creating an absolute new legal framework. The European Commission, the Government of Canada, and a number of non-profit associations have done a great job in this direction over the past few years.[192]

[191] Johns Hopkins Coronavirus Resource Center. 2020. COVID-19 Racial Data Transparency - Johns Hopkins Coronavirus Resource Center.

[192] Gershuni, S., 2020. Technologiya suverennoi lichnosti - rynok v million dollarov. VC.ru.

Government credentials: Passports, Digital IDs, Driving Licenses, Business Licenses

In June 2020, the first stage of a pilot commissioned by the US Department of Homeland Security (DHS) to develop a digital version of the resident card was completed. Many other countries are also considering using SSI technology to solve the problem of creating digital passports and identity cards. The program solves a number of tasks: from creating a digital identity for use in other government and commercial services to solving the problem of forgery of physical documents. During the first stage of the program, seven independent solutions were proposed, each of which automatically supports all the others (which was demonstrated during the interaction tests, interop testing) without requiring special integration.[193]

ESSIF is part of the European initiative for the development of advanced technologies, including the SSI and blockchain. The initiative creates regulation and a "gold standard" for the use of SSI as a digital notary, certification, and trusted data exchange. In addition to specific application cases, this initiative regulates the operation of SSI systems with eIDAS.

The California parliament has passed changes to the Civil Code, according to which VC is the standard for the release, storage, and verification of medical documents and, in particular, the results of testing for COVID-19.

The goal of the Pan-Canadian Trust Model is to move to a fully digital interaction of citizens, the state, and business in the country. It is a set of practices, regulations, and recommendations for system design that address the two main challenges that arise in the transition to a digital, decentralized trust model:

1. Digital identity and the hierarchy of such personalities. For example, how a digital record in a house book, a digital passport, and a bank account relate to each other, and what rights the owner of a particular type of record has.
2. Digital interaction. What type of atomic functions should be available to citizens and businesses.

Ultimately, the PCTF serves to empower Canadians by ensuring that a person's right to a digital identity cannot be compromised, that privacy and security remain critical, and that the spread of technology gives people convenience and choice from a variety of providers.

Kiva[194] is developing an identity protocol that will be rolled out across Sierra Leone, demonstrating the program's strength and the importance of providing vulnerable people with a digital identity system. Kiva is based on the previously mentioned DID and credentials model, with Hyperledger Indy as the underlying blockchain layer. Kiva will provide a DID and associated public/private key pair with signing identity claims to any Sierra Leone citizen who is qualified for a government-issued ID, as well as a first attestation from the Sierra Leone government (in the form of a verifiable credential comprising hashes of the citizen's biometrics and other government-issued identifiers).[195]

[193] Gershuni, S., 2020. Technologiya suverennoi lichnosti - rynok v million dollarov. VC.ru.

[194] Davie, M., 2021. Kiva's next frontier: Kiva Protocol. Kiva.org.

[195] Wang, F. and De Filippi, P., 2020. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain, 2.

Education: Degrees, Certificates, Transcripts, Examinations, Badges

The capabilities of self-sovereign identity technologies play an important role in the possible synergistic relationship between blockchain and education. The blockchain has been related to the unbundling of higher education[196] and, from a practical standpoint, with the fundamental building component of education, certification.
Credential definitions are typically connected with the evidence of authority, position, rights, eligibility to privileges, or the like, typically in written form.[197]

Digital diplomas and certificates based on the technology of SSI are issued by many universities around the world, including Russian ones. However, one of the leading non-profit organizations in this direction — the Digital Credentials Consortium, created on the basis of MIT and Harvard University-went further and set its task to standardize not only the technical format but also the data structure in relation to education specifically. This work is carried out on the basis of the IEEE — the largest association that is engaged in the standardization of technological standards in microelectronics and information systems.

Digital diplomas not only solve the problem of forgery and significantly reduce the cost of creating a single document — but they also allow you to combine data on competencies and qualifications obtained at different levels of education in a single profile. For example, in a single profile, the employer will be able to check the signed facts of obtaining a certificate and diploma, work experience, online courses, and participation in a conference. Each fact has an issuer and a legally significant signature, which helps to reduce the costs of employers when scoring and verifying facts from the applicant's resume.

According to Gallagher[198] the increasing digitalization of credentials signals a new era of increased openness for educational achievements, offering corporate executives with more and better data on which to base recruiting choices. Some authors express the view on digital credentials stating that higher education must do the shift to digital credentials using a standardized document format and data standard that institutions may employ to supplement or replace their conventional academic record. At the same time, higher education must accomplish all of this in a way that secures, maintains, and limits access to data while still making it portable, accessible, and actionable.[199]

In the last few years, the technology of digital credentials (digital certificates) has been gaining popularity. 8 years ago, the Mozilla Foundation started working on its own standard: Open badges. Customers of another company working in this direction — Credly are IBM, Dell, and Oracle.

The most active work is carried out on digital educational certificates. Why are they needed?

[196] Sood, I., Pirkkalainen, H. and Camilleri, A., 2020. Can Blockchain Technology Facilitate the Unbundling of Higher Education. Proceedings of the 12th International Conference on Computer Supported Education, Volume 2. Scitepress.org.

[197] Grech, A., Sood, I. and Ariño, L., 2021. Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. Frontiers in Blockchain, 4.

[198] Gallagher, S., 2019. How the Value of Educational Credentials Is and Isn't Changing. Hbr.org.

[199] Pittinsky, M., 2015. Credentialing in Higher Education: Current Challenges and Innovative Trends. Educause.edu.

1. Lack of opportunity to demonstrate all their skills to people who continue to study even in addition to academic programs.

2. The need to interact with the issuing organization to confirm the authenticity of the certificate, which can delay the process for weeks. How does it work? Thanks to the development of the blockchain in the last 3 years, the technology of digital certificates have started to develop much faster. The blockchain allows you to verify the authenticity of the certificate and its belonging to the student. Blockcerts was among the first open standards for creating, issuing, viewing, and verifying blockchain-based certificates. These digital records are registered on a blockchain, cryptographically signed, tamper-proof, and shareable. The goal is to enable a wave of innovation that gives individuals the capacity to possess and share their own official records[200.] Blockcerts was designed from the start to promote a set of common standards for blockchain certification, from which interoperability would develop.[201] Here's how it works with Blockcerts, one of the digital certificate standards being developed at MIT:

a) Basic information such as the name of the recipient, the name of the certifying organization and the date of issue is stored in an electronic file in the format of the Open Badges standard. This file is cryptographically signed with a private key that only the issuing party has.

b) The hash can be used to verify the authenticity of the document. There is only a single hash combination to the original file. Changing it will change the hash.

c) The electronic certificate itself can be stored on a hard disk or in a mobile wallet, from where it can be shared with others or printed out. The data required for identity verification is stored in the blockchain. So you can combine certificates from different educational institutions, which allows you to build a path of lifelong learning.

Reputation: Portable community reputation, Certificates of participation, Awards

Trust metrics are often used to assess recommendation and reputation-based trust frameworks. Such metrics are derived utilizing trust data that is collected and pooled in the form of recommendations or reputations declared by other entities.[203] SSI holds great promise and could be a game-changer for reliable reputation management systems in this blockchain and decentralized world. Digital Self-Sovereignty solutions enable individuals to receive official records that they entirely control, with no ongoing reliance on a vendor for viewing, sharing, or confirming these records.

[200] Blockcerts. 2021. Blockchain Credentials.

[201] Grech, A., Sood, I. and Ariño, L., 2021. Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. Frontiers in Blockchain, 4.

[203] Schanzenbach, M., 2020. Towards Self-sovereign, Decentralized Personal Data Sharing and Identity Management. Mediatum.ub.tum.de.

Finance: KYC, AML reports, bank statements, NFT authorship proofs

Banks are subject to plenty of legal regulatory frameworks which centered on determining who their clients are — Anti-Money Laundering (AML) and Anti-Terrorism Financing (ATF) (ATF). The Financial Action Task Force (FATF) enforces global compliance, and the cost of doing all necessary inspections is rather significant.[204]

Some current technologies are combined in a novel way to enable indefinitely scaled low-cost federation, resulting in SSI technology. Smartphones, PKI, DLTs, and personal cloud computing are examples of these technologies. The digital versions of credentials function in the same way as the paper and plastic papers that people keep in their wallets. Individuals who deliver paper documents do not 'phone home' to the issuers, and they carry them in their digital wallets.[205] As a result, when a financial institution asks for information, the user has the option to accept or refuse requests to disclose data from their phone.

FinID is a project established by CPqD, one of Latin America's leading telecommunications research and development institutions, that employs the notion of decentralized digital identification. The FinID project seeks to provide a decentralized financial identity management system that includes identity generation and administration, digital account accreditation (called onboarding), and authentication of financial identities.[206]

The use of decentralized digital identification of this kind may enable and ease the implementation of the Know Your Customer concept because financial entities will be able to directly

Enable the implementation of the Know Your Customer concept. Because financial institutions will be able to directly query verifiable credentials authorized by other institutions — whether financial or not — through FinID solutions, they will also be capable of assessing the ownership, issuer, and authenticity of the information by having access to appropriate documentation from each of your clients.

A blockchain-based model provides a feature by using uPort as middleware. When banks or other institutions want to use the data of a consumer, they must request permission from the consumer. When banks or other institutions want to use a consumer's data, they must first obtain permission from the consumer. Instead of granting administrative third-party tracking access or granting these sensitive credentials to show their credentials instead of revealing detailed personal information, the blockchain based model empowers users to control their own identities. [207]

[204] Ciobanu, M., 2020. The potential of Self-Sovereign Identity to reduce the growing regulatory burden. Thepaypers.com.

[205] Ciobanu, M., 2020. The potential of Self-Sovereign Identity to reduce the growing regulatory burden. Thepaypers.com.

[206] Vieira, F., 2020. Educação Ambiental para além da pandemia: aprendizados decoloniais com outras comunidades e com outras pedagogias. Revista Brasileira de Educação Ambiental (RevBEA), 15(4), pp.259-278.

[207] Dong, C., Wang, Z., Chen, S. and Xiang, Y., 2020. BBM: A Blockchain-Based Model for Open Banking via Self-sovereign Identity. Blockchain – ICBC 2020, pp.61-75.

Workplace: employment records, references, invoices, access management credentials

Europass, a pan-European resume system, is preparing to switch to SSI-based verifiable digital documents. More than 100 million residents of the European Union will have the opportunity to create a verifiable resume with automatic consideration of all sources of education, all possible languages, and a detailed competence model.

The Velocity Network project, which is a non-profit partnership of the largest employers in the field of IT, allows not only Europeans but also citizens of any country to create a verifiable and provable resume with work experience, additional education, and evaluation of results. More than 20 IT corporations have already joined the project, including Oracle, SAP, IBM, Microsoft, and Workday.

Existing solutions

Evernym

Evernym was founded in 2013 to solve the digital identity crisis. We envisioned a world where consumers are in complete control of their digital identity, where privacy is a basic human right, and where consumers and organizations can foster a new relationship rooted in trust.

MATTR

Decentralized identity and verifiable data present a new way to solve and restore trust in digital interactions. MATTR products provide the building blocks to solve and remove the historical challenges of digital security, privacy and data verification, opening up a new world of trust.

Microsoft

Evernym was founded in 2013 to solve the digital identity crisis. We envisioned a world where consumers are in complete control of their digital identity, where privacy is a basic human right, and where consumers and organizations can foster a new relationship rooted in trust.[208]

IBM

Cloud identity and access management (IAM) solutions. IBM Blockchain Platform, the leading blockchain open source for business — interoperable and available anywhere for enterprises and entrepreneurs.[209]

Affinidi

Affinidi is founded by Temasek, a global investment firm headquartered in Singapore. Affinidi is building technology solutions as well as two applications, GoodWorker and Trustana, to promote the growth of a Self-Sovereign Identity-enabled ecosystem

Trustana is a curated B2B marketplace and trade platform connecting verifiable, international partners for seamless cross-border trade. GoodWorker is a digital job matching platform for blue-collar workers and employers in India.[210]

uPort/Veramo

When uPort began at ConsenSys in 2015, the self-sovereign identity space was also in its infancy. Early concepts existed as little more than academic theories with few attempts at implementation. Despite the lack of standards or the guidance of a marketplace, uPort began experimenting with our first architecture using smart-contract based identities.

Over time the technical limitations with on-chain identities began to pile up, which led to uPort's 1.0 architecture and pioneering the use of decentralized identifiers (DIDs) with our open-source libraries. At the time, DIDs, together with verifiable credentials (VCs), were proposed W3C standards and are now nearing official status. Dozens of projects are still using several of our popular libraries: uport-connect, uport-credentials, uport-mobile, did-jwt, and did-resolver, to name a few.

[208] Identity.foundation. 2021. Identity.foundation. n.d. ION - an open, public, permissionless decentralized identifier network.

[209] Ibm.com. 2021. IBM Blockchain Platform - IBM Blockchain.

[210] Affinidi.com. 2021. About us.

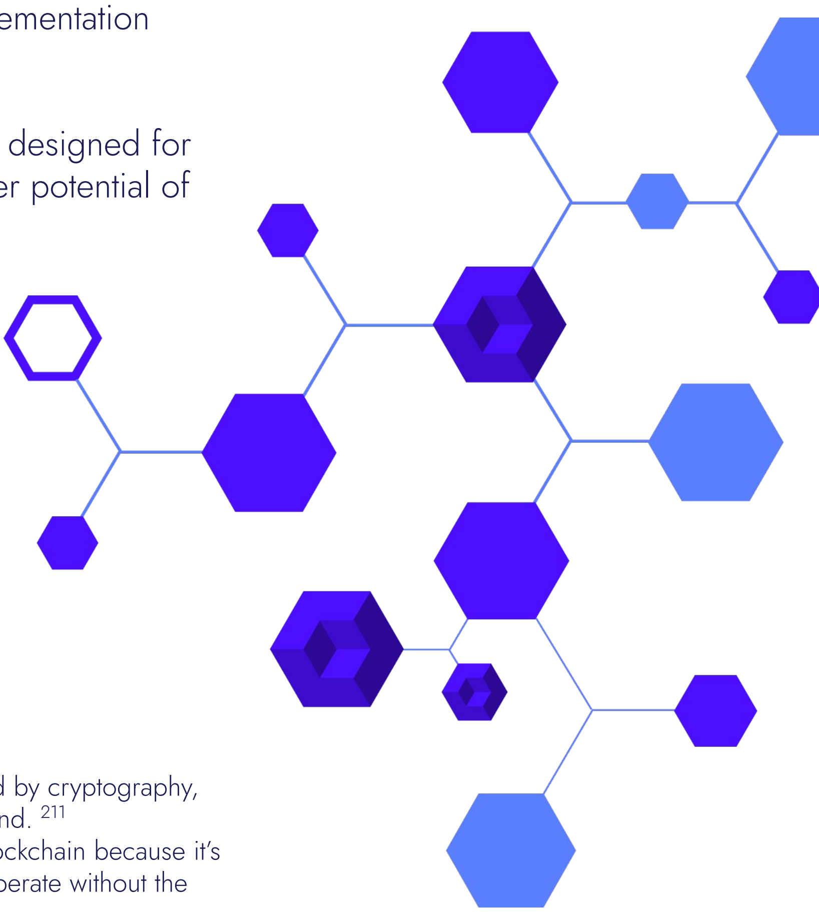
Part 5.

Blockchain Technology and the SSI Ecosystem

The current situation in the context of a blockchain ecosystem

Blockchain systems play a significant role in the SSI ecosystem, being a single point of truth that every participant of VC turnover should trust. Moreover, it was the DLT technology that gave the initial impetus to the SSI practical implementation attempts.

Although the blockchain concept was originally designed for Bitcoin cryptocurrency, currently, it has the wider potential of being used in a variety of other spheres



SSI and cryptocurrencies

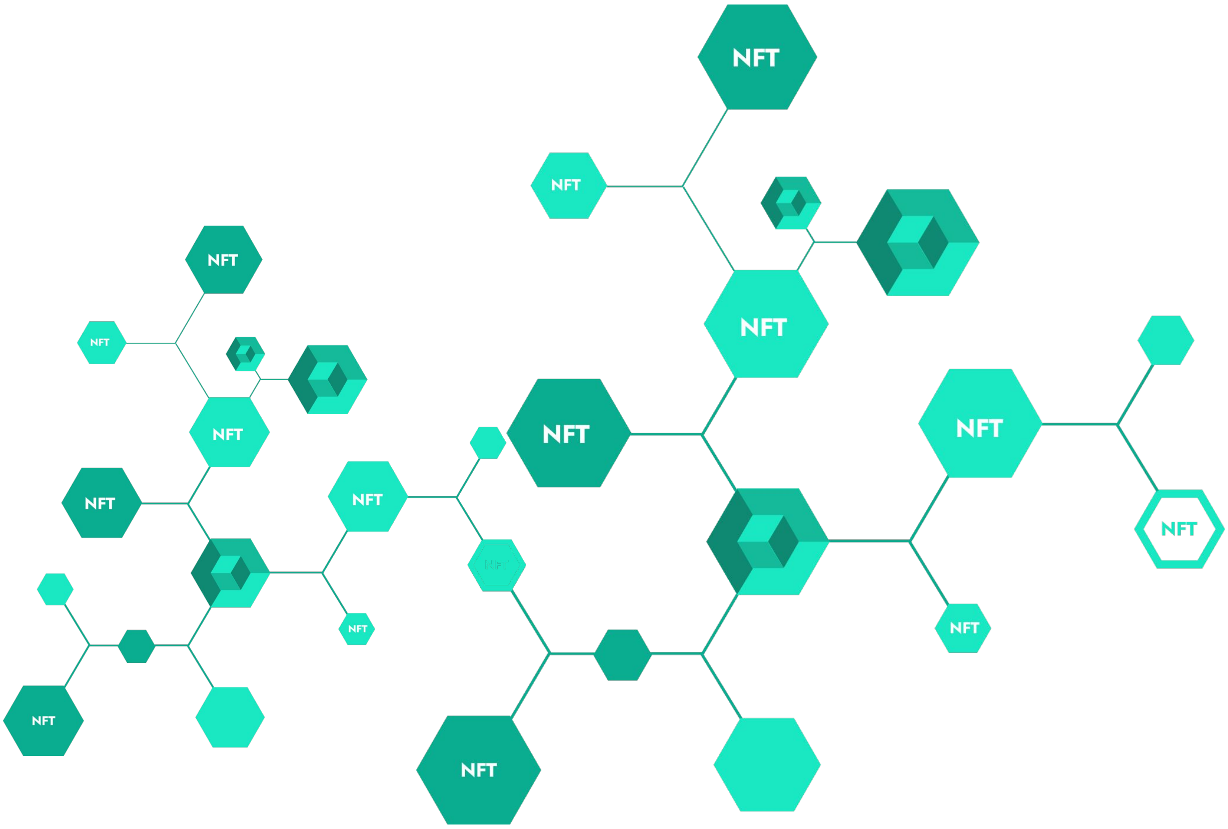
A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. [211] Cryptocurrency is the most commonly known use case for blockchain because it's the blockchain technology that enables cryptocurrencies to operate without the need for a central money issuance authority.

Cryptocurrency, being a digital cash, performs store of value and measure of exchange functions. But in our real lives, that exchange almost never happens by itself without the exchange of corresponding authenticated data. Additionally, cryptocurrencies are usually anonymous or pseudonymous by design. Therefore, the activity of exchange service providers is the subject of strict regulatory oversight. The synergy of SSI and cryptocurrencies may significantly change the landscape of online payments making them more secure and continuous, replacing the necessity of filing huge forms and scanning documents with one-click VC provision. Today online payments are often accompanied by two processes: registration providing identity information and direct payments.[212] SSI can improve user experience here by merging these two processes into one, fast and safe. Cryptocurrency key pairs may be used as a tool for DID signing or even be included in the VC data structure.

[211] Frankenfield, J., 2021. Cryptocurrency. Investopedia.

[212] Barclaycard.co.uk. n.d. SSI impact on payments. Barclaycard Business.

SSI and non-fungible tokens (NFTs)



A NFT is a unit of data stored in a blockchain that certifies digital crypto assets to be unique and therefore not interchangeable: nobody can modify the record of ownership or copy/paste a new NFT.[213] Currently, a standard interface for non-fungible tokens is ERC-721.[214]

Currently, NFTs are used to tokenize a variety of things like music, photos, arts replicating into the digital area their properties from the real world like scarcity, uniqueness, and proof of ownership. In theory, the scope of NTFs usage can be expanded to any unique things when provable ownership is needed.[215]

NFT's ability to identify digital assets gave rise to a hypothesis that they can serve the same functions as VCs currently do in the SSI ecosystem. Although they have much in common, there are some differences. Firstly, a VC is strongly tied to the identity via cryptographic mechanisms: that proceed from its purpose and technical implementation. In contrast, NFTs are tied to the asset but not to the owner. Therefore, generally, to anchor the uniqueness of NFT it's enough to deploy on a blockchain with a timestamp. Secondly, NFTs can be easily transferred between the owners, while VCs cannot. VCs reflect the properties of a particular subject. And thirdly, NFTs technical implementation relies on DLT technologies only, while identity data documented by verifiable credentials, on the contrary, in many cases, should be stored off-chain for privacy and performance reasons.[216]

And yet, there is a point where NFTs and VCs can meet each other. One of the core NFT problems is the lack of an identity layer. It is nothing more than a token represented in the blockchain. SSI can solve this issue by binding NFT to the owner via a set of VC. The next owner, in turn, can ensure that NFT originates from definitely the right identity if it's important for some reason (f.e. when NFT is bought from a celebrity).[217]

[213] ethereum.org. 2020. Non-fungible tokens (NFT) | ethereum.org.

[214] Entriken, W., Sachs, N., Shirley, D. and Evans, J., 2021. EIP-721: ERC-721 Non-Fungible Token Standard. Ethereum Improvement Proposals.

[215] ethereum.org. 2020. Non-fungible tokens (NFT) | ethereum.org.

[216] Medium. 2021. Non-Fungible Tokens (NFTs) vs Verifiable Credentials (VCs).

[217] Tanner, J. and Roeloefs, C., 2021. NFTs and the need for Self-Sovereign Identity — Gimly Blockchain Projects.

SSI and decentralized finance (DeFi)

In simple words, DeFi is "a system by which financial products become available on a public decentralized blockchain network, making them open to anyone to use, rather than going through middlemen like banks or brokerages." [218]

DeFi aims to remove intermediaries from financial relations. The traditional financial institutions are centralized. That means that all the financial transactions are under the control of certain centralized bodies like banks or governments. DeFi significantly changes this situation. The fundamental basis for DeFi is blockchain which makes it possible for parties to set either peer-to-peer or software-based middleman connections instead of relying on centralized bodies. Smart contracts are used to automate agreement terms making transactions more secure and transparent.

DeFi services are relatively a new phenomenon. However, they are gradually falling under the scope of conventional legal regulation. Hence, in particular, services may be forced to establish customer identification and KYC/AML procedures applied to traditional fintech products. The decentralized and independent nature of both DeFi and SSI ecosystems will complement each other here, providing a brilliant user experience to end consumers.

[218] Investopedia. 2021. Decentralized Finance (DeFi) Definition and Use Cases.

Identity is still fragmented across blockchains

Unlike other layers of SSI stack, the L1 blockchain is neither single nor standardized. Nowadays plenty of solutions exist from common like Ethereum to special-purpose and more focused on identity like Sovrin, KILT. It's difficult to imagine that there will be a single solution — one network — for all the entities across the world. Therefore, a focus should be made on establishing cross-chain communication mechanisms in a scalable and interoperable way. A credential exchange between networks seems to be a huge challenge next.

Interoperability between layer 1 is possible, but it's not free and not always available. Following solutions are available currently for this purpose:

1. Blockchain bridges. A blockchain bridge provides cross-chain interoperability, enabling transfer of tokens between two networks, even significantly different. Can be either decentralized or centralized. [219]

2. Cosmos. Cosmos defines itself as "The Internet of Blockchains." [220] It's a decentralized network of independent parallel blockchains. Each blockchain of the network can be connected to another one through the Cosmos Hub (acts like a router in TCP/IP networks) via the Inter-Blockchain Communication protocol (IBC). That architecture sets the conditions for the development of scalable and interoperable ecosystems with high performance (no need to perform all the transactions in a single ledger and, therefore, performance increased).

3. Polkadot Parachains. According to the Polkadot Wiki, Parachains are individual layer-1 blockchains that run in parallel on Polkadot, connected to the Polkadot Relay Chain, and secured by the Relay Chain's validator set. Being extremely flexible and customizable for specific use-cases, they seem to be the key element in Polkadot's multichain architecture that allows cross-chain transition not only of the tokens but of any type of data and asset. Parachains may also establish their own economies with their own native tokens.

4. Pairwise encrypted channels via DIDcomm. As DIDcomm is designed to be maximally interoperable and transport-agnostic, it works across different platforms and operating systems, networks (including blockchains), vendors, legal jurisdictions, hardware, etc.[221] Thus, an encrypted channel between DIDs placed in different chains may be established.

It is no doubt that interoperability between blockchains is essential for digital trust ecosystems. But this is true the other way too: SSI itself may increase blockchain value and adoption. Interoperability between multiple networks is provided not at the L1 but at that higher layer where the VC exchange performs. Properly designed, verifiable presentation exchange protocol will support VC combinations no matter which ledger it belongs to or whether it belongs to any at all. Practically, it means that one can create a VP containing his ID credential from his personal secured storage, a vaccination certificate issued with KILT blockchain, and provide them when presenting an Ethereum-based plane ticket before boarding the flight. As in SSI, all technical layers are built on top of open standards, and data exchange is virtually free among multiple networks, trust domains, and jurisdictions.

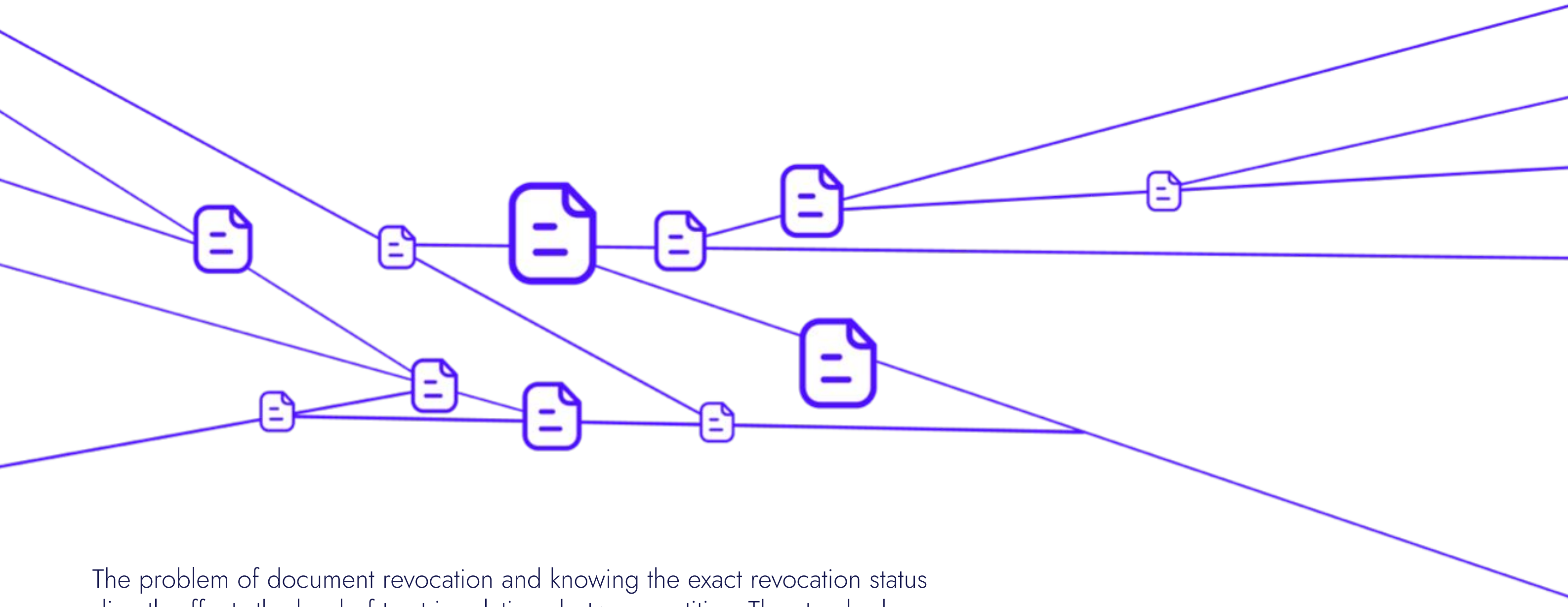
[219] Maker Blog. 2021. What Are Blockchain Bridges, and Why are they Important for DeFi?

[220] Maker Blog. 2021. What Are Blockchain Bridges, and Why are they Important for DeFi?

[221] Identity.foundation. 2021. DIDComm Messaging Specification.

How blockchain technology can foster the development of SSI

Revocation in a decentralized public manner



The problem of document revocation and knowing the exact revocation status directly affects the level of trust in relations between entities. The standard objective criterion that determines the revocation status of a document is its expiration date. Being included in a document as one of the fields, it can be easily checked later by the verifier. However, in cases of unpredictable and unexpected revocation of a document in conventional systems, there are only a few options to check its status. The Verifier will never be absolutely sure that a document is not revoked until he contacts the issuer and checks the status or unless there is a special registry that is 1) enforced to be updated on time 2) available to all interested verifiers. With the conventional system of document flow, only the first, rather impractical way option seems viable. The way of maintaining a centralized source of truth here inherits all those drawbacks that are typical for centralized systems as a whole and are described in Part 1.

The SSI ecosystem with a blockchain can solve the specified issue. As a verifiable data registry that serves as a source of truth for all the entities involved in VC turnover — issuers, holders, and verifiers, a blockchain can also be used to store a VC revocation registry. When a verifiable credential has to be revoked, the issuer will simply update this registry by writing a transaction to the ledger so that there is no need for direct communication of issuers and verifiers.

It's noted that a revocation registry inside VDR with ZKP cryptography support should be used in order to guarantee the privacy and prevent data leaks.[222]

[222] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p 123

Non-custodial key rotation

Both conventional PKI+CA and Web of Trust models described in Part 3 require trusted third parties. With the help of blockchain as a verifiable data registry and DID as the core identifier in the SSI ecosystem, a new, decentralized key management approach comes. Instead of binding an existing identifier to a public key, the DID is generated on the base of this public key. [223]

One of the fundamental security features of key management systems is key rotation. Key rotation means replacing an old public/private key pair by generating a new one. Firstly, a public key-based DID is generated. Then a DID document containing DID and the public key is published to a blockchain. When the key is to be rotated, the DID owner creates an updated DID document and signs it with the previous private key. This chain of trust between DID documents can be traced back through any number of updates to the original DID document with the original public key-based DID. So that non-custodial, i.e., non-dependent from any other side, key rotation becomes available.

Decentralized Key Management Service (DKMS) is an approach to cryptographic key management intended for use with blockchain. Developed by Evernym Inc. under a contract with the U.S. Department of Homeland Security Science & Technology Directorate. The initial and global root of trust for all participants is a distributed ledger, so there is no need for any certifying authorities or other third parties: "DKMS uses the security, immutability, availability, and resiliency properties of distributed ledgers to provide highly scalable key distribution, verification, and recovery." [224]

[223] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p. 176 – 178

[224] GitHub. 2021. sovrin-foundation/protocol.

Limitations of blockchain technology in the context of SSI implementation

On-chain identity issues

It is worth noting that implementing an SSI system on a blockchain remains a technical challenge. Because of the decentralized nature of blockchain, any transaction data is visible to all the participants. The immutability of the ledger makes the enforcement of legal measures such as the "right to be forgotten" particularly difficult. As underlined in the EU Blockchain Observatory and Forum report dedicated to Blockchain and Digital Identity, SSI implementations should aim to minimize the data irrevocably stored on the blockchain.[225]

Therefore, not all identity data should be stored "on-chain." However, not only the privacy considerations make us move identity data out of chain:

1. Storing all the identities data inside the ledger makes it significantly grow in size.
2. On a large scale, It may take a long time before a transaction is validated.
3. "On-chain" transactions have a certain value. The higher the transaction volume, the bigger the transaction costs.[226]

SSI ecosystem, which aims to cover a variety of relations, all these drawbacks do not allow relying only on "on-chain" transactions. However, it's possible to store certain data somewhere outside of the ledger and link it to the blockchain if necessary (off-chain identity). This identity data can be linked to the blockchain via DIDs and revealed only when requested using peer-to-peer methods.[227] However, this approach is technically more complex and has its own issues:

1. Interactions with a blockchain are more complicated.
2. There are privacy issues as entity personal data is linked to a data structure inside a blockchain.
3. Bigger transaction fee size because of the increased size of a signed transaction.
4. Key management becomes complicated.[228]

[225] Eublockchainforum.eu. 2020. BLOCKCHAIN FOR GOVERNMENT AND PUBLIC SERVICES p. 19

[226] Investopedia. 2021. What are on-chain transactions?

[227] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p. 430

[228] Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.p. 430

Performance and scalability

The issues of performance and scalability were inherent in the blockchain from the very beginning. These aspects directly affect technology adoption, especially SSI, which potentially generates multiple thousands of transactions per second.[229]

Depending on the approach, from three to five generations of the blockchain are distinguished today. .[230] [231]

The first generation was originally designed as a revolutionary method of value transfer without centralized financial institutions. The most commonly known example Bitcoin network received such popularity that it is now mainly associated with the word "blockchain" in the minds of ordinary users. That was a single-chain solution based on Proof-of-Work (PoW) consensus algorithm with no smart-contracts support and low capacity, but it was enough at that time to revolutionize payments networks.

The second generation of blockchains gave the world a new phenomenon — a smart contract. Along with the function of storing an immutable sequential chain of blocks, the blockchain has become an environment for the execution of a certain kind of Turing complete computer program. Ethereum with smart contracts has given impetus to the emergence of new decentralized phenomena, expanding the scope of blockchain, previously focused only on cryptocurrencies: DeFI, DAOs owe their appearance to smart contracts. Although these technologies became a breakthrough, there is still a missing link to widespread adoption — in particular, Ethereum, in its original form, supports handling of about 30 transactions per second.[232]

The third generation (Polkadot, Cosmos, Ethereum 2.0) is focused on solving performance and scaling problems using the multichain concept, which supports significantly more transactions per second but at the cost of increased technical complexity. PoW consensus algorithm, energetically inefficient on large scales, is replaced by the Proof-of-Stake one.

With the launch of FreeTON in May 2020 we can talk about the birth of another blockchain generation. As the developers declare, FreeTON is fast and scalable enough to be capable of handling millions of transactions per second simultaneously. Having all the key features of bottom generations (smart contracts, PoS, multichain architecture), FreeTON adds to them new ones, such as sharding mechanism and tightly-coupled mutlichain architecture.

[229] Medium. 2019. The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed.

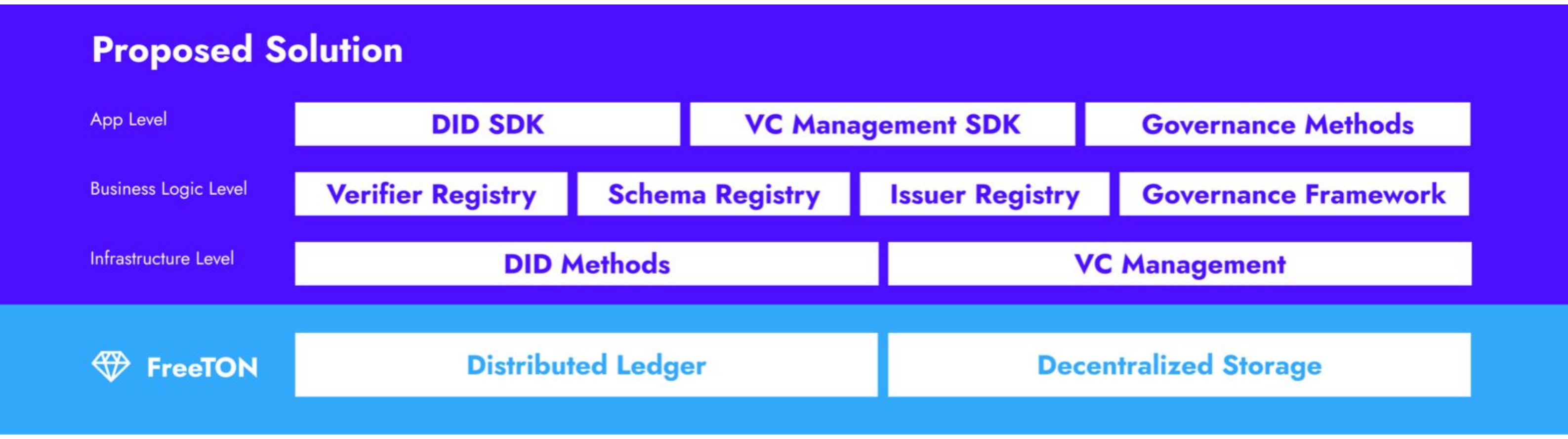
[230] Ledger. 2021. The Blockchain Generations | Ledger.

[231] En.freeton.wiki. 2021. Comparison to other blockchain projects - Free TON Wiki.

[232] Conway, L., 2021. Ethereum 2.0: What You Need To Know. The Street Crypto: Bitcoin and cryptocurrency news, advice, analysis and more.

Developing SSI ecosystem on the basis of L1 blockchain systems

What is the necessary infrastructure for blockchains to have to enable SSI apps?



Proposed Solution

App Level: DID SDK | VC Management SDK | Governance Methods

Business Logic Level: Verifier Registry | Schema Registry | Issuer Registry | Governance Framework

Infrastructure Level: DID Methods | VC Management

FreeTON: Distributed Ledger | Decentralized Storage

DID Method. As stated in the previous Part, plenty — either blockchain-based or not — DID methods are available at the moment. It seems that both p2p and blockchain-based methods will be suitable in the SSI infrastructure. The latter being anchored to the ledger enables decentralized self-sovereign key management systems to operate.

Verifiable data registry. As described in Part 3, a verifiable data registry is a significant part of the whole SSI infrastructure. Blockchains at this layer are not the only option — but one of the most suitable because of their core properties:

1. **Immutability**. Immutability means "the ability for a blockchain ledger to remain a permanent, indelible, and unalterable history of transactions."[233] Blockchain, as its name suggests, is a chain of data blocks. Those blocks consist of sets of timestamped transactions and are cryptographically secured by a hashing process: each block contains the hash of a previous one. That makes all the chain of blocks tamper-evident and tamper-resistant. Once a piece of data changes, the corresponding hash is changed too. Therefore, the improper transaction will be rejected. Immutability determines data integrity, which is important in the context of VDR, where such critical data as public keys or identifiers is stored.
2. **Continuous availability**. Unlike centralized storage, blockchain is a distributed network of multiple nodes connected to each other and keeping in sync constantly. Blockchain node stores transaction history or its' part. Since there are typically hundreds and thousands of running nodes, a blockchain network is resistant to outages and infrastructure attacks: even if a significant part of notes become offline, others will keep all the data. That property is critical for VDR as its data should also be publically available and resolvable.[234]

[233] Doubleday, K., 2018. Blockchain Immutability—Why does it matter?. Medium.

[234] S., J., 2018. Blockchain: What are nodes and masternodes? Medium.

Revocation registry. Distributed ledger technologies allow to set up of a non-custodial decentralized VC revocation registry. As revocation lists should be publicly available to be available for verifiers, a blockchain is a good solution for this purpose.

Personal data pods. In the SSI ecosystem, only the user has control over his personal data. Therefore, like with physical credentials which are stored somewhere with the user — f.e. in his wallet, verifiable credentials are to be stored within special software solutions — VC wallets. At the moment, these are primarily mobile applications. However, users may want to store their identity data in some kind of secure remote storage accessible anywhere.

Here the concept of remote personal data storage comes. Solid is a specification that lets people store their data securely in decentralized data stores called Pods.[235] Due to the specification, any type of data can be stored in a pod. Specifically mentioned that Solid supports storing Linked Data. It seems pods can act as secure remote repositories for identity data like verifiable credentials. Pods are external storages, but they remain "self-sovereign" for the following reasons:

1. Only the user controls access to the pod and makes any decision to share data.
2. Access to any data can be revoked.
3. Data is located in decentralized storage.

Other implementations of secured private decentralized data storages exist like Storj, Filecoin.

Onchain governance system for SSI ecosystem. As stated in the previous Part, governance for or SSI is extremely essential. This is not surprising given that this is an environment where social interactions take place. Some note that decentralized systems require even more governance efforts, as they consist of entities that act independently, unlike centralized systems where there is a single authority empowered to set mandatory rules for all. [236]

The peculiarity of a computer network is that governance rules can be incorporated directly into the protocols' architecture. Thus, network participants can't break these rules without losing the functionality.[237]

With blockchain as L1 of the stack, smart-contract may become such a mechanism that injects governance rules directly into the technical elements. A DAO, as a blockchain-based decision-making platform, can take decentralized governance to the next level. Actually, it's just a set of smart contracts. Storing all the transactions inside blockchain makes the decisions transparent to everyone and therefore easily auditable. Smart contracts may contain credential issuance and verification policies, VC exchange rules that are automatically enforceable and based on a democratic consensus achieved by token-based voting mechanisms. As a result, there will be no single policy-maker that owns or controls the whole system.

Decentralized reputation system. As relationships are moving to the digital world rapidly, a problem of online reputation arises because it's not obvious how one can sufficiently trust the subject if there is no direct contact. At the moment, reputation systems have a huge impact on consumer behavior because of e-commerce's constant growth. However, centralized reputation systems, widely used, have the following issues:

[235] Capadisli, S., Berners-Lee, T., Verborgh, R., Kjernsmo, K., Bingham, J. and Zagidulin, D., 2021. Solid Protocol. Solidproject.org.

[236] Windley, P., 2018. Decentralized Governance in Sovrin. Windley.com.

[237] Windley, P., 2018. Decentralized Governance in Sovrin. Windley.com.

1. They are not transparent and, therefore, can be easily manipulated. Currently, producing fake reviews is becoming a whole industry.
2. Almost every marketplace has its own one.[238] That means one product, service of a company may have a different reputation depending on the platform which they use to be presented.
3. Reputation is not permanent, and there is no guarantee of its integrity. Once a corresponding marketplace ceases to exist, reputation is lost. This is strikingly different from how it happens in our ordinary, non-digital life, where reputation is shared through social contacts.

The key reason for that issue is centralization and non-transparency again. Providing a blockchain-based decentralized reputation system can restore proper veracity and trust level. SSI can make this reputation more substantively independent and transferable across the services. Especially, a verifiable credential proof may be generated and provided to verifiers. Blockchain, on the other hand, is responsible for the transparency, verifiability, and inviolability of reputation.

But reputation isn't just about consumer relationships, goods, and services. The topic is much deeper. The reputation of a person himself, which still practically does not exist as an institution in the digital sphere, is seen as a huge separate sphere. Certain "synthesized" kinds of reputation may be generated based on the user's activity on multiple services. For example, a set of user's gamer achievements in Steam with his streamer profile status from Twitch in combination with an endless number of statuses from other gaming-related services may produce his collective gamer reputation. Then, a corresponding VC is generated. Subsequently, it can be used to access specific services or to obtain benefits, such as beta access to new products or esports tournaments.

This is just one example. The possibilities of such a reputation are limited only by the imagination of the developers. Possible cases with a professional reputation can be especially valuable.

Presentation exchange process. In the previous part, VCs and VPs are described. However, there is a missing piece that enables to establish a certain level of understanding between entities (no matter entities themselves or machines) about which credentials a verifier initially needs to perform a service and for holder — how to submit those credentials.[239] Also, a certain claim can be proven by multiple credentials. For example, a user's name and birth date can be claimed in an ID document, driver's license, college degree, and in less authoritative documents. Therefore, some selective rules, which state acceptance criteria, should be present.

To solve these issues, DIF proposes a draft Presentation Exchange specification that describes how verifiers can ask for credential-based proof in a universal way so that no matter which credential technologies are in use. The presentation exchange mechanism solves the problem of establishing a common direction of efforts for verifiers and clients. DIF proposes a Presentation definition data structure that verifies use to describe the requirements. Holders, in turn, use Presentation Submission data format to describe proofs submitted in accordance with them.

If VP submission is a one-to-one relationship between holders and verifiers, verifiers' Presentation Definitions, in turn, are aimed at widespread demonstrations and refer to the one-to-many communication. Thus, blockchain technology with smart contracts is useful again as a verifiable decentralized registry for these definitions.

[238] Lee, S., 2018. A Decentralized Reputation System: How Blockchain Can Restore Trust In Online Markets. Forbes.

[239] Buchner, D., Zundel, B. and Riedel, M., 2021. DIF Presentation Exchange. Identity.foundation.

Token-curated registry of Issuers/Verifiers (TCR). At first sight, that's the function of a verifiable data registry — either centralized or decentralized — to store a list of trusted public entities like issuers or verifiers, and there is nothing to add more. However, even decentralized registries themselves are not without problems. They may become the target of spam or social engineering. Thus, the involvement of trusted parties (like registry moderators) is still sometimes necessary.[240]

TCR aimed to solve the problems described above through the mechanism of economic incentives. TCR is maintained in a decentralized manner by token holders motivated by financial incentives. The original concept, in an extremely simplified form, is as follows.

Each registry has a native token that anyone can buy. Once anybody buys that token, he is interested in maintaining it properly as to involve new contributors. In order to add an entry to the list, an interested person buys the native token and places an application deposit. Token holders may challenge an application if they believe the application does not belong on the list. Challenges require a stake to initiate. Token holders vote to either accept or reject the application. Their vote is proportional to the number of tokens they own. If the application is rejected, the deposit is lost. If the application is accepted, the data is added to the list, and the Applicant keeps their deposit. [241]

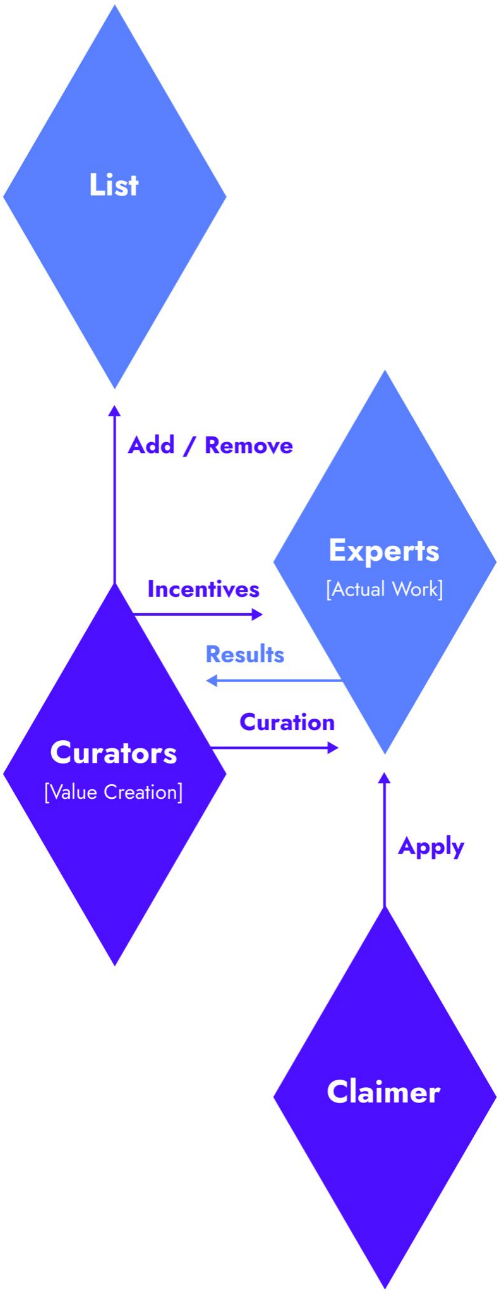
Blockchain has certain features making it a suitable repository for TCRs. TCRs are useful only if the following conditions are met simultaneously:

1. There is an objective answer to the particular question.
2. The answer is publicly observable.
3. The answer is very cheap to observe.[242]

The last two points are technically dependent and solved by the blockchain efficiently while at the same time guaranteeing the independence of the storage in comparison with a centralized approach. In addition, smart contracts, stored and executed on the blockchain, can take over the two functions at the same time. First, they can implement the voting functionality necessary to make a decision to accept items into the registry. Second, the mechanism of economic incentives itself is easier to implement in combination with the help of cryptoeconomics tools: token depositing can also be performed via smart contracts. Thus, a smart contract automatically controls all the processes and provides the results in a globally verifiable way.

BOTLabs, the organization behind the KILT protocol, expands TCR ideas in KILT Whitepaper. The original concept of TCRs is not free of drawbacks. The registry is curated directly by investors — token holders. That means anybody can become a curator by investing in the TCR, and there's no quality guarantee. KILT's concept is based on involving qualified parties — experts. The curator organization provides experts with certain incentives for registry curation. The experts, in turn, maintain the registry properly since doing a bad job results in being expelled from the experts' list by the curators and damaging their reputation. Reputation, and finally losing her income. Once experts' replies are received and the decision is positive, the curated list is populated.[243]

Token-curated registries seem to be one of the ways of authorizing issuers and verifiers in a decentralized manner. As anybody may wish to apply for these roles, a certain governance mechanism, setting appropriate limits and rules, must be present anyway.



[240] Medium. 2018. What is a Token Curated Registry?

[241] Kilt.io. 2020. White Paper Kilt.io.

[242] Kilt.io. 2020. White Paper Kilt.io.

[243] Kilt.io. 2020. White Paper Kilt.io. p 50

Selective Disclosure / ZKP. As stated in the previous Part, selective disclosure is one of the fundamental privacy-enhancing features of SSI. SSI is grounded on the principle of data minimization. Since a typical credential is a set of multiple properties, there should be a mechanism to reveal only the part of them (selective disclosure) or just to provide a true/false statement based on the value without revealing it (so-called predicate proofs).

Smart contracts executed in blockchain may serve ZKP implementations. For that purpose, smart-contract stores Verifier's publicly observable question, determining which predicate proof is needed. In order to provide the proof, a transaction is written to the blockchain. In this way, a smart-contract acts as a certain kind of gate, where communication between holders and verifiers takes place.

Cryptoeconomic incentives for SSI. Since lots of digital trust ecosystems are closely intertwined with blockchain (several initially SSI-focused blockchains already exist, like KILT or Sovrin), a mutual connection between SSI and cryptoeconomics suggests itself.

One of the possible use-cases is connected with the VC issuance process. Typically, credentials are issued by bodies that, as a rule, exist as some kind of centralized bodies outside the digital world and themselves have a certain authority. In the example of professional qualifications, it is usually a university or college that finally confirms competence based on results of education. However, it is not necessary to exactly follow only conventional relations models when transferring them to the digital environment. A trusted digital environment based on the SSI concept provides new opportunities with the help of blockchain technologies.

There is an option to issue competence confirming credentials in a way that doesn't require a centralized assessor or an institution, proposed on the ninth Rebooting the Web of Trust workshop. The proposed solution takes as a basis the web of trust paradigm, expanding it to the network of competencies. Instead of any centralized party, the decision to qualify a subject is made by an expert or group of experts. Token staking/slashing model acts for assurance purposes preventing fraud.[244]

The power of decentralized communities in combination with cryptoeconomics has great power. The concept is not abandoned and seems to continue to evolve. For instance, KILT proposes a concept of token-curated attestors (TCAs) in its whitepaper, which is also based on the economic involvement of experts in the issuance process, which do the inspection work before issuing verifiable credentials.[245]

Having developed this concept appropriately in combination with other achievements of blockchain technologies (e.g., DAOs, DPKI, etc.), it is theoretically possible to create completely decentralized systems governed by themselves.

[244] Gershuni, S., 2019. Paper: VC for decentralized assessment. GitHub.

[245] Kilt.io. 2020. White Paper Kilt.io. p. 51

Why use FreeTON for building digital identity systems

FreeTON is a modem solution that has been recently launched in spring 2020. It is presented as a new generation blockchain that combines the best approaches of previous generations, but at the same time has added new ones that make it as scalable and efficient as possible, and, therefore, potentially, one of the most suitable for digital trust ecosystems.

FreeTON is scalable and fast

For a relatively long time, blockchains referred to only single-chain systems. Even Ethereum - a widely used blockchain in other areas beyond cryptocurrencies (like DeFi where scalability is essential) - is currently a single-chain. But the emergence of new use cases aimed to transfer the useful properties of blockchain into our daily life revealed the weaknesses of such an approach. They are most noticeable if we compare a transaction limit of a single-chain ledger with the normal operations intensity of some centralized systems. Visa, which processes approximately 1,700 transactions per second, has become a classic example for comparison here.[246] It's obvious that the capacity of single-chain blockchains is not enough for their widespread use.

Thus, if we speak about modern solutions from the latest generations, it is correct to call them not blockchains but complex blockchain systems. That is what we call multi-chain architecture.

FreeTON, as it seems, the representative of the last blockchain generation, promises to be able to handle millions of transactions per second. For this, the mechanisms described below were incorporated into its architecture.

As a new generation blockchain, FreeTON is based on multi-chain architecture. At the same time, FreeTON is a tightly coupled system. An interoperable multi-chain architecture implies cross-chain interaction, but the difference is between the level of that interaction. In a loosely coupled system, the way that blockchain "communicate" between each other does not significantly differ from that applied to the interaction of two completely different networks like Bitcoin and Ethereum. Thus, typically an initial "out" transaction in one network is required while the subsequent confirmation in the second is expected. It's noted that this time lag, in addition to its presence, may cause specific problems. On the contrary, "tightly-coupled" systems by design include a special fast messaging mechanism working across all blockchains in order to make message delivery almost instantaneous.

FreeTON natively supports dynamic sharding. In simple words, in FreeTON, sharding refers to the technique that allows splitting the whole system into separate areas performing distributed computations — sharding blockchains or shardchains. Sharding can be either static or dynamic. While the first approach is strongly limited to a defined finite number of shards, the second seems more scalable, allowing shards to be dynamically splitted and merged where certain conditions are reached. In fact, efficient sharding requires the system to be tightly coupled.

[246] Li, K., 2019. The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed | Hacker Noon.

Once the distributed system is launched, making changes to it becomes an extremely complicated procedure. Hence, it seems reasonable to thoroughly think over the infrastructure from the beginning, even covering the configurations, which now seem unnecessary and overhead. Therefore, FreeTON natively supports heterogeneous workchains in combination with a masterchain that stores a set of active blockchains, a list of validators, and other common configurations. The term "heterogeneous" refers to blockchains with different configurations: signs such as different VMs, native tokens, and other rules indicate that the system is heterogeneous. However, as FreeTON supports several blockchains with the same rules to be present, technically, it's rather a heterogeneous-homogeneous system, still one of a kind and therefore the most flexible now.

Extremely low transaction fees

As for digital trust ecosystems, which aim to cover whole countries and even countries, high transaction fees can ruin the idea from the very beginning. Right now, at the peak moments, Ethereum's gas price reaches enormous values. As for FreeTON, It's declared that the transaction fee will not exceed $ 0.1.

For blockchains, a transaction fee is not only a way of rewarding subjects. As blockchain typically acts as a public utility, there must be certain protective measures against the abuse of records. That's why any action with a smart contract in FreeTON is accompanied by a small value of tokens, making such sabotage thriftless.[247]

FreeTON uses BFT PoS consensus algorithm

The Proof-of-Work consensus algorithm is still common to many blockchains. However, as it's based on solving computational problems in order for the blocks to be created, it requires large computing power involved, which becomes a problem on a large scale.

The Proof-of-Stake is another consensus approach. Validators of the network, in fact, are doing the same job as miners in PoW-based blockchains: they are responsible for verifying and adding new blocks to the chain. However, the mechanism is rather different. It's based on depositing some great value (actually, a certain amount of native blockchain tokens) to assert that they have checked some blocks and have found them correct. Validators are rewarded for this work. However, if they are found to validate invalid blocks, they are losing their stake (that is, the so-called slashing mechanism). So, staking serves as an economic guarantee mechanism, ensuring the correctness of the chain.

At the moment, there are two primary PoS concepts: Delegated Proof-of-Stake (DPOS) and Byzantine Fault Tolerant (BFT). In simple words, DPOS specifies a certain universally known group of validators for each block, and only that persons are authorized to sign them, while with BFT, multiple nodes may produce a new block independently, but the right one is selected by a special algorithm. While DPOS-based are faster separately, when off-chain or cross-chain transactions are needed, it takes a lot longer to properly confirm their validity. [248] Thus, BFT PoS is preferred to establish an interoperable system.

[247] En.freeton.wiki. n.d. Smart contracts - Free TON Wiki.

[248] En.freeton.wiki. n.d. Comparison to other blockchain projects - Free TON Wiki.

Asynchronous smart contracts

Smart contracts no longer surprise anyone. It should only be noted that in FreeTON their usage reached its apogee. Almost everything in TON is a smart contract. In particular, each account in TON must be associated with a smart contract code (or initialized) in order for a user to be able to perform any operation with it. TON virtual machine proposes an extensible and storage thrifty environment for their execution. [249]

So that smart contracts are executed inside the ledger like regular software on personal computers. Even more, the immutable ledger is just a small part of FreeTON, and the whole FreeTON stack is being labeled as a distributed computer, having its own abstract "operating system" consisting of software components.[250]

For the SSI ecosystem, it's essential that all interactions between smart contracts are asynchronous, providing better common network performance.

Bridge to Ethereum (Broxus)

Ethereum blockchain, launched in 2015, gave a big impetus to the DLT development. Such phenomenon as a smart contract, DeFI, DAOs, are mostly associated with Ethereum. The breakthrough he brought after Bitcoin allowed him to take second place in terms of capitalization

A link to the second most liquid chain seems a nice essential bonus for network popularization and adoption. Thus, a bridge between FreeTON and Ethereum is currently under development.[251] The bridge aims to connect the high performance and low fees of FreeTON to the liquidity of the ETH ecosystem.[252]

Upper level, the mechanism is as follows: "when a token leaves one blockchain, it is burned or blocked, and an equivalent token appears in the opposite blockchain if a token is returned, then a double token is burned or blocked." [253] The bridge does not transfer the original tokens from one network to another: Instead, special wrapped tokens are used: wrapped Ether (WETH) and wrapped TON (WTON). To perform a transfer, the tokenholder first puts wanted TONs value to the FreeTON network storage. TONs are blocked, the user receives the corresponding value of WTON tokens, compatible with ERC-20 specification. Thus, they can be freely sent to any ethereum address. It works the same way in the opposite direction. [254]

The described solution is expected to combine maximum scalability and performance of FreeTON with Ethereum's high liquidity and its biggest background as a DeFI-platform.

[249] En.freeton.wiki. n.d. TVM - Free TON Wiki.

[250] Docs.ton.dev. n.d. What is TON OS?.

[251] GitHub. n.d. Tokens fungible smart contracts.

[252] CryptoNinjas.net. 2021. Free TON: "Bridges of love and friendship" — we will offer developers around the world the fastest Ethereum bridge.

[253] CryptoNinjas.net. 2021. Free TON: "Bridges of love and friendship" — we will offer developers around the world the fastest Ethereum bridge.

[254] FreeTON House. 2021. Free TON↔Ethereum Bridge: Broxus Style Architecture

FreeTON distributed storage is under developing

A modern blockchain is valuable not only as an immutable registry but also for a stack of additional components that surround it. Thus, FeeTON is a set of components (TON P2P Network, TON Storage, TON Services) centered around the TON blockchain itself.[255]

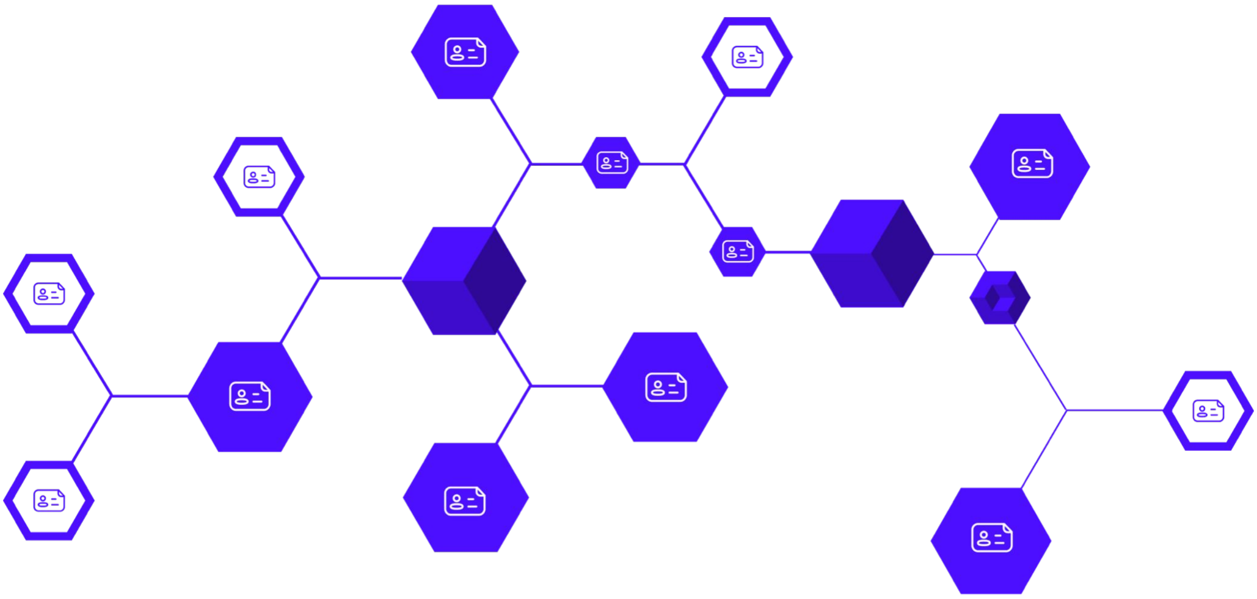
As it mentioned earlier, for the SSI ecosystem, it's essential to have no less "self-sovereign" way to store identity data. Here the concept of decentralized storage comes.

FreeTON's decentralized storage concept is a bit like a torrent protocol: the data pieces are shared between the nodes, which are rewarded for keeping them. As the master chain already launched in May 2020, the core FreeTON storage functional is pre-built into the code. However, the more abstract layers that allow such functions as indexing and searching are to be built until this component will start to function.[256]

[255] En.freeton.wiki. n.d. Comparison to other blockchain projects - Free TON Wiki.

[256] FreeTON.house. n.d. TON Storage.

SSI and blockchain technology tandem potential



The popularity of blockchain as a disruptive technology continues to grow. However, today blockchains are used mainly just for value transfers.

In our physical world, value transfers are usually accompanied by the provision of some corresponding documents. It is even more typical for business relations. As digital transformation moves these relationships into the digital world, it does not cease to be so. Providing the authenticated data, on the contrary, becomes the basis of trust between participants.

So, for every value transfer transaction, there are multiple authenticated data transfer transactions to be present. It gives the SSI market potential to become much larger, resulting in trillions of verifiable data transactions. Thus, an ecosystem where blockchain as Layer 1 and other SSI components complement each other should be chosen as the next direction:

1. Blockchain for SSI helps to establish the key infrastructure elements such as VDR or self-sovereign PKI system, spreading its qualities of data immutability and resolvability where necessary.
2. SSI covers a variety of blockchain use-cases with corresponding verifiable data flows and thus expands the boundaries of their application, helps to provide greater user experience and protects the privacy of end-users.

Blockchain was a disruptive technology itself. In addition to its initial original purpose — secure independent payments — a variety of additional areas of use have been proposed. But without a trustworthy and interoperable way of fact confirmation, those use cases will stay vendor/network locked-in and hard to spread widely. SSI solutions' support at the L1 layer significantly increases the number of really applicable cases and blockchain technology adoption in general, while the more transactions in the ecosystem, the greater its economic value.

Conclusion

Conclusion

The fundamental advantages of the SSI have already been discussed in previous Parts. It is clear that SSI is more than just a technology that aids in data security. Identity is the cornerstone of evolution; it is critical to interactions in the digital economy. It might potentially be used for espionage, as well as against human rights and humanity itself. Following the high-profile security breaches witnessed by the worldwide community with Equifax in the United States, Aadhaar in India, and even Facebook and Google internationally, it is clear that we are on the verge of something really dangerous happening here. It is something that affects all of us.

It is concerned with fundamental problems such as our identification and the right to privacy. Identity management systems are vital; as a global society, it is vital to collaborate to create the most effective strategies to resist these threats. Because technology has the potential to be a double-edged sword that can be used for both good and evil, it is important to create a new human-census model.

In Part 1, the reader was taken on a journey that began with the creation of the Internet as we know it today, progressed through the development of digital identity, e-commerce, rapid digitization of personal data, and our daily lives, and ended with the notion of SSI. For centuries, the only form of proof of facts was paper documents. Despite the continuous digitization of all aspects of life, a substantial portion of papers and data are still in paper form. Paper documents do not correspond to the level of technological breakthrough that has occurred in recent years when the Internet has become a universal means of communication between people, corporations, and governments.

If the advantages of bits over paper are obvious, then what was holding the world back from the transition, and why did the technology for this not appear until 2021? The first reason is the fragmentation of a large number of IT systems. Solutions that are designed to simplify life in reality only complicate it: now, instead of a single folder with documents, the user must remember dozens of different usernames and passwords from Internet services. Each of them has its own interface, rules of use, mobile application, which only confuses users. Data is not transferred between the systems at all (how many times have you filled in the same fields in the forms of different sites?), or it requires a long and expensive integration.

Another reason is the lack of security of centralized registries and databases. The reason for this is not poor security but the high value of the data. If a single database, even a well-protected one, stores data on the financial history of millions of people, there is a serious motivation for attackers to bribe the administrator or conduct a very complex and expensive attack to gain illegal access to the data as a result. The proof of this is the regular hacking of major banks, corporations, and even government IT systems, the references to which can be found throughout the paper, as well as the solution to it that SSI can be.

Five years ago, the notion of SSI appeared to be a utopian fantasy expressed in a few papers by a small academic community, but it is today a movement and a trillion-dollar industry of commercial potential that aims to make our lives better, our data more secure and is being actively implemented by the largest businesses and government agencies of the world's leading economies.

Part 2 focuses on the SSI concept and elaborates on the current state of affairs, the actual practical benefits of using the SSI, and how governments in the European Union, the United States, and Canada, as well as tech companies and prominent colleges throughout the world, are transitioning to an SSI system. The benefits of this kind of software architecture are decentralized user data storage and a shift in control towards the user. At the same time, the legal significance and provable verifiability of such data and documents were observed. In this case, the data is not stored centrally but belongs only to the data owner, that is, the user.

This approach has the potential to assist in resolving the issue of certain vulnerable populations eventually receiving an ID and not being left behind in times of tragedy and misfortune, as well as having no hurdles to using essential services. The United Nations has endorsed the usage of the SSI concept, and more and more initiatives are springing up in the never-ending drive to make our planet a better place for everyone. Businesses will benefit from lower switching costs and compliance with the legal framework, such as GDPR CCPA, FISMA, EFF. End-users will enjoy the security of their personal data and control over sharing their credentials and so much more.

Part 3 is a submarine that invites the reader to take a deep dive into the SSI structure, and it talks about technical aspects of SSI. It mentions, among other things, SSI standards. In November 2019, Verifiable Credentials were adopted by the W3C international consortium, which develops standards for the Internet, such as HTML, XML, and HTTP. This standard defines the compilation, release, and verification of any information and documentation in digital format. Using a single standard means that you no longer need to integrate different IT systems. The job search system will automatically recognize your digital diploma issued according to the VC standard. The receipt, warranty card, and certificate of conformity of the goods will automatically be in the buyer's wallet.

Conclusion

The SSI approach includes the use of distributed storage technology to guarantee the availability of data for life, as well as selective disclosure of information — for example, using zero-knowledge proof. This makes it possible to prove digitally and legally significant any fact about yourself without disclosing details: for example, to prove that the age is more than 18 years old, without giving the date of birth. In addition to convenience, this approach provides a higher level of security: it is not enough for an attacker to hack a single, even the most secure, database to steal 5 million bank cards — instead, he will need to hack 5 million separate systems, which is an order of magnitude more difficult, if at all feasible. Part 3 expands on the governance stacks and is concluded by the typical journey of SSI user case illustration.

As has been shown above, SSI enables hundreds of use cases in the public sector, corporate authenticated data exchange, and also purely digital areas like the concept of web3 or DeFi. This variety of spheres is determined by the key role of the identity issue. Each and every business goes digital, and we can declare that the necessity of digital subjectivity is growing.

It's claimed that the value of the SSI ecosystem, being the subject of Metcalfe's Law, directly depends on the scope of SSI adoption. Thus, any party from the relations must clearly benefit from SSI to make that technology spread widely. The efforts should be made even not so much to develop technical solutions, but to find suitable business models in the first place.

The next **Part 4**, outlined business opportunities that arise with the development and the use of SSI. The European Commission, the US Department of Homeland Security, the Government of Canada, major universities from the Massachusetts Institute of Technology and Harvard to the University of Munich, as well as large businesses — Oracle, SAP, IBM, Microsoft, Workday-are already prioritizing the development of SSI systems for solving various tasks: from issuing passports and driver's licenses to increasing the transparency of accounting for competencies in the labor market. SSI is a key to solving many issues across all sectors, including healthcare and education, finance, and the workplace.

Part 5 discusses the synergy between SSI and cryptocurrencies, as well as the possibilities it opens up in terms of drastically altering the landscape of online payments, making them more secure and continuous, and eliminating the need to fill out lengthy forms and scan documents in favor of one-click VC provision. At the moment, both blockchain-based and non-blockchain-based SSI solutions are available; blockchain-based technologies for the SSI infrastructure tied to the ledger expand the decentralized nature of SSI with such great features as trustworthy credentials revocation, decentralized key management, reputation and governance.

Throughout the paper, the reader can find sufficient evidence that SSI has the potential to become a ubiquitous technology that serves millions of customers. As previously demonstrated, SSI supports hundreds of use cases in the public sector, corporate verified data exchange, and entirely digital sectors such as web3 or decentralized finance. SSI is based on the same basic technology and principles as blockchains.

As a consequence, any decentralized protocol, such as blockchain or decentralized data storage, will benefit greatly by enabling SSI infrastructure and supporting SSI applications. Following an examination and research on the subject, the paper suggests that protocol developers begin by developing fundamental infrastructure that enables SSI applications to be easy to construct and robust, with examples of DID method, issuer registry, JSON schema registry, revocation registry, etc.

Implementing this infrastructure will result in more decentralized applications that use the protocol, resulting in widespread adoption among decentralized web aficionados but, more crucially, among a broad variety of end customers who are not even familiar with the blockchain concept. Increased adoption and production usage will result in a positive feedback loop that reinforces the utility and value of layer one.

We believe that enabling SSI infrastructure and supporting SSI applications will be extremely valuable for any decentralized protocol, be it blockchain or decentralized data storage. We suggest that protocol developers should start with building core infrastructure that makes SSI applications easy to build and robust. We expect implementing this infrastructure will lead to more decentralized applications utilizing the protocol. That, in turn, will create a wide adoption among decentralized web enthusiasts and, more importantly, among a broad range of end-users that are not even necessarily familiar with the blockchain concept. The increased adoption and more product usage will create a positive feedback loop reinforcing the L1 blockchain ecosystem's utility and value.

References

References

[Paper] Formalizing Trust in Artificial Intelligence: Prerequisites, C., 2021. [Paper] Formalizing Trust in Artificial Intelligence: Prerequisites, Causes and Goals of Human Trust in AI.   Tusharc.dev. Available at: <https://tusharc.dev/papers/formalizing_trust_ai_goldberg.html> [Accessed 20 June 2021].

[Paper] Formalizing Trust in Artificial Intelligence: Prerequisites, C., 2021. [Paper] Formalizing Trust in Artificial Intelligence: Prerequisites, Causes and Goals of Human Trust in AI.   Tusharc.dev. Available at: <https://tusharc.dev/papers/formalizing_trust_ai_goldberg.html> [Accessed 21 June 2021].

2020. Decentralised Identity: What's at Stake? A Position Paper by the INATBA Identity Working Group. [ebook] International Association for Trusted Blockchain Application, p.p.10. Available at: <https://inatba.org/wp-content/uploads/2020/11/2020-11-INATBA-Decentralised-Identity-001.pdf> [Accessed 20 June 2021].

2021. Blockchain and Digital Identity: the path to Self Sovereign Identity.   Available at: <https://www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf> [Accessed 13 June 2021].

2021. Privacy for sale — To the highest bidder, Data and ethics survey. [ebook] Deloitte LLP and affiliated entities., pp.1-18. Available at: <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-data-ethics-and-privacy-surveyaoda.pdf> [Accessed 20 June 2021].

2021. W3.org. 2021. DID Core..   Available at: <https://www.w3.org/TR/vc-data-model/> [Accessed 6 June 2021].

Acrobat.adobe.com. n.d. What is a digital signature | Adobe Sign.   Available at: <https://acrobat.adobe.com/ua/ua/sign/glossary/digital-signatures.html> [Accessed 13 June 2021].

Acrobat.adobe.com. n.d. What is a wet signature | Wet vs electronic signature | Adobe Sign.   Available at: <https://acrobat.adobe.com/us/en/sign/esignature-resources/wet-signature.html> [Accessed 13 June 2021].

Affinidi.com. 2021. About us.   Available at: <https://www.affinidi.com/about-us> [Accessed 21 June 2021].

Allen, C., 2016. The Path to Self-Sovereign Identity.   Lifewithalacrity.com. Available at: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html> [Accessed 3 June 2021].

Andrade-Walz, A., 2020. Self-sovereign identity: The true password killer.   Securitymagazine.com. Available at: <https://www.securitymagazine.com/articles/93356-self-sovereign-identity-the-true-password-killer> [Accessed 17 June 2021].

Andrade-Walz, A., 2020. The Future of Authentication is Self-Sovereign - Evernym.   Evernym. Available at: <https://www.evernym.com/blog/the-future-of-authentication-is-self-sovereign/> [Accessed 20 June 2021].

Antonopoulos, A., 2014. Bitcoin Security Model: Trust by Computation. O'Reilly- Radar.. http://radar.oreilly.com/2014/02/bitcoinsecurity-model-trust-by-computation.htm. Available at: <http://radar.oreilly.com/2014/02/bitcoinsecurity-model-trust-by-computation.html> [Accessed 3 June 2021].

Appelcline, S., Newton, J., Farmer, R. and Crocker, D., 2021. Rebranding the Web of Trust, A White Paper from Rebooting the Web of Trust.   https://nbviewer.jupyter.org/. Available at: <https://nbviewer.jupyter.org/github/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/rebranding-web-of-trust.pdf> [Accessed 20 June 2021].

Atzori, M., 2017. Blockchain technology and decentralized governance: Is the state still necessary?. Journal of Governance and Regulation,   6(1), pp.45-62. Available at: <https://virtusinterpress.org/IMG/pdf/10.22495_jgr_v6_i1_p5.pdf> [Accessed 3 June 2021].

Bansal, A., Garg, C. and Padappayil, R., 2020. Optimizing the Implementation of COVID-19 "Immunity Certificates" Using Blockchain. Journal of Medical Systems, 44(9).

Barclaycard.co.uk. n.d. SSI impact on payments | Barclaycard Business.   Available at: <https://www.barclaycard.co.uk/business/accepting-payments/corporate-payment-solutions/news/self-sovereign-identity> [Accessed 21 June 2021].

Bar-Zik, R., 2021. Day before election, entirety of Israel's voter data leaked online — again. haaretz.com. Available at: <https://www.haaretz.com/israel-news/elections/.premium-just-before-election-entirety-of-israel-s-voter-data-leaked-online-again-1.9642920> [Accessed 13 June 2021].

Belchior, R., Putz, B., Pernul, G., Correia, M., Vasconcelos, A. and Guerreiro, S., 2020. SSIBAC: Self-Sovereign Identity Based Access Control. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),.

Blockcerts. 2021. Blockchain Credentials. Available at: <https://www.blockcerts.org/about.html> [Accessed 20 June 2021].

Bodle, R., 2013. THE ETHICS OF ONLINE ANONYMITY OR ZUCKERBERG VS. "MOOT". 1st ed. [ebook] Computers and Society, pp.Volume 43, Number 1. Available at: <https://www.ohchr.org/Documents/Issues/Opinion/Communications/BodleRobert.pdf> [Accessed 7 June 2021].

Bosch Global. 2021. Digital identity — enabling secure collaboration with blockchain technology. Available at: <https://www.bosch.com/stories/self-sovereign-identities/> [Accessed 17 June 2021].

Bouras, M., Lu, Q., Zhang, F., Wan, Y., Zhang, T. and Ning, H., 2020. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors, 20(2), p.483.

Boysen, A., 2021. Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. https://www.frontiersin.org/. Available at: <https://www.frontiersin.org/articles/10.3389/fbloc.2021.624258/full#B8> [Accessed 1 June 2021].

Buchner, D., Zundel, B. and Riedel, M., 2021. DIF Presentation Exchange. Identity.foundation. Available at: <https://identity.foundation/presentation-exchange/> [Accessed 21 June 2021].

Capadisli, S., Berners-Lee, T., Verborgh, R., Kjernsmo, K., Bingham, J. and Zagidulin, D., 2021. Solid Protocol. Solidproject.org. Available at: <https://solidproject.org/TR/protocol> [Accessed 21 June 2021].

Carter, S., 2021. PKI Infrastructure: 4 Common Challenges | Venafi. Venafi.com. Available at: <https://www.venafi.com/blog/4-ways-machine-identities-will-challenge-you> [Accessed 11 June 2021].

Casino, F., Dasaklis, T. and Patsakis, C., 2019. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, pp.55-81.

CEF Digital. 2021. CEF Digital Home. Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home> [Accessed 17 June 2021].

CEF Digital. 2021. EBSI. Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI> [Accessed 13 June 2021].

Chadwick, D., Longley, D., Sporny, M., Terbu, O., Zundel, B. and Zagidulin, D., 2019. Verifiable Credentials Implementation Guidelines 1.0. W3.org. Available at: <https://www.w3.org/TR/vc-imp-guide/#zero-knowledge-proofs> [Accessed 20 June 2021].

Cheesman, M., 2020. Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. Geopolitics, pp.1-26.

Ciobanu, M., 2020. The potential of Self-Sovereign Identity to reduce the growing regulatory burden. Thepaypers.com. Available at: <https://thepaypers.com/interviews/the-potential-of-self-sovereign-identity-to-reduce-the-growing-regulatory-burden--1241738> [Accessed 21 June 2021].

Constine, J., 2018. A flaw-by-flaw guide to Facebook's new GDPR privacy changes. Techcrunch.com. Available at: <https://techcrunch.com/2018/04/17/facebook-gdpr-changes/> [Accessed 13 June 2021].

Conway, L., 2021. Ethereum 2.0: What You Need To Know. The Street Crypto: Bitcoin and cryptocurrency news, advice, analysis and more. Available at: <https://www.thestreet.com/crypto/ethereum/ethereum-2-upgrade-what-you-need-to-know> [Accessed 21 June 2021].

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W., 2008. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Datatracker.ietf.org. Available at: <https://datatracker.ietf.org/doc/html/rfc5280> [Accessed 20 June 2021].

Cordeiro Domenech, M., Comunello, E. and Silva Wangham, M., 2014. Identity management in e-Health: A case study of web of things application using OpenID connect. 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), Available at: <http://vigir.missouri.edu/~gdesouza/Research/Conference_CDs/IEEE_HealthCom_2014/papers/p158-domenech.pdf> [Accessed 21 June 2021].

Cosmos: The Internet of Blockchains. 2021. Cosmos: The Internet of Blockchains. Available at: <https://cosmos.network/> [Accessed 21 June 2021].

Covidcreds.org. 2021. COVID-19 Credentials initiative : Home. Available at: <https://www.covidcreds.org/> [Accessed 21 June 2021].

CryptoNinjas.net. 2021. Free TON: "Bridges of love and friendship" — we will offer developers around the world the fastest Ethereum bridge. Available at: <https://www.cryptoninjas.net/2021/03/02/free-ton-bridges-of-love-and-friendship-we-will-offer-developers-around-the-world-the-fastest-ethereum-bridge/> [Accessed 21 June 2021].

Davie, M., 2021. Kiva's next frontier: Kiva Protocol. Kiva.org. Available at: <https://www.kiva.org/blog/kivas-next-frontier-kiva-protocol> [Accessed 21 June 2021].

de Filippi, P., 2016. The interplay between decentralization and privacy: the case of blockchain technologies. Journal of Peer Production, Alternative Internets(7). Available at: <https://hal.archives-ouvertes.fr/hal-01382006/document> [Accessed 10 June 2021].

Diacc.ca. 2020. Pan-Canadian Trust Framework Model Document Status: Final Recommendation V1.0. Available at: <https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf> [Accessed 20 June 2021].

Diacc.ca. 2021. PCTF Overview. Available at: <https://diacc.ca/trust-framework/pctf-overview/> [Accessed 20 June 2021].

Docs.ton.dev. n.d. What is TON OS?. Available at: <https://docs.ton.dev/86757ecb2/p/7941cd-what-is-ton-os> [Accessed 21 June 2021].

Dong, C., Wang, Z., Chen, S. and Xiang, Y., 2020. BBM: A Blockchain-Based Model for Open Banking via Self-sovereign Identity. Blockchain – ICBC 2020, pp.61-75.

Doubleday, K., 2018. Blockchain Immutability—Why does it matter?. Medium. Available at: <https://medium.com/fluree/immutability-and-the-enterprise-an-immense-value-proposition-98cd3bf900b1> [Accessed 21 June 2021].

Du Seuil, D., 2021. European Self Sovereign identity framework. [ebook] Available at: <https://www.eesc.europa.eu/sites/default/files/files/1._panel_-_daniel_du_seuil.pdf> [Accessed 20 June 2021].Duffy, K., 2020. APPLYING SELF-SOVEREIGN IDENTITY PRINCIPLES TO INTEROPERABLE LEARNING RECORDS. [ebook] U.S. CHAMBER OF COMMERCE FOUNDATION,T3 INNOVATION NETWORK. Available at: <https://www.uschamberfoundation.org/sites/default/files/media-uploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf> [Accessed 17 June 2021].

Edwards, J., 2020. How to Fight The Fraud Crisis Through Blockchain and Self-sovereign Identity. Linkedin.com. Available at: <https://www.linkedin.com/pulse/how-fight-fraud-crisis-through-blockchain-identity-jason-edwards/> [Accessed 17 June 2021].

En.freeton.wiki. 2021. Comparison to other blockchain projects - Free TON Wiki. Available at: <https://en.freeton.wiki/Comparison_to_other_blockchain_projects> [Accessed 21 June 2021].En.freeton.wiki. n.d. Comparison to other blockchain projects - Free TON Wiki. Available at: <https://en.freeton.wiki/Comparison_to_other_blockchain_projects#Variants_of_Proof-of-Stake._DPOS_vs._BFT.> [Accessed 21 June 2021].

En.freeton.wiki. n.d. Smart contracts - Free TON Wiki. Available at: <https://en.freeton.wiki/Smart_contracts> [Accessed 21 June 2021].

En.freeton.wiki. n.d. TVM - Free TON Wiki. Available at: <https://en.freeton.wiki/TVM> [Accessed 21 June 2021].

Entriken, W., Sachs, N., Shirley, D. and Evans, J., 2021. EIP-721: ERC-721 Non-Fungible Token Standard. Ethereum Improvement Proposals. Available at: <https://eips.ethereum.org/EIPS/eip-721> [Accessed 21 June 2021].

ethereum.org. 2020. Non-fungible tokens (NFT) | ethereum.org. Available at: <https://ethereum.org/en/nft/> [Accessed 21 June 2021].

ethereum.org. 2021. Proof-of-stake (PoS) | ethereum.org. Available at: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> [Accessed 20 June 2021].

Eublockchainforum.eu. 2020. BLOCKCHAIN FOR GOVERNMENT AND PUBLIC SERVICES An initiative of the a thematic report prepared by THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM BLOCKCHAIN AND DIGITAL IDENTITY. Available at: <https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf> [Accessed 21 June 2021].

Fleishman, G., 2000. Cartoon Captures Spirit of the Internet (Published 2000). Nytimes.com. Available at: <https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html> [Accessed 5 June 2021].

Frankenfield, J., 2021. Cryptocurrency. Investopedia. Available at: <https://www.investopedia.com/terms/c/cryptocurrency.asp> [Accessed 21 June 2021].

FreeTON HOUSE. 2021. Free TON↔Ethereum Bridge: Broxus Starts and Wins | Reviews | Free TON House. Available at: <https://freeton.house/en/freeton-ethereum-bridge-broxus-style-architecture/> [Accessed 21 June 2021].

Freeton.house. n.d. TON Storage | Free TON House. Available at: <https://freeton.house/en/tag/ton-storage/> [Accessed 21 June 2021].

Gallagher, S., 2019. How the Value of Educational Credentials Is and Isn't Changing. Harvard Business Review. Available at: <https://hbr.org/2019/09/how-the-value-of-educational-credentials-is-and-isnt-changing> [Accessed 21 June 2021].

Gans, R., Ubacht, J. and Janssen, M., 2021. Self-sovereign Identities for Fighting the Impact of COVID-19 Pandemic. Digital Government: Research and Practice, 2(2), pp.1-4. Available at: <https://dl.acm.org/doi/fullHtml/10.1145/3429629> [Accessed 21 June 2021].

Gershuni, S., 2019. Digitals Credentials. Medium. Available at: <https://medium.com/credentia/> [Accessed 21 June 2021].

Gershuni, S., 2019. Paper: VC for decentralized assessment ·. GitHub. Available at: <https://github.com/WebOfTrustInfo/rwot9-prague/commit/6cf2855785a8368118a17286f854098d74651476> [Accessed 20 June 2021].

Gershuni, S., 2020. Technologiya suverennoi lichnosti - rynok v million dollarov.. VC.ru. Available at: <https://vc.ru/crypto/177852-tehnologiya-suverennoy-lichnosti-rynok-v-trillion-dollarov> [Accessed 21 June 2021].

Gershuni, S., 2021. Bullish Case for Self-Sovereign Identity. Medium. Available at: <https://sgershuni.medium.com/bullish-case-for-self-sovereign-identity-c2c26857f0ab> [Accessed 3 June 2021].

Giannopoulou, A. and Wang, F., 2021. Self-sovereign identity. Internet Policy Review. Available at: <https://policyreview.info/glossary/self-sovereign-identity> [Accessed 17 June 2021].

GitHub. 2021. sovrin-foundation/protocol. Available at: <https://github.com/sovrin-foundation/protocol/blob/master/dkms/README.md> [Accessed 21 June 2021].

GitHub. n.d. Tokens fungible smart contracts. Available at: <https://github.com/broxus/ton-eth-bridge-token-contracts> [Accessed 21 June 2021].

Glaude, M., 2021. About Trust Over IP — A Comprehensive Resource Page.   Northern Block | Self Sovereign Identity Solution Provider. Available at: <https://northernblock.io/trust-over-ip/> [Accessed 20 June 2021].

Graglia, M., Robustelli, T. and Mellon, C., 2018. The Nail Finds a Hammer.   New America. Available at: <https://www.newamerica.org/future-land-housing/reports/nail-finds-hammer/> [Accessed 17 June 2021].

Grech, A., Sood, I. and Ariño, L., 2021. Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. Frontiers in Blockchain, 4.

Guillén, F., 2018. Blockchain Accomplishments - BLOCKTAC.   BLOCKTAC. Available at: <https://www.blocktac.com/en/news/blockchain-accomplishments/> [Accessed 1 June 2021].

Hardman, D., 2021. DIDComm Messaging Specification.   Identity.foundation. Available at: <https://identity.foundation/didcomm-messaging/spec/> [Accessed 20 June 2021].

Helmy, N., 2020. A solution for privacy-preserving verifiable credentials.   Medium. Available at: <https://medium.com/mattr-global/a-solution-for-privacy-preserving-verifiable-credentials-f1650aa16093> [Accessed 20 June 2021].

Helmy, N., 2020. Overview of Decentralized Identity Standards.   Medium. Available at: <https://medium.com/decentralized-identity/overview-of-decentralized-identity-standards-f82efd9ab6c7> [Accessed 13 June 2021].

Home of internet privacy. 2020. What is a zero-knowledge proof and why is it useful?.   Available at: <https://www.expressvpn.com/blog/zero-knowledge-proofs-explained/> [Accessed 20 June 2021].

https://essif-lab.pages.grnet.gr/framework/. 2021. eSSIF-Lab Business Architecture.   Available at: <https://essif-lab.pages.grnet.gr/framework/docs/essifLab-fw-bus-arch> [Accessed 20 June 2021].

https://www.mckinsey.com/. 2018. DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH. SUMMARY OF FINDINGS J. Available at: <https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf> [Accessed 13 June 2021].

https://www.sbir.gov. 2016. Applicability of Blockchain Technology to Privacy Respecting Identity Management.   Available at: <https://www.sbir.g ov/sbirsearch/detail/867797> [Accessed 3 June 2021].

Hydraledger.io. 2021. What is SSI & DID — Hydraledger.   Available at: <https://hydraledger.io/what-is-ssi-did/> [Accessed 13 June 2021].

Ibm.com. 2021. IBM Blockchain Platform - IBM Blockchain.

Icann.org. 2020. What Does ICANN Do? - ICANN.   Available at: <https://www.icann.org/resources/pages/what-2012-02-25-en> [Accessed 3 June 2021].

ID2020. 2021. ID2020 | Manifesto.   Available at: <https://id2020.org/manifesto> [Accessed 13 June 2021].

Identity.foundation. 2021. DIDComm Messaging Specification.   Available at: <https://identity.foundation/didcomm-messaging/spec/> [Accessed 21 June 2021].

Identity.foundation. 2021. Peer DID Method Specification.   Available at: <https://identity.foundation/peer-did-method-spec/> [Accessed 20 June 2021].

Identity.foundation. n.d. ION - an open, public, permissionless decentralized identifier network.   Available at: <https://identity.foundation/ion/> [Accessed 21 June 2021].

In: 10th Latin American and Caribbean Conference for Engineering and Technology. 2012. Cloud Computing Security and Privacy. Panama: Universidad Tecnológica de Panamá, pp.1-9

Indicators.report. 2021. 16.9 by 2030 provide legal identity for all including free birth registrations — Indicators and a Monitoring Framework. Available at: <https://indicators.report/targets/16-9/> [Accessed 13 June 2021].

Investopedia. 2021. Decentralized Finance (DeFi) Definition and Use Cases. Available at: <https://www.investopedia.com/decentralized-finance-defi-5113835> [Accessed 21 June 2021].

Investopedia. 2021. What are on-chain transactions?. Available at: <https://www.investopedia.com/terms/c/chain-transactions-cryptocurrency.asp> [Accessed 21 June 2021].

Jacovi, A., Marasovic, A., Miller, T. and Goldberg, Y., 2021. Formalizing Trust in Artificial Intelligence | Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. Dl.acm.org. Available at: <https://dl.acm.org/doi/10.1145/3442188.3445923> [Accessed 20 June 2021].

Javelin. 2021. 2021 Identity Fraud Study: Shifting Angles. Available at: <https://www.javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud> [Accessed 2 May 2021].

Johns Hopkins Coronavirus Resource Center. 2020. COVID-19 Racial Data Transparency - Johns Hopkins Coronavirus Resource Center. Available at: <https://coronavirus.jhu.edu/data/racial-data-transparency> [Accessed 21 June 2021].

Joinup.ec.europa.eu. 2021. SSI eIDAS bridge. Available at: <https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI%20eIDAS%20Bridge_Flyer_1.pdf> [Accessed 13 June 2021].

Joosten, R., den Breeijen, S. and Drummond, R., 2021. Decentralized SSI Governance, the missing link in automating business decisions. . (2021). Decentralized SSI Governance, the missing link in automating business decisions. 10.13140/RG.2.2.35491.68640., Available at: <https://www.researchgate.net/publication/348325716_Decentralized_SSI_Governance_the_missing_link_in_automating_business_decisions> [Accessed 13 June 2021].

JOSHI, N., 2019. Blockchain's role in curbing identity theft | prevent identity theft |. Allerin.com. Available at: <https://www.allerin.com/blog/blockchains-role-in-curbing-identity-theft> [Accessed 2 June 2021].

Json-ld.org. 2021. JSON-LD - JSON for Linking Data. Available at: <https://json-ld.org/> [Accessed 20 June 2021].

Jwt.io. 2020. JWT.IO - JSON Web Tokens Introduction. Available at: <https://jwt.io/introduction> [Accessed 20 June 2021].

Kilt.io. 2020. White Paper Kilt.io. Available at: <https://www.kilt.io/wp-content/uploads/2020/01/KILT-White-Paper-v2020-Jan-15.pdf> [Accessed 21 June 2021].

Kravchenko, P., Skriabin, B. and Kurbatov, O., 2019. Engineer's Guide to Financial Internet. Distributed Lab.

Krotoski, A., 2012. Online identity: is authenticity or anonymity more important?. the Guardian. Available at: <https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity> [Accessed 4 June 2021].

Kumar Sharma, T., n.d. Widespread Adoption of Self-Sovereign Identity in the Wake of COVID-19. Blockchain-council.org. Available at: <https://www.blockchain-council.org/blockchain/widespread-adoption-of-self-sovereign-identity-in-the-wake-of-covid-19/> [Accessed 21 June 2021].

Kuperberg(B), M., Kemper, S. and Durak, C., 2021. Blockchain Usage for Government-Issued Electronic IDs: A Survey. Dbsystel.de. Available at: <https://www.dbsystel.de/resource/blob/5169670/47330c9be63205c5ccd5c70d288b3209/Blockchain-Usage-for-Government-Issued-Electronic-IDs-A-Survey-data.pdf> [Accessed 2 June 2021].

Laube, A. and Hassenstein, G., 2020. Self-Sovereign Identities Will the identities of Swiss university members be controlled by themselves in future?. 1st ed. [ebook] Bern University of Applied Sciences Department of Engineering and Information Technology Institute for Data Applications and Security (IDAS), p.p.24. Available at: <https://www.switch.ch/export/sites/default/about/innovation/.galleries/files/SWITCHInnovationLab_IDAS.pdf> [Accessed 13 June 2021].

Lawtrust. 2021. Wet signature vs. Electronic Signature vs. Digital Signature.   Available at: <https://www.lawtrust.co.za/news/general/2020/07/22/wet-signature-vs.-electronic-signature-vs.-digital-signature> [Accessed 20 June 2021].

Ledger. 2021. The Blockchain Generations | Ledger.   Available at: <https://www.ledger.com/academy/blockchain/web-3-the-three-blockchain-generations> [Accessed 21 June 2021].

Lee, S., 2018. A Decentralized Reputation System: How Blockchain Can Restore Trust In Online Markets.   Forbes. Available at: <https://www.forbes.com/sites/shermanlee/2018/08/13/a-decentralized-reputation-system-how-blockchain-can-restore-trust-in-online-markets/?sh=48ce14e8481a> [Accessed 21 June 2021].

Li, K., 2019. The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed | Hacker Noon. Hackernoon.com. Available at: <https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44> [Accessed 21 June 2021].

Lim, J., 2020. Self-Sovereign Identity: The Harmonising of Digital Identity Solutions Through Distributed Ledger Technology. Anujolt.org. Available at: <https://anujolt.org/article/17432-self-sovereign-identity-the-harmonising-of-digital-identity-solutions-through-distributed-ledger-technology> [Accessed 13 June 2021].

Lim, S., Tankam Fotsing, P., Almasri, A., Musa, O., Mat Kiah, M., Ang, T. and Ismail, R., 2018. Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. International Journal on Advanced Science, Engineering and Information Technology, 8(4-2), p.1735.

Lohr, S., 2021. He Created the Web. Now He's Out to Remake the Digital World..   Nytimes.com. Available at: <https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html> [Accessed 1 June 2021].

López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications.   Publications.iadb.org. Available at: <https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf> [Accessed 13 June 2021].

Maker Blog. 2021. What Are Blockchain Bridges, and Why are they Important for DeFi?.   Available at: <https://blog.makerdao.com/what-are-blockchain-bridges-and-why-are-they-important-for-defi/> [Accessed 21 June 2021].

Mayer, D., Warner, D., Siedel, G. and Lieberman, J., 2012. Law of Commercial Transactions - Open Textbook Library.   Open Textbook Library. Available at: <https://open.umn.edu/opentextbooks/textbooks/280> [Accessed 4 June 2021].

Mayer, R., Davis, J. and Schoorman, F., 1995. An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), p.709.

Medium. 2018. Digital ID: The Power, Promise, and Challenge.   Available at: <https://words.democracy.earth/the-power-promise-and-challenge-of-digital-identity-7f85ca673ae> [Accessed 13 June 2021].

Medium. 2018. What is a Token Curated Registry?.   Available at: <https://medium.com/@tokencuratedregistry/a-simple-overview-of-token-curated-registries-84e2b7b19a06> [Accessed 21 June 2021].

Medium. 2019. The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed.   Available at: <https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44> [Accessed 21 June 2021].

Medium. 2020. A Unified Theory of Decentralization. Available at: <https://medium.com/swlh/a-unified-theory-of-decentralization-151d6f39e38> [Accessed 13 June 2021].

Medium. 2020. Self-Sovereign Identity Principle #4: Transparency. Available at: <https://medium.com/metadium/self-sovereign-identity-principle-4-transparency-82d168a51e35> [Accessed 17 June 2021].

Medium. 2021. eSSIF: The European self-sovereign identity framework. Available at: <https://ssi-ambassador.medium.com/essif-the-european-self-sovereign-identity-framework-4572f6875e12> [Accessed 20 June 2021].

Medium. 2021. Non-Fungible Tokens (NFTs) vs Verifiable Credentials (VCs). Available at: <https://academy.affinidi.com/non-fungible-tokens-nfts-vs-verifiable-credentials-vcs-cd0ebb13f1fb> [Accessed 21 June 2021].

Medium. 2021. What are Verifiable Credentials?. Available at: <https://academy.affinidi.com/what-are-verifiable-credentials-79f1846a7b9> [Accessed 20 June 2021].

Mirani, L., 2014. How Facebook and Google are taking over your online identity. Quartz. Available at: <https://qz.com/271286/how-facebook-and-google-are-taking-over-your-online-identity/> [Accessed 3 June 2021].

Monokee. 2021. Trust and data protection: SSI potential regarding privacy - Monokee. Available at: <https://monokee.com/en/2021/04/02/trust-and-data-protection-ssi-potential-regarding-privacy/> [Accessed 17 June 2021].

Mullins, C., 2021. What is data portability? The right to data portability explained. SearchCloudComputing. Available at: <https://searchcloudcomputing.techtarget.com/definition/data-portability> [Accessed 13 June 2021].

Nakamoto, S., 2009. Bitcoin Whitepaper — Satoshi Nakamoto. Satoshinakamoto.me. Available at: <http://satoshinakamoto.me/whitepaper/> [Accessed 1 June 2021].

Naquin, C. and Paulson, G., 2003. Online bargaining and interpersonal trust. Journal of Applied Psychology, 88(1), pp.113-120.

National Science and Media Museum. 2021. A short history of the internet | National Science and Media Museum. Available at: <https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-Internet> [Accessed 6 June 2021].

News.bbc.co.uk. 2021. BBC NEWS | Technology | Itunes user sues Apple over iPod. Available at: <http://news.bbc.co.uk/2/hi/technology/4151009.stm> [Accessed 13 June 2021].

Page, K., Venkataramani, M., Beyrer, C. and Polk, S., 2020. Undocumented U.S. Immigrants and Covid-19. New England Journal of Medicine, 382(21), p.e62. Available at: <https://www.nejm.org/doi/10.1056/NEJMp2005953> [Accessed 21 June 2021].

Peng, T., 2020. Blockchain Charity Platform to Fight Against the Coronavirus Outbreak. Cointelegraph. Available at: <https://cointelegraph.com/news/blockchain-charity-platform-to-fight-against-the-coronavirus-outbreak> [Accessed 21 June 2021].

Perez, S. and Whittaker, Z., 2018. Everything you need to know about Facebook's data breach affecting 50M users. Techcrunch.com. Available at: <https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/> [Accessed 9 June 2021].

Pittinsky, M., 2015. Credentialing in Higher Education: Current Challenges and Innovative Trends. https://er.educause.edu/. Available at: <https://er.educause.edu/articles/2015/3/credentialing-in-higher-education-current-challenges-and-innovative-trends> [Accessed 21 June 2021].

Press release. 2021. Commission proposes a trusted and secure Digital Identity for all Europeans. Available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663> [Accessed 13 June 2021].

Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications.

Rane, S., Wang, Y., Draper, S. and Ishwar, P., 2013. Secure Biometrics: Concepts, Authentication Architectures, and Challenges. IEEE Signal Processing Magazine, 30(5), pp.51-64.

Raval, S., 2021. Decentralized Applications. O'Reilly Online Learning. Available at: <https://www.oreilly.com/library/view/decentralized-applications/9781491924532/ch01.html> [Accessed 3 June 2021].

Reed, D. and Preukschat, A., 2021. MEAP of "Decentralized Digital Identity: The advent of Self-Sovereign Identity (SSI)".. Manning, pp.68-93.

Refugees, U., 2020. Figures at a Glance. UNHCR. Available at: <https://www.unhcr.org/figures-at-a-glance.html> [Accessed 13 June 2021].

Rofle, A., 2020. The inevitable rise and rise of the global digital wallet. Payments Cards & Mobile. Available at: <https://www.paymentscardsandmobile.com/the-inevitable-rise-and-rise-of-the-digital-wallet/> [Accessed 3 June 2021].

Rowe, G., Nikols, N. and Simmons, D., 2018. The Future of Identity Management (2018-2023). Techvisionresearch.com. Available at: <https://techvisionresearch.com/wp-content/uploads/2018/01/The-Future-of-Identity-Management-2018-final.pdf> [Accessed 11 June 2021].

Ruff, T., 2018. The Three Models of Digital Identity Relationships. Medium. Available at: <https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186> [Accessed 2 June 2021].

S., J., 2018. Blockchain: What are nodes and masternodes?. Medium. Available at: <https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f> [Accessed 21 June 2021].

Sabadello, M. and Zagidulin, D., 2021. Decentralized Identifier Resolution (DID Resolution) v0.2. W3c-ccg.github.io. Available at: <https://w3c-ccg.github.io/did-resolution/> [Accessed 20 June 2021].

Savage, N., 2018. Making digital government a better government. Nature.com. Available at: <https://www.nature.com/articles/d41586-018-07502-x> [Accessed 3 June 2021].

Schanzenbach, M., 2020. Towards Self-sovereign, Decentralized Personal Data Sharing and Identity Management. Mediatum.ub.tum.de. Available at: <http://mediatum.ub.tum.de/doc/1545514/t1o114y0kknu54px6o05n88ek.Schanzenbach-Martin.pdf> [Accessed 21 June 2021].

Securekey.com. 2021. A Primer and Action Guide to Decentralized Identity. Available at: <https://securekey.com/wp-content/uploads/2020/07/VerifiedMe_OWIWhitepaper_APrimertoDecentralizedIdentity.pdf> [Accessed 4 June 2021].

Shaping Europe's digital future. 2021. eIDAS Regulation. Available at: <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation> [Accessed 11 June 2021].

Simic, B., 2018. Council Post: Can Blockchain Solve Identity Fraud?. Forbes. Available at: <https://www.forbes.com/sites/forbestechcouncil/2018/05/31/can-blockchain-solve-identity-fraud/?sh=47c2174e7289> [Accessed 13 June 2021].

Sindi, A., 2019. Adoption Factors of a Blockchain Digital Identity Management System in Higher Education: Diffusing a Disruptive Innovation - ProQuest. Proquest.com. Available at: <https://www.proquest.com/openview/a85e5edc48014246f9eb1d93ede6e535/1.pdf?pq-origsite=gscholar&cbl=51922&diss=y> [Accessed 13 June 2021].

Sood, I., Pirkkalainen, H. and Camilleri, A., 2020. Can Blockchain Technology Facilitate the Unbundling of Higher Education. Proceedings of the 12th International Conference on Computer Supported Education, Volume 2. Available at: <https://www.scitepress.org/PublicationsDetail.aspx?ID=+gNsg2h3oL8=&t=1> [Accessed 21 June 2021].

Sovrin. 2018. Is Sovrin 'Permissioned'? - Sovrin. Available at: <https://sovrin.org/faq/is-sovrin-permissioned/> [Accessed 21 June 2021].

Sovrin. 2018. What is Sovrin? - Sovrin. Available at: <https://sovrin.org/faq/what-is-sovrin-2/> [Accessed 21 June 2021].

Sovrin. n.d. Sovrin Governance Framework - Sovrin. Available at: <https://sovrin.org/library/sovrin-governance-framework/> [Accessed 21 June 2021].

Sovrin.org. 2019. Sovrin Governance Framework V2 Master Document V2. Available at: <https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V2.pdf> [Accessed 21 June 2021].

Sporny, M., Chadwick, D. and Longley, D., 2019. Verifiable Credentials Data Model 1.0 Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web. W3.org. Available at: <https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations> [Accessed 20 June 2021].

Ssh.com. n.d. (PKI) is a technology for authenticating users and devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents. Available at: <https://www.ssh.com/academy/pki> [Accessed 20 June 2021].

Status.cloud.google.com. 2021. Google Cloud Status Dashboard. Available at: <https://status.cloud.google.com/incident/zall/20013> [Accessed 20 June 2021].

Tanner, J. and Roeloefs, C., 2021. NFTs and the need for Self-Sovereign Identity — Gimly Blockchain Projects. Gimly Blockchain Projects. Available at: <https://www.gimly.io/blog/nfts-the-need-for-self-sovereign-identity> [Accessed 21 June 2021].

Thales Group. n.d. Self-sovereign identities at work - Digital identity 2.0. Available at: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-identity> [Accessed 17 June 2021].

Trust Over IP. 2021. Trust Over IP - Defining a complete architecture for Internet-scale digital trust. Available at: <https://trustoverip.org/> [Accessed 20 June 2021].

Trustoverip.org. 2020. Introducing the Trust over IP Foundation V1. Available at: <https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf> [Accessed 20 June 2021].

Trustoverip.org. 2020. Trust over IP Foundation.. Available at: <https://trustoverip.org/wp-content/uploads/sites/98/2020/05/Introducing-The-Trust-over-IP-Foundation-V1.pdf> [Accessed 17 June 2021].

Tykn. 2021. SSI Explained in 10 Quotes by 3 Industry Experts - Tykn. Available at: <https://tykn.tech/ssi-in-10-quotes-by-3-industry-experts/> [Accessed 21 June 2021].

Un.org. 2021. ID2020 Summit 2016. Available at: <https://www.un.org/partnerships/news/id2020-summit-2016> [Accessed 13 June 2021].

UNHCR Blog. 2018. Bridging the identity divide — Is Portable User-Centric Identity Management the Answer? - UNHCR Blog. Available at: <https://www.unhcr.org/blogs/bridging-identity-divide-portable-user-centric-identity-management-answer/> [Accessed 13 June 2021].

Venkataramakrishnan, R., 2018. Scroll Explainer: What is the Aadhaar case and what is at stake for Indians?. Scroll.in. Available at: <https://scroll.in/article/893285/scroll-explainer-what-is-the-aadhaar-case-and-what-is-at-stake-for-indians> [Accessed 13 June 2021].

Verborgh, R., 2021. Power to the people: Re-decentralizing the Web, for good this time. SocietyByte. Available at: <https://www.societybyte.swiss/en/2021/01/07/part-1-power-to-the-people-re-decentralizing-the-web-for-good-this-time/> [Accessed 1 June 2021].

Vieira, F., 2020. Educação Ambiental para além da pandemia: aprendizados decoloniais com outras comunidades e com outras pedagogias. Revista Brasileira de Educação Ambiental (RevBEA), 15(4), pp.259-278.

W3.org. 2019. W3C Working Group Note 24 September 2019. Available at: <https://www.w3.org/TR/vc-imp-guide/> [Accessed 20 June 2021].

W3.org. 2021. DID Specification Registries. Available at: <https://www.w3.org/TR/did-spec-registries/> [Accessed 20 June 2021].

W3.org. 2021. Semantic Web - W3C. Available at: <https://www.w3.org/standards/semanticweb/> [Accessed 13 June 2021].

W3.org. 2021. Use Cases and Requirements for Decentralized Identifiers. Available at: <https://www.w3.org/TR/did-use-cases/> [Accessed 20 June 2021].

W3.org. 2021. Verifiable Credentials Data Model 1.0. Available at: <https://www.w3.org/TR/vc-data-model/> [Accessed 21 June 2021].

W3.org. 2021. W3C Recommendation 19 November 2019. Available at: <https://www.w3.org/TR/vc-data-model/> [Accessed 6 June 2021].

W. Bilder, G., 2006. In Google We Trust?. The journal of electronic publishing, 9(1).

Wagner, K., Vila, X., Vandy, N., Bachenheimer, D. and Beron, D., 2020. Decentralised Identity: What's at Stake? A Position Paper by the INATBA Identity Working Group. International Association for Trusted Blockchain Applications, p.p.10.

Wang, F. and De Filippi, P., 2020. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain, 2.

Who.int. 2018. Digital Opportunities for Displaced Women, Children and Adolescents. Available at: <https://www.who.int/pmnch/media/news/2019/PMNCH-knowledge-brief-2.pdf?ua=1> [Accessed 13 June 2021].

Williams, M., 2007. Cross-border issues fracture iTunes offerings in Europe. https://www.networkworld.com/. Available at: <https://www.networkworld.com/article/2297397/cross-border-issues-fracture-itunes-offerings-in-europe.html> [Accessed 3 June 2021].

Windley, P., 2018. Decentralized Governance in Sovrin. Windley.com. Available at: <https://www.windley.com/archives/2018/02/decentralized_governance_in_sovrin.shtml> [Accessed 21 June 2021].

Windley, P., 2021. Comparing X.509 Vertificates with SSI. Windley.com. Available at: <https://www.windley.com/archives/2021/05/comparing_x509_vertificates_with_ssi.shtml> [Accessed 20 June 2021].

World Wide Web Foundation. 2017. Three challenges for the web, according to its inventor. Available at: <https://webfoundation.org/2017/03/web-turns-28-letter/> [Accessed 1 June 2021].

Wright, P., 2021. Can digital signatures be forged? · Viafirma's Blog. Viafirma's Blog. Available at: <https://www.viafirma.com/blog-xnoccio/en/digital-signatures-forged/> [Accessed 20 June 2021].