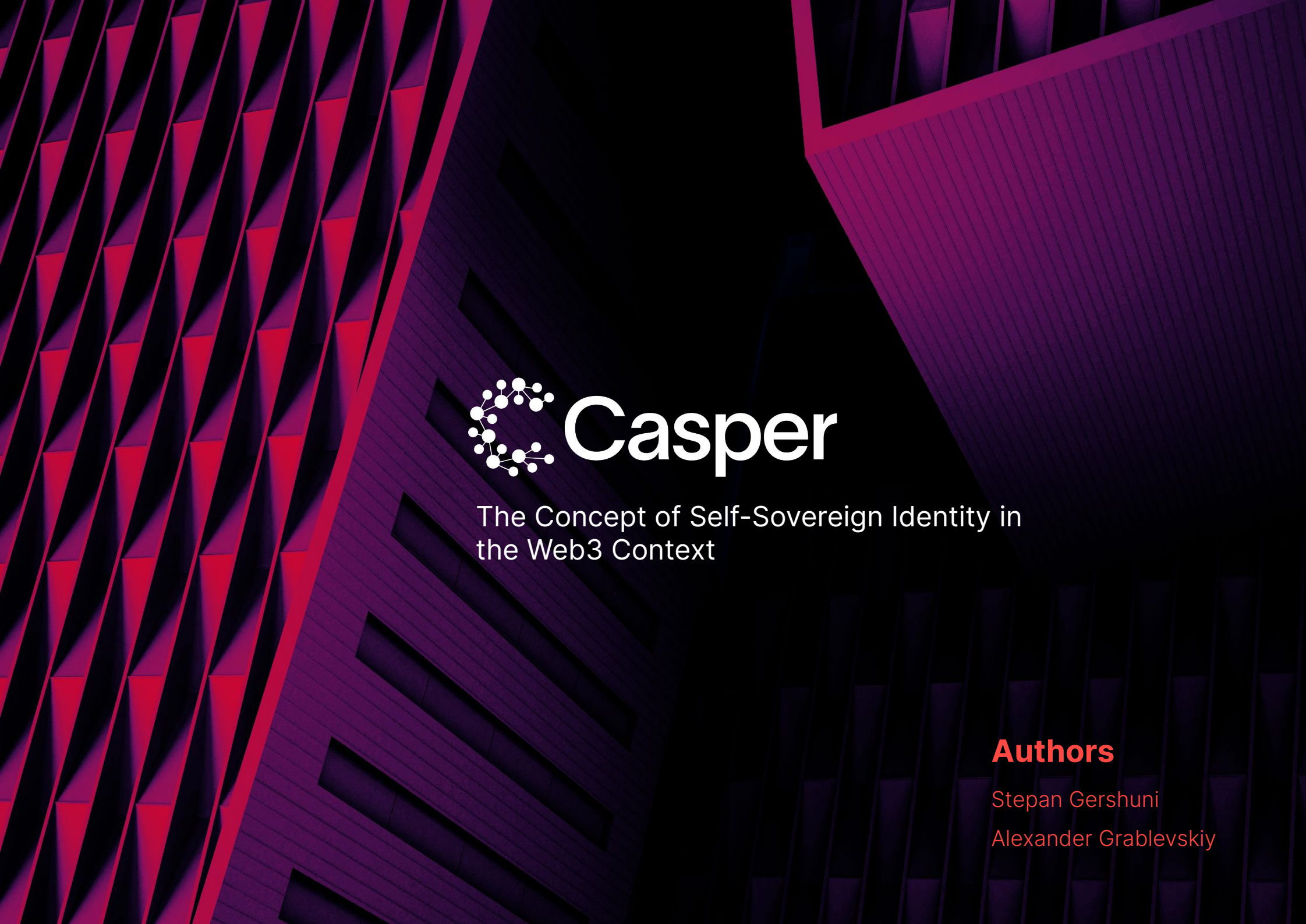


The Concept of Self-Sovereign Identity in the Web3 Context

Authors

Stepan Gershuni

Alexander Grablevskiy

Content

Glossary and Key Terms

Chapter 1 **Identity Concept in the Internet** 5

Chapter 2 **The SSI Concept in the Context of Digital Identity** 14

Chapter 3 **SSI Technical Overview** 26

Chapter 4 **SSI Governance** 38

Chapter 5 **SSI for Casper Network** 51

Chapter 6 **Legal Aspects of SSI Implementation** 61

Chapter 7 **SSI Use Cases** 75

Chapter 8 **Decentralized Reputation and SSI** 93

Conclusion 138

Glossary and Key Terms

Glossary and Key Terms

Verifiable credential is a tamper-evident digital set of claims made by an Issuer that has authorship that can be cryptographically verified.
Verifiable presentation 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 and encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification.
Verifiable data registry is a role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, Issuers' public keys, and so on, which might be required to use verifiable credentials.
Isser is a role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a Holder.
Holder is a role an entity might perform by possessing one or more VCs and generating presentations from them. A Holder is 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.[1]
Decentralized identifier (DID) is a globally unique persistent identifier that does not require a centralized registration authority.
DID document is a set of data describing the DID subject, including mechanisms, such as cryptographic public keys, that the DID subject can use to authenticate itself and prove its association with the DID.[2]
Reputation event (repute) is a piece of data encapsulating information that is used to generate reputation scores for a reputee.
Reputable entity (eputee) is a uniquely identifiable entity which is the target of reputes. The repute is about a distinct reputational activity of the reputee.
Reputer is the originator or primary source of the information items in a repute about the reputee.[3]

1 W3.org. 2019. W3C Recommendation 19 November 2019.

2 W3.org. 2021. Decentralized Identifiers (DIDs) v1.0. *Decentralized Identifiers (DIDs) v1.0.* [online] [Accessed 14 August 2021].

3 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 3-5

Chapter 1

Identity Concept in the Internet

Introduction

Many people associate the birth of the Internet with the creation of its ancestor in 1969, the ARPANET network, when the first node was put into operation in Los Angeles, USA. Since the 70s, there has not been a year that has not had another technological advancement in the field of telecommunications. ARPANET, the link of the National Science Foundation NSFNET to a supercomputer center at thousands bits per second, ushered in a new era for humanity. CERN launched the World Wide Web in 1991. Tim Berners-Lee proposed a new way of structuring and linking all the information available on CERN's computer network that made it quick and easy to access.

On August 6, 1991, the code for creating new web pages, as well as the software to view them, became publicly available on the Internet. Computer enthusiasts around the world began setting up their own websites. Berners-Lee's vision of a free, global and shared information space began to take shape.[4] A real boom in the development of the Internet occurred in 1993-1995 in connection with the promotion of the World Wide Web technology, when the number of users and servers doubled in months.

In the next decade Skype, WordPress, Facebook, Mozilla Firefox, Twitter and YouTube premiered and has become our everyday digital reality. In 2021, according to Digital 2021 April Global Statshot Report, more than 60 percent of the world's total population is online and these figures are only increasing every day.[5] More than 330 million people started using the Internet in the past 12 months, taking the total number of global Internet users to 4.72 billion by the start of April 2021.[6]

At the beginning, personal profiles did not initially enforce the realness of the persons behind the screen, but as Facebook developed to become the most popular social network, the problem of real identity became essential to their policy and idea.

4 National Science and Media Museum. 2021. A short history of the internet | National Science and Media Museum. [Accessed 15 July 2021].

5 Kemp, S., 2021. 60% of the World's Population Is Now Online — DataReportal – Global Digital Insights. [online] DataReportal – Global Digital Insights. [Accessed 5 August 2021].

6 Kemp, S., 2021. 60% of the World's Population Is Now Online — DataReportal – Global Digital Insights. [online] DataReportal – Global Digital Insights. [Accessed 5 August 2021].

History of Digital Identity

For the first several decades, this interconnected world was envisioned as an unrestricted civic forum: a place where opposing viewpoints, ideas, and discussions could productively collide.[7] The Internet is a fantastic leveler: no one knows your gender, whether you are a boss or underling, gray-haired or adolescent.[8] 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.

Identity has emerged as one of the most pressing issues confronting technology progress. Eventually, the various social systems and structures that humans create are intended to make social interactions easier, more efficient, or less unclear. It is difficult to prove identity over time and space, and human identity, in particular, is complicated and multifaceted.[9]

In virtual communities, identity is particularly important. Knowing the identity of persons you talk with is critical for comprehending and evaluating an interaction in communication, which is the fundamental activity. However, identification is uncertain in the virtual community's disembodied environment. Many of the basic indications about personality and social role that we are used to seeing in the physical world are missing.[10] In contemporary social institutions, identity is less concerned with enclosing the person and more concerned with the act of naming. The goal of these names (or numbers) is to demonstrate an individual's originality, to assure accountability, and to establish mutual trust between individuals and institutions, as well as to offer points of reference for the framework of laws and other social contracts that govern our society.[11]

7 Rainie, L., Anderson, J. and Albright, J., 2021. The Future of Free Speech, Trolls, Anonymity and Fake News Online. [online] Pew Research Center: Internet, Science & Tech. [Accessed 5 August 2021].

8 Donath, J., 1996. Identity and Deception in the Virtual Community. [online] Smg.media.mit.edu. [Accessed 5 August 2021].

9 Donath, J., 1996. Identity and Deception in the Virtual Community. [online] Smg.media.mit.edu. [Accessed 5 August 2021].

10 Breckenridge, G., 2018. A Brief History of Digital Identity. [online] Medium. [Accessed 5 August 2021].

11 Breckenridge, G., 2018. A Brief History of Digital Identity. [online] Medium. [Accessed 5 August 2021].

History of Digital Identity

One of the most significant inventions of the 70s that has shaped the current image of identity is public-key cryptography. In 1977, the National Bureau of Standards created the Data Encryption Standard (DES), which was quite revolutionary at the time. DES was the first attempt at creating a universal encryption standard. DES was extremely successful and still remains as the most widely used cryptosystem of all time.[12] We would not have been able to protect the public networks on which global communication and commerce rely if it had not been for it.[13] From the OpenPGP standard to the entire blockchain ecosystem, public key cryptography has been the backbone of identity in the Internet.[14]

In 1991 “Pretty Good Privacy” (PGP) arrived, invented by Phil Zimmerman. One of PGP's most prominent features is its answer to the problem of connecting persons who have never met and hence have never had the opportunity to exchange secure keys. This method immediately received the moniker "Web of Trust," which precisely explains how the system works as any word can.[15] Phil Zimmerman stated in 1992 in the manual for PGP version 2.0:

> “As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.”

12 Roberts, E., 1996. The History of Cryptography. [online] Cs.stanford.edu. [Accessed 5 August 2021].

13 Breckenridge, G., 2018. A Brief History of Digital Identity. [online] Medium. [Accessed 5 August 2021].

14 Breckenridge, G., 2018. A Brief History of Digital Identity. [online] Medium. [Accessed 5 August 2021].

15 Oram, A. and Viega, J., 2009. Beautiful Security. [online] O’Reilly Online Learning. [Accessed 5 August 2021].

History of Digital Identity

However, the certificate authority (CA) paradigm that emerged from public key infrastructure and became the Internet standard was constrained by its reliance on centralized trust.[16] Certificate authorities (CAs) are the components of PKI that enable us to provide basic security services in wired networks and the Internet.[17] Individual users had limited recourse if the CAs were corrupted or had questionable integrity when it came to certificate issuing and signing.[18] Many of the "identity" schemas of the 1980s and 1990s were based on the CA model in some form or another, and social networking sites sparked the next significant revolution in digital identity.[19] The vast majority of today's Internet platforms are built with centralized regulation and control in mind, and Facebook is one of the most famous.

16 Breckenridge, G., 2018. A Brief History of Digital Identity. [online] Medium. [Accessed 5 August 2021].

17 Masdari, M., Jabbehdari, S., Ahmadi, M., Hashemi, S., Bagherzadeh, J. and Khadem-Zadeh, A., 2011. A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks. EURASIP Journal on Wireless Communications and Networking, 2011(1).

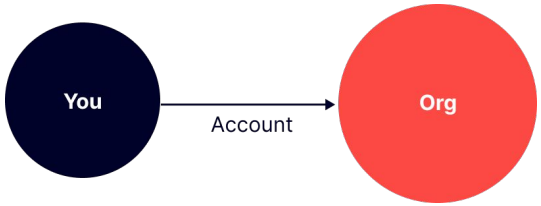
18 Breckenridge, G., 2018. A Brief History of Digital Identity. [online] Medium. [Accessed 5 August 2021]

19 Breckenridge, G., 2018. A Brief History of Digital Identity. [online] Medium. [Accessed 5 August 2021].

Types of digital identity

Users have long utilized almost all types of IDs and credentials, including government ID numbers, passports, identification cards, driver's licenses, invoices, Facebook logins, LinkedIn profiles, and so on. All of these are granted by central governments or service providers such as banks or telecommunications companies.
Depending on how the data is stored and the system operates, how various models apply, 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.

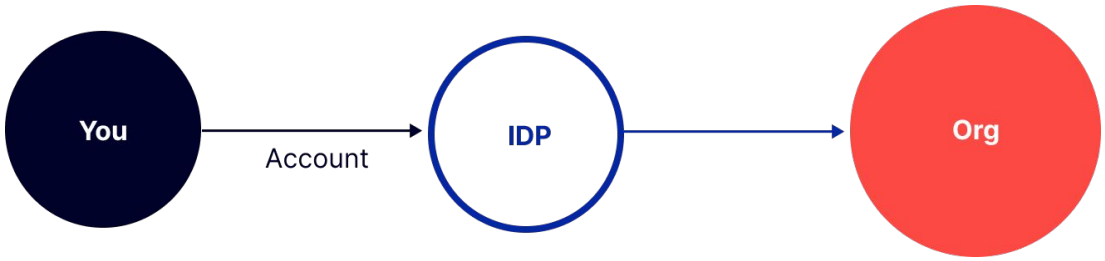
Centralized identity model



A centralized identity is an "account" that is owned and controlled by a single service provider. A bank, for example, when you open an account to access online banking. It centralizes user data in a "honeypot" that is readily hacked due to the creation of a single point of failure.
From technological platforms to bank cards, today's cutting-edge identification systems establish asymmetric trust relationships and contracts of adhesion on their users, which include both individual users and local authorities, corporations, unions, and community organizations. Moreover, these trust relationships are frequently structured as a hierarchical trust infrastructure, forcing users to accept either a specific set of trusted certifying authorities ("trust anchors") or identification cards with private keys provided by a trusted third party.[20]

20 Goodell, G. and Aste, T., 2019. A Decentralized Digital Identity Architecture. Frontiers in Blockchain, 2.

Federated identity model

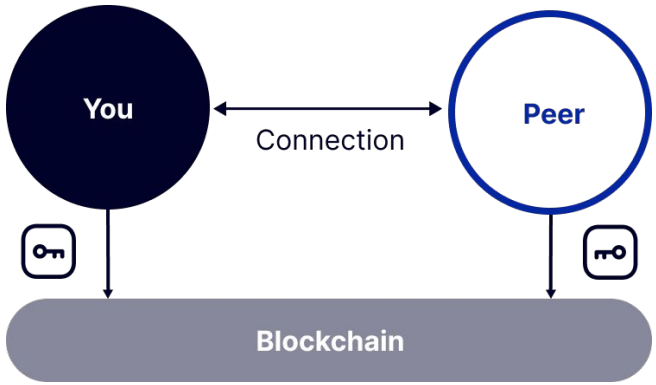


Federated identity systems are single sign-on (SSO) techniques that enable access to numerous distinct services, such as Facebook Connect. The purpose of the federation is to enable the sharing of security principal identities and attributes across trust boundaries and between organizations.[21] Federated identity management 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.[22]

21 Spinaci, L., 2018. Digital Identity. [online] Medium. [Accessed 5 August 2021].

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

Decentralized identity model



Digital identity systems are becoming more complex since they need to provide access to an increasingly heterogeneous technology environment. Thus, digital identity systems are moving from centralized systems to more federated or even decentralized solutions.[23]

Decentralized IDs enable people to be linked to their associated data without relying on third parties. As a result, users get more privacy and acquire broader sovereignty over the present centralized systems, which expose them to risks of cyber attacks and exploitation.[24] As in the pre-digital era, the decentralized identity model gives people back control by providing digital credentials that can be self-managed and shared exclusively with trustworthy parties.[25]

23 Stockburger, L., Kokosioulisa, G., Mukkamalaab, A. and Rao, R., 2021. Blockchain-Enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation. Elsevier B.V. on behalf of Zhejiang University Press., [online] [Accessed 5 August 2021].

24 Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K., Maler, E., Reed, D. and Sporny, M., 2019. Decentralized Identity: Where Did It Come From and Where Is It Going?. [online] Ieeexplore.ieee.org. [Accessed 5 August 2021].

25 Spinaci, L., 2018. Digital Identity. [online] Medium. [Accessed 5 August 2021].

Types of digital identity

Decentralized identities rely on blockchain's two primary capabilities: distributed ledger and cryptography. Distributed ledger enables trust in the network without the control of one central authority. Through the consensus mechanism (the agreements between parties on the status of the ledger), the information is replicated, shared, and synchronized geographically, spread across multiple countries or organizations. No central administrator or centralized data storage exists since the network is formed by peers that have the same grants and transact freely with each other. The ledger is immutable, which means that data can be updated through consensus gained among the participant but can never be erased or rewritten. Cryptography creates an appropriate level of security in the authorization and sharing of information. In addition, it provides data integrity since the data in the transaction are verified, along with the ownership of the transactions themselves.[26]

Self-sovereign identity (SSI) systems are envisioned to function as public utilities, with the underlying blockchain acting as a foundational "identity Internet." SSI, in effect, offers security measures that allow entities to agree on the type and context of exchanged information during an online engagement. In this sense, SSI seeks to provide users control over their identities and associated data. The ability to own and govern one's private information is a core concept of self-sovereign identity, and these components are also embedded in the concept of blockchain technology.[27] The next part will describe the concept of SSI in more detail.

26 Spinaci, L., 2018. Digital Identity. [online] Medium. [Accessed 5 August 2021].

27 Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K., Maler, E., Reed, D. and Sporny, M., 2019. Decentralized Identity: Where Did It Come From and Where Is It Going?. [online] Ieeexplore.ieee.org. [Accessed 5 August 2021].

Chapter 2

The SSI Concept in the Context of Digital Identity

Casper

Background and principles

Presently, governments and companies confuse driver's licenses, social security cards, and other state-issued credentials with identity. This is troublesome because it implies that a person's basic identity might be lost if a state revokes his credentials or if he just crosses state borders.[28] As the virtual world grows increasingly relevant to the real world, it also gives a fresh opportunity for rethinking current ideas of identity. It may allow us to reclaim control of our identities, reconnecting them with the mysterious "I."

Five years ago, Christopher Allen, an Executive Director and Principal Architect of Blockchain Commons, a "not-for-profit" social benefit corporation committed to open infrastructure, defined a concept of SSI — self-sovereign identity in his blog, where he discussed the history of digital identity and laid out principles for creating a new sort of identity, based on individual control and human rights. He used it to define a principle-based framework for developing a decentralized system of user-centric, self-managed, interoperable digital identities. This methodology is guided by ten fundamental concepts derived from Kim Cameron's Laws of Identity (2005), that would aim to constitute the missing identity layer on the Internet:

1. **Existence**
2. **Control**
3. **Access**
4. **Transparency**
5. **Persistence**
6. **Portability**
7. **Interoperability**
8. **Consent**
9. **Minimalisation**
10. **Protection**[29]

28 Allen, C., 2016. The Path to Self-Sovereign Identity. [online] Lifewithalacrity.com. [Accessed 5 August 2021].

29 Giannopoulou, A. and Wang, F., 2021. Self-sovereign identity. [online] Internet Policy Review. [Accessed 5 August 2021].

Background and principles

The philosophy behind SSI has evolved from a growing need for greater control over our identities and personal information. SSI is a concept, or rather a philosophical movement, that can meet this requirement. It is based on an individual's' ability to own and manage their own identity without relying on a centralized authority or the state. This trend is being driven by people who want more control over their lives and data. SSI is a beautiful notion that Christopher Allen believes is based on principles of Enlightenment and the Universal Declaration of Human rights. He believes that we as individuals have inherent dignity that does not depend on where we were born and who we are, simply because we are humans.[30] In the current system of centralized identity model, the state and corporations are often the holders of our personal information, and they tend to ignore the voice of ordinary people. Christopher Allen states:

"Our relationships with authorities are changing. We are more and more part of global civil society. We are increasingly part of networks, not hierarchies. Borders and nature of social contract are changing — trans-national federations (EU), nation states, regional states (Wyoming, Scotland, Swiss Cantons), indigenous/tribal/ethnic (First Nations, Kurd) city-states/megalopolis (London, SF Bay Area, BoshWash). Corporations & employment cross borders too. All of these parties are re-negotiating the nature of their sovereignty."

The overall concept of SSI is built on personal mobile devices that we can use to securely store and manage all of our private keys, authenticators, digital tokens, and credentials.[31] To be self-sovereign, an identity must have a user-centered design. Interoperability is essential. Users will be able to confirm their identity on many platforms and in different locales. As a result, a SSI is portable, private, and secure.[32]

30 Allen, C., 2020. Self-Sovereign Identity: Ideology and Architecture with Christopher A.... [online] Slideshare.net. [Accessed 5 August 2021].

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

32 Tykn. 2021. Self-Sovereign Identity: The Ultimate Beginners Guide!. [online] [Accessed 5 August 2021].

Background and principles

Practitioners in the SSI community believe that using SSI will help people acquire control over their personal data while also boosting access to human rights and the world economy.[33] They believe that the influence of SSI technology, as well as the numerous new patterns of trustworthy interactions that it will enable, will be felt throughout all lives.[34]

SSI must protect against financial and other losses, prevent powerful people from abusing human rights, and support an individual's right to be themselves and freely associate. Any technology solution addressing concerns of human identity management and private data is fraught with ethical quandaries.[35]

Personal data is not stored on a centralized server.[36] Unlike centralized and federative methods, the SSI technique does not require an organization to maintain people's identities. It is not necessary for an identity provider or a service provider to manage one's credentials and authenticators on their behalf. The job of an identity supplier has now been limited to that of an identity issuer.[37]

33 Allen, C., 2016. The Path to Self-Sovereign Identity. [online] Lifewithalacrity.com. [Accessed 5 August 2021].

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

35 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.

36 Tykn. 2021. Self-Sovereign Identity: The Ultimate Beginners Guide!. [online] [Accessed 5 August 2021].

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

The application of SSI has been linked to the use of a blockchain. SSI, on the other hand, is blockchain-adjacent but not blockchain-dependent.[38] The decentralized identifier (DID) system is the fundamental component of SSI. Blockchain-based DID is an individual's unique ID in the digital world that cannot be annulled by anybody or an organization other than the individual. However, DID presence by itself is useless. It must be supplemented by additional technologies, such as verifiable credentials (VCs).[39] A VC can convey the same information as a physical credential.

With the inclusion of technology like digital signatures, VCs become more tamper-evident and reliable than their physical equivalents.[40] The Issuer generates a VC and sends it to the Holder. It includes a collection of assertions regarding characteristics, such as the Issuer's name, birth date, grade, ID, or any other information the Issuer wishes to assign to the recipient. A presentation is prepared in order to send a claim to a Verifier. The processes are provided in line with the standard,[41] beginning with establishing a DID and concluding with verifying a claim derived from a VC. The processes are divided into three parts based on the players involved: the Issuer of a VC, the Holder of a VC, and the Verifier of chosen claims.[42]

DIDs provide a way for individuals to create their own unique identifiers in order to participate in the virtual environment. DIDs are intended to be "self-sovereign," meaning that, unlike conventional identifiers such as passport numbers and phone numbers, which are granted by external authorities, an entity can generate an identifier and prove sovereignty over it with cryptographic keys. Another area where DIDs, in conjunction with blockchain technology, that is beneficial, is offered by decentralized public key infrastructure. When cryptographic keys are implemented into a blockchain as a means of certifying credentials, new opportunities emerge; for instance, instead of having a point-to-point connection with an individual or organization, any user can validate their information on the blockchain ledger.[43]

38 Giannopoulou, A. and Wang, F., 2021. Self-sovereign identity. [online] Internet Policy Review. [Accessed 5 August 2021]

39 Liu, D. and Qian, Y., 2021. Self-Sovereign Identity — The Nash Equilibrium Point of the Personal Identity Information Game. [online] Thoughtworks.com. [Accessed 5 August 2021]

40 Sporny, M., Longley, D. and Chadwick, D., 2019. Verifiable Credentials Data Model 1.0. [online] W3.org. [Accessed 5 August 2021].

41 Sporny, M., Longley, D., Sabadello, M., Reed, D., Allen, C. and Steele, O., 2021. Decentralized Identifiers (DIDs) v1.0. [online] W3.org. [Accessed 5 August 2021].

42 Brunner, C., Gallersdörfer, U., Knirsch, F., Engel, D. and Matthes, F., 2020. DID and VC:Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. 2020 the 3rd International Conference on Blockchain Technology and Applications.

43 Lim, J., 2020. Self-Sovereign Identity: The Harmonising of Digital Identity Solutions Through Distributed Ledger Technology. [online] Anujolt.org. [Accessed 15 July 2021].

Background and principles

The SSI community has focused on personal identity and data privacy for individuals, but the fundamental computer science principles can be applied to any type of entity, including digital assets like datasets and physical things participating in the Internet of Things.[44] Nonetheless, despite many of its benefits and exquisite architecture, there are still barriers to its implementation; however, there are also benefits, and they will both be discussed below.

Self-sovereignty does not imply complete authority over your own identity. Trusted authorities are still relied on to authenticate and issue VCs. Before they may transact in today's digital world, users must still get such VCs from several trusted sources and keep them in a safe wallet on their smartphone.[45] The scenario of how users can move their verified credentials from one device wallet to the other or when they lose their trusted device is another challenge worth noting.[46]

However, what is significantly lacking is a digital ecosystem with long-term economic models and suitable incentives for all participants that can eventually drive adoption. This comprises the creation and storing of a person's numerous digital identities, as well as the management of proof that these digital identities are trustworthy. Methods for conducting and tracking transactions transferring rights of use to other people and services are also necessary.[47] Building trust in these systems must be adapted to the environment, industry, or jurisdiction; in other words, a one-size-fits-all approach to trust will not work.[48]

44 Barclay, I., Freytsis, M., Bucher, S., Radha, S., Preece, A. and Taylor, I., 2020. Towards a Modelling Framework for Self-Sovereign Identity Systems.

45 Pakkath, R., 2019. Self-Sovereign Identity: A Distant Dream or an Immediate Possibility? | Idaptive. [online] Idaptive.com. [Accessed 5 August

46 Pakkath, R., 2019. Self-Sovereign Identity: A Distant Dream or an Immediate Possibility? | Idaptive.[online] Idaptive.com. [Accessed 5 August 2021].

However, what is significantly lacking is a digital ecosystem with long-term economic models and suitable incentives for all participants that can eventually drive adoption. This comprises the creation and storing of a person's numerous digital identities, as well as the management of proof that these digital identities are trustworthy. Methods for conducting and tracking transactions transferring rights of use to other people and services are also necessary.[47] Building trust in these systems must be adapted to the environment, industry, or jurisdiction; in other words, a one-size-fits-all approach to trust will not work.[48]

There have been significant reforms that have aided the spread of identification solutions. However, there are still a number of legal compliance issues with decentralized identity implementation and acceptance.[49] Specifically, the eIDAS Regulation defines different levels of trust services and provides the regulatory environment that enables the creation of numerous of the framework. The eIDAS Regulation goal is to create a strengthened level of trust in services, which is noteworthy in that trust in these services appears to be based on the fact that they are legally controlled, rather than only on their technological features.[50]

It should be noted that establishing an SSI system on a blockchain is still a technological difficulty. The ledger's immutability makes enforcing legal provisions like the "right to be forgotten" extremely challenging.[51] If a user wishes to withdraw a previously issued claim, he simply requests that the claim be revoked and forgotten by the service provider. There are no automatic mechanisms or standards in place to satisfy this right to be forgotten scenario, which might lead to the data breaches that self-sovereign identification was designed to prevent.[52]

To make an SSI scenario a reality, the ecosystem must improve governance, interoperability, scalability, and legislation, resulting in an organic and stable structure to encourage DLT and digital identity.[53]

47 Der, U., Jähnichen, S. and Sürmeli, J., n.d. Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution. [online] Arxiv.org. [Accessed 5 August 2021].

48 Renieri, E. and 4, 2021. Liability under GDPR and the Self-Sovereign Identity Model. [online] SSI Meetup. [Accessed 5 August 2021].

49 Giannopoulou, A. and Wang, F., 2021. Self-sovereign identity. Internet Policy Review, 10(2).

50 Domingo, I., 2020. SSI eIDAS Legal Report How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. [online] Joinup.ec.europa.eu. [Accessed 5 August 2021].

51 Noro, P., 2020. What is Self-Sovereign Identity and should States be afraid of it?. [online] Sciencespo.fr. [Accessed 5 August 2021]

52 Pakkath, R., 2019. Self-Sovereign Identity: A Distant Dream or an Immediate Possibility? | Idaptive. [online] Idaptive.com. [Accessed 5 August 2021].

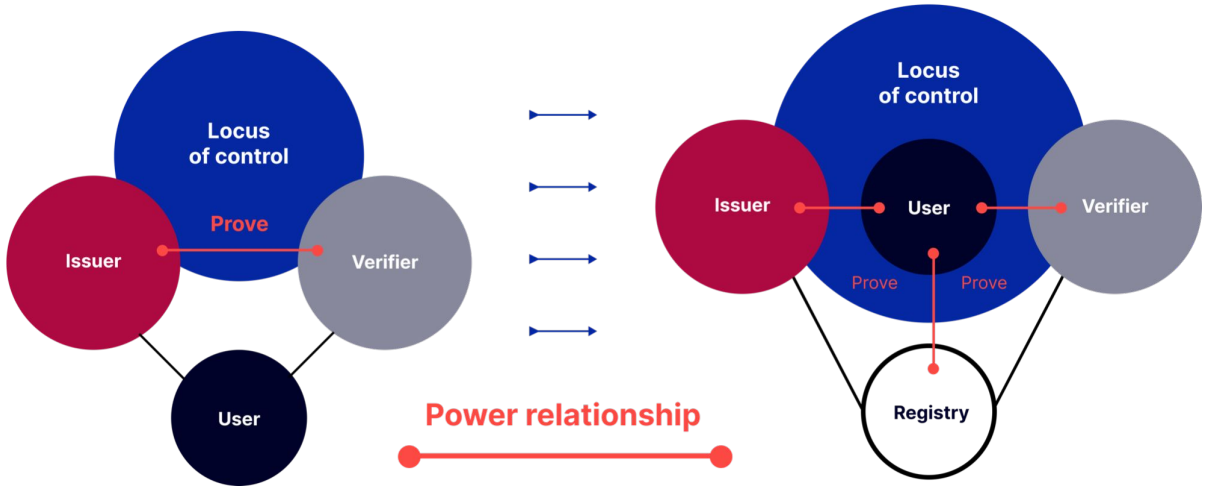
53 Lim, J., 2020. Self-Sovereign Identity: The Harmonising of Digital Identity Solutions Through Distributed Ledger Technology. [online] Anujolt.org. [Accessed 15 July 2021].

Benefits of SSI

The whole book “Self-sovereign identity,” written by SSI pioneers Alex Preukschat and Drummond Reed, is dedicated to promoting the major significance of SSI technology and how it symbolizes a change in control. They anticipate that the influence of SSI technology, as well as the uncountable new patterns of trusted relationships it will enable in all sectors of life, will be similarly significant.

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

Centralized/federated model



This shift of control is well portrayed in the above-mentioned book's figure by Tim Bouma, co-author. The locus of control in the centralized and federated identity models is with the network's Issuers and Verifiers. The point of control transfers to the individual user in the decentralized SSI identity paradigm, who may now engage with everyone else as a complete peer.[54]

Benefits of SSI

SSI allows individuals to access an app on their phone that records their private info, then use an ID number and personal data to validate who they are. SSI offers the user both additional safety and flexibility, empowering them to reveal data only whenever they want.

Aside from the benefits mentioned above, some scholars believe that SSI can assure interoperability.[55] Adoption of global SSI protocols and standards, for example, allows individual and public entities to keep proofs of information inside the same accessible decentralized networks by employing decentralized technology and private and mobile management units. In addition to this, SSI can assist users in having full ownership of their electronic money, just like cash. Individuals generate their own IDs under the SSI paradigm, supporting the possibility of pseudonymity. Individuals are permitted to develop as many IDs as they require in order to connect with various services in a way that prevents these entities from associating the individual with their various other identities. Furthermore, SSI protocols support selective information sharing and zero-knowledge proofs.[56]

55 Sovrin. 2020. Interoperability Series: Sovrin Stewards Achieve Breakthrough in Wallet Portability — Sovrin. [online] [Accessed 5 August 2021].

56 López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications.[online] Publications.iadb.org. [Accessed 13 July 2021].

Benefits of SSI

Currently, many tangible papers, such as passports, degrees, CVs, property titles, and others, are required to verify our identity or what we have done to another organization. SSI enables the storage and administration of multiple identifiers within a single digital wallet. This is considerably more portable than the management units provided in the previous sections' identity models. At the same time, it is easily recoverable, as it is a common problem that people tend to lose physical documents and chip cards. Most of us have lost a physical ID at some point in their life, and the hassles and expenses associated with obtaining new ones are well known. If we lost access to our SSI digital wallet, we could retrieve all of our data using secure and encrypted cloud backups.

In terms of scalability, decentralized ledgers can be joined from anywhere in the world; all you need to access a digital wallet is an internet connection and a smartphone. However, this would necessitate the use of international standards and protocols in order for the solutions to be reproduced across countries. Certainly, researchers and practitioners that advocate for SSI place a great emphasis on the ability of the majority of digital wallets to satisfy the highest security requirements.[57]

SSI protocols use several levels of identification, authentication, and authorization to ensure that only the identity's owner has access to it. Usability is accompanied by portability, recovery, security, interoperability, and anonymity. In order for SSI to serve a purpose, both public and private services must be provided through the SSI framework.

57 López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications. [online] Publications.iadb.org. [Accessed 13 July 2021].

Benefits of SSI

Many sectors are required to gather and handle specific client data in order to authenticate the identity of individuals they serve, e.g., "know your customer" or KYC rules. For other companies, it all boils down to offering a safe and seamless consumer experience. You want to be able to remember and greet your consumers every time they phone, visit, or log in. Onboarding will be mostly automated using the decentralized identity. Applying for and qualifying for a new loan can take seconds rather than hours or days. The consumer just has to give a set of credentials that have previously been validated by a trustworthy institution stored in their digital wallet.[58] Digital wallets make it easier to create, manage, and present verifiable IDs. This enables improved identity proofing across all services, not only those offered by government and financial institutions, as is now the case.

Moreover, given the quantity of personal information available on the dark web, committing fraud is really not hard but is not the sole complicating factor. The complexity and lack of accountability in big payment processing consortiums provide attractive possibilities for dishonest people.[59] With SSI, as individuals are in control of their data, and differing and unassociated pseudonymous identifiers can be used to interact with various digital services, privacy abuse, and data aggregation is much less likely. Furthermore, it is intended to be private. Identity providers are not required to store and reveal user data, and service providers can maintain private databases with pseudonymous identities. Regulations, on the other hand, must constantly improve and change in order to be followed.

58 Goldfarb, S., 2019. 5 Ways Decentralized Identity Will Cut Costs and Grow Revenues — Evernym. [online] Evernym. [Accessed 5 August 2021].

59 Goldfarb, S., 2019. 5 Ways Decentralized Identity Will Cut Costs and Grow Revenues — Evernym. [online] Evernym. [Accessed 5 August 2021].

Benefits of SSI

SSI not only gives individuals the highest level of control over their data, but selective sharing of personal data with service providers follows the idea of data economy and privacy by default.[60] Compliance with laws such as HIPAA, GDPR, and AML-regulation cause excessive expenses for organizations each year. These rules seek to safeguard consumers, businesses, and the economy as a whole from potentially harmful or malevolent business activities, yet they impose significant costs on even the most ethical of businesses. Decentralized identification protocols are designed to meet these criteria. Decentralized identity makes it simple for businesses to specify what information they need to gather and how it will be used, as well as for consumers to securely keep and distribute that information as they see fit.[61] As users gain ownership over their identities, authenticators, data, and credentials, silos dissolve.

Hacks to centralized repositories become considerably more difficult, whereas hacks to decentralized repositories become much more complex. The owner is now in command and may quickly revoke credentials and identifiers if they suspect theft. Identity issuers can still cancel credentials, but the decentralized ledger or blockchain network provides traceability of issuance and revocation.[62] SSI benefits are numerous, and this list is not exhaustive, but how does this work in practice?

60 Der, U., Jähnichen, S. and Sürmeli, J., n.d. Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution. [online] Arxiv.org. [Accessed 5 August 2021].

61 Goldfarb, S., 2019. 5 Ways Decentralized Identity Will Cut Costs and Grow Revenues — Evernym. [online] Evernym. [Accessed 5 August 2021].

62 López, M., 2020. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications. [online] Publications.iadb.org. [Accessed 13 July 2021].

Chapter 3

SSI Technical Overview

Key Entities and Technical Components of SSI

In the previous chapters, the reasons for the emergence of SSI, as well as the benefits that it gives to the world, were outlined. For further understanding of the technology and effective work with the concept, decomposition is needed. We will attempt to show the role of each participant in the ecosystem, as well as decompose the ecosystem into key technical components.

The core actors in the SSI ecosystem are Issuers, Holders, and Verifiers.

The Issuer is responsible for verifiable claims assertion and their provision to the Holder. Actually, any entity that provides verifiable data may become an Issuer, from governments and government bodies to universities, employers, tourist agencies, and other much smaller organizations.

The Verifier is the party that checks verifiable claims provided by their Holder. Depending on the data received and its validity, he makes a decision on a further procession. If we draw an analogy with the physical world, any party that now requests documents (e.g., for the provision of services) can become a Verifier when joining the SSI ecosystem.

The Holder is the party that directly owns the verifiable claims. SSI is designed in such a way that, in essence, this ownership is not much different from the possession of physical documents, especially if we talk about privacy, the right to decide when and to whom to disclose that verifiable claims.

Key Entities and Technical Components of SSI

Generally, the SSI ecosystem is built in such a way that it's the Holder who sits at the center of the verifiable data flow. These complex relations are usually designated by the term "Trust triangle."

1. **The Verifier** trusts the Issuer to issue the credential he receives.

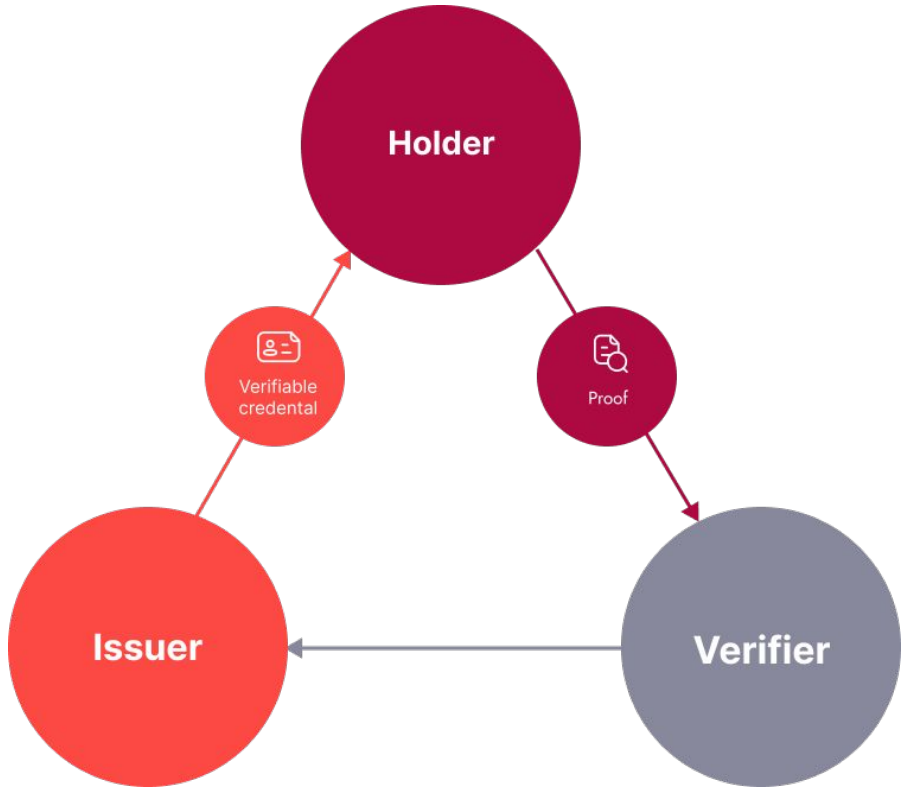
2. **Holders and Verifiers** trust Issuers to issue true credentials and to revoke them quickly when necessary.

3. **The Holder** trusts the storage where his credentials are placed.

4. All the parties trust the **verifiable data registry** to be the source of truth for the ecosystem.[63]

The technical trust is provided by the architecture of SSI, in particular its key elements listed below.

63 Sporny, M., Longley, D. and Chadwick, D., 2019. Verifiable Credentials Data Model 1.0. [online] W3.org. [Accessed 5 August 2021].



Key Entities and Technical Components of SSI

Decentralized identifiers
eliminate the need to rely on centralized authorities to identify and resolve entities in the SSI ecosystem.

Verifiable credentials
is a format of digital documents proposed by W3C and designed to deliver and store verifiable claims in an encrypted privacy-preserving way.

Verifiable data registry
is a system acting as a trust anchor mediating the creation and verification of identifiers, cryptographic keys, and other relevant public-visible data necessary for the system to work in a trustworthy way.
In the next paragraphs, we will take a closer look at how they work and ensure trust in the SSI ecosystem.

Decentralized Identifiers

People deal with thousands of identifiers both in their everyday life and on the Internet. But all of them, as a rule, are united by the fact that they are issued and controlled by centralized registration authorities, which makes them unsuitable for the needs of SSI, based on the principle of decentralization.

To meet the requirements of trust, ecosystems identifiers must be globally unique, permanent, and cryptographically verifiable.[64] Actually, the need for persistent identifiers is already covered with Uniform Resource Names (URNs standard, while Universally Unique Identifiers (UUIDs) are globally unique identifiers that do not require a centralized registration authority. However, as a rule, UUIDs can't be resolved globally, while UNRs require centralized registration for that purpose. But most importantly, neither URNs nor UUIDs ensure cryptographical verification of their ownership.[65]

That is the reason why Decentralized Identity Foundation (DIF) proposed a new type of identifier "that enables verifiable, decentralized digital identity." In July 2021 Candidate Recommendation Draft of the specification was published, and now DIF is expecting developers and DID Method specification authors to provide experimental implementations to test the implementability of the standard. DIDs are the core layer of decentralized identity infrastructure.

In general, a **DID is a string of characters** consisting of three blocks.

The first one — **scheme** — is just a string "did" indicating to the systems that in front of them it is a decentralized identifier. This is important because DIDs are primarily designed to be machine-readable identifiers.

64 W3.org. 2021. Use Cases and Requirements for Decentralized Identifiers. [online]. [Accessed 6 August 2021].

65 Credentials Community Group (W3C), 2020. A Primer for Decentralized Identifiers. [online] W3c-ccg.github.io. [Accessed 6 August 2021].

Decentralized Identifiers

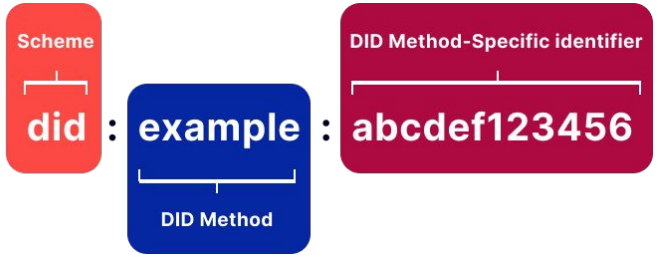
The **DID method** stipulates how and where DID is generated, updated, resolved, and deleted. Methods are often associated with a particular verifiable data registry, but not necessarily. As there are dozens of DID methods already present, it makes sense to highlight the key types and dwell on them.

1. **Blockchain-based DID** methods constitute an absolute majority in the DID Specification Registries, which among other things, summarizes all the DID method specifications currently in development. Examples include methods for dominant blockchains such as did:ethr for Ethereum and did:btcr for Bitcoin. The address of a transaction or a smart contract on the blockchain is involved in DID generation. It does not matter whether the blockchain is public, private, permissionless, or permissioned.

2. **Peer DID method**, as it follows from its name, is designed for pairwise or n-wise encrypted connections. Although p2p connections are also possible using blockchain-based DIDs, that kind of DIDs makes them private and unlinkable. In addition, peer DIDs have no transaction costs and can scale greatly as they do not depend on any centralized or decentralized system's capacity.[66]

3. **DID Web method** is designed to incentivize mass adoption as it allows bootstrap trust using a web domain's existing reputation. The method-specific identifier here is a fully qualified domain name that is secured by a TLS/SSL certificate. E.g., an organization's website www.example.com produces did:web:example.com identifier. DID resolution is quite simple as it only requires a DID Document to be placed on one of the routes belonging to the website. DID Document revocation, in turn, requires just disabling the route in any way.[67]

66 Deventer et al, 2021. Peer DID Method Specification. [online] Identity.foundation. [Accessed 6 August 2021].



Decentralized Identifiers

The last block of DID — **method-specific identifier** — provides the global uniqueness of a DID. Each DID method independently determines how it is generated, but that string must be unique in the context of that DID method.

One of the properties of DID remained undisclosed — cryptographic verifiability. It is provided by the JSON-LD structure called DID Document containing public keys, authentication protocols, and service endpoints. The process of obtaining DID Documents by DIDs is called **DID resolution**. Parties can use DID Documents to authenticate themselves and prove their association with DIDs. Relations in DID infrastructure reflect a key-value structure, where DIDs are the keys and DID Documents are the values.[68]

There is a certain freedom in DID resolution implementations. Some DID documents may be stored directly on the blockchain or in other storage. Others may be constructed dynamically by DID resolvers based on attributes of a blockchain record.[69]

DIF proposes a secure, private communication methodology built atop the DID infrastructure called DIDComm Messaging. As current communication mechanisms strongly rely on centralized intermediaries like identity providers, certificate authorities, browser, or app vendors, there is a need for another solution for SSI. DIF proposes an asynchronous message-based approach that is not coupled to the sequential request-response paradigm and therefore is closer to email protocols. The desired mass adoption of the technology (not only for SSI purposes) also imposed requirements for the protocol to be transport-agnostic, which means it's designed to work regardless of the environment using HTTPS 1.x and 2.0, WebSockets, BlueTooth, chat, push notifications, AMQP, SMTP, NFC, sneakernet, snail mail, etc.[70]

67 Steele, Gribneau, C., Prorock, M., Terbu, O., Xu, M. and Zagidulin, D., 2021. did:web Method Specification. [online] W3c-ccg.github.io. [Accessed 6 August 2021].

68 Hamilton-Duffy, K., Grant, R. and Gropper, A., 2021. Use Cases and Requirements for Decentralized Identifiers. [online] W3.org. [Accessed 6 August 2021].

69 Sabadello, M. and Zagidulin, D., 2021. Decentralized Identifier Resolution (DID Resolution) v0.2. [online] W3c-ccg.github.io. [Accessed 6 August 2021].

70 Identity.foundation. 2021. DIDComm Messaging Specification. [online]. [Accessed 6 August 2021].

Verifiable Credentials

W3C defines VCs as "a tamper-evident credential that has authorship that can be cryptographically verified." The layer of VC exchange is where most of the SSI value is unlocked.[71]

In our real world, the word "credential" refers to a document that contains some assertions made about its subject by an authorized third party. Examples of credentials include IDs, diplomas, certificates, tickets, proxies, and any other documents that confirm qualification, competence, authority, the right, or any other claims about the subject. VCs may contain the same data that physical credentials represent. But the addition of digital technologies makes them much more trustworthy.[72]

VC is essentially a standard way for digitally expressing credentials in a cryptographically safe, privacy-preserving, and machine-verifiable way. It represents a significant shift in developing digital system design options, moving towards systems that provide more portable and user-centric digital identity, which is essential for 'self-sovereign' or 'decentralized' systems.'

71 Credentials Community Group (W3C), 2020. A Primer for Decentralized Identifiers. [online] W3c-ccg.github.io. [Accessed 6 August 2021].

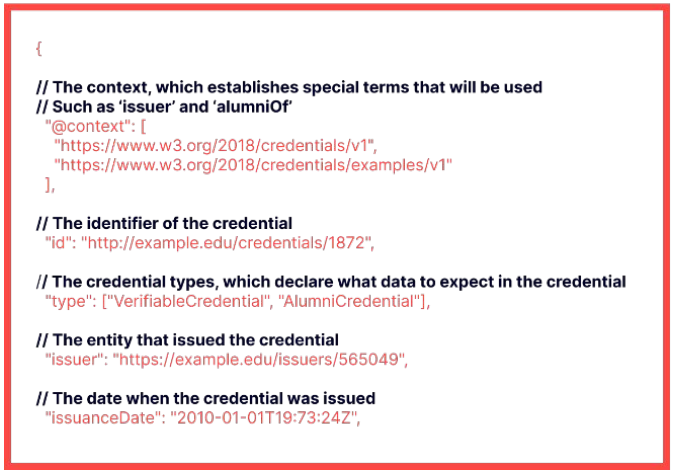
72 Sporny, M., Longley, D. and Chadwick, D., 2019. Verifiable Credentials Data Model 1.0. [online] W3.org. [Accessed 5 August 2021].

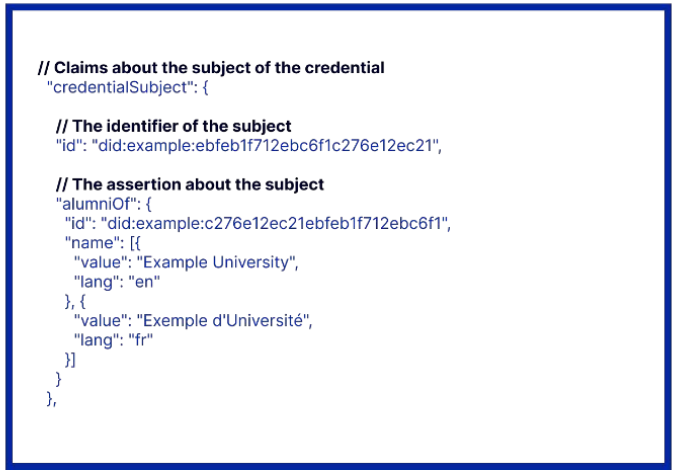
Verifiable Credentials

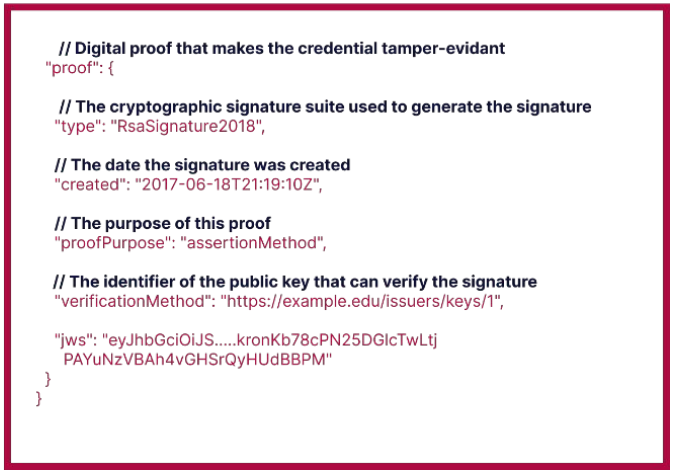
Technically, a VC is just a set of properties packed into the JSON-LD format. Essentially like a paper document, a VC contains the following blocks:

73 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 140

A simple example of a verifiable credential (W3C)







Metadata. JSON-LD context ensures that software will interpret the keys and types in the VC JSON in a globally consistent way. Credential type property allows Verifiers' systems to detect whether a particular VC can be accepted and handled. Metadata also includes VC issuance date and identifiers of VC itself and its Issuer.

Verifiable claims. The content part of a VC containing the Issuer's assertions about the credential subject. Issuer is free to choose the properties of this part, but the JSON-LD schema should be posted to some public place. Such schemas must be stable and unlikely to change significantly for the systems to operate correctly, so storing them in an immutable distributed environment (like blockchain or IPFS).

Proof. That part makes VCs verifiable and tamper-evident, relying on cryptographic techniques. Proof confirms that the VC was issued by a certain Issuer and has not been tampered with.[73] Technically a VC may contain multiple proofs.

But why do VCs significantly change the state of trust in digital relations?

First, **the level of security** that digital cryptography provides seems significantly greater than paper documents do. Actually, modern asymmetric encryption algorithms leave no chance for many attack methods, as private keys are not revealed to other parties directly. Compromising such a key by brute-force selection is also not possible due to the huge number of variations. In practice, attacks are more likely to boil down to gaining illegal access to private keys through vulnerabilities in other systems or their improper configuration. Also, detecting mismatched keys is a trivial procedure, which may be performed automatically, while forgery of paper documents is not always noticeable at first sight.

Second, they are **privacy-preserving by design**. The SSI ecosystem as a whole is built to minimize the disclosure of personally identifiable information. For that purpose, the following mechanisms are intended:

1. **Selective disclosure.** That means only the part of claims present in VC can be disclosed. You can reveal only your name and country of birth from the ID credential issued by the government without providing any other data to the Verifier.

2. **Derived predicates.** These are boolean assertions based on the attributes from VC. They are answers on such conditions as "greater than," "equal to," and etc. In our example with ID, a user can provide proof that he is over 18 years old without disclosing his date of birth.

Third, VCs are **portable**. Only the Holder decides where to store credentials and when to disclose them. Typically, they are stored in a digital VC wallet — a mobile application that, in addition, provides functionality to obtain and disclose them. Anyway, the Holder has full possession of credentials, like if he stores physical documents in his pocket.

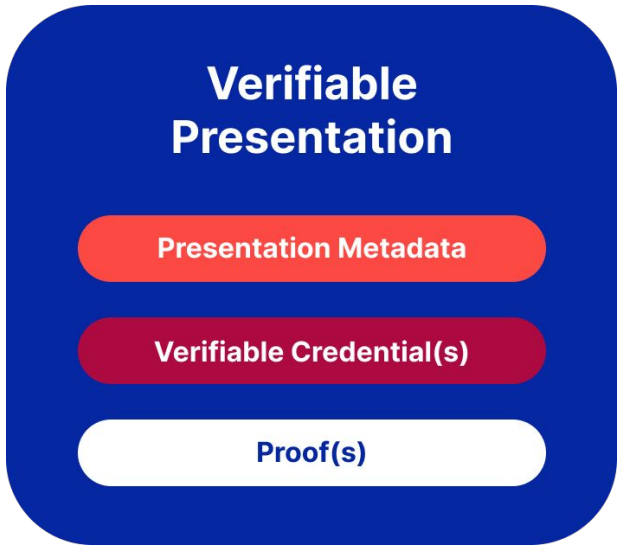
Fourth, unlike physical credentials, in which authenticity is confirmed by some kind of tags present directly on the document, VCs **can be digitally verified in seconds or even milliseconds.**[74] In the case of physical documents, Verifiers must either initially trust what they see when just looking at the document or use complex technical devices to check the authenticity. The latter is quite a time-consuming procedure.

To make the flow for all the parties involved complete, additional standards and data structures are under development.

Verifiable presentations as data structures to which multiple VCs assembled are designed to deliver claims to Verifiers. W3C defines it as a "tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification." The structure is close to VC, but there is a set of VCs or derived data from various Issuers in the content part.

Other protocols, currently being developed by DIF, complement the picture of how the "Trust triangle" will function as a whole. **Credential Manifest** defines which data and proofs about the subject are required to issue verifiable credentials. **Presentation Exchange**, in turn, allows Verifiers to describe proof requirements, and for VC Holders, it enables them to describe submissions of proof that align with those requirements.

74 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 23



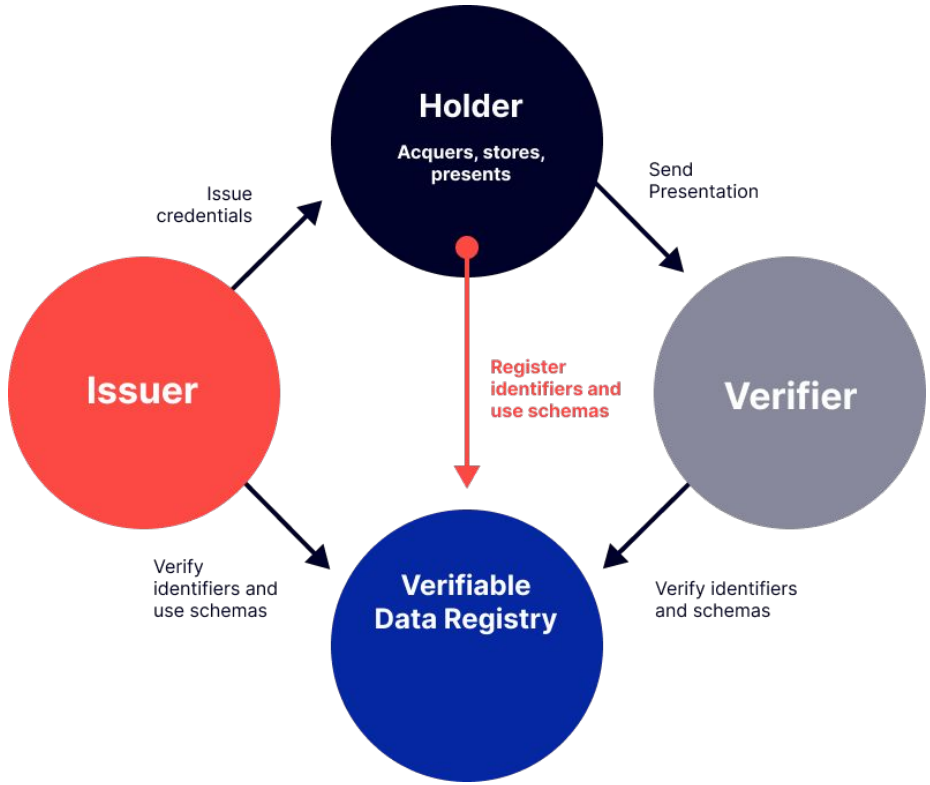
Verifiable Data Registry

Verifiable data registry (VDR) is the element of SSI infrastructure that combines components described above into a single trustworthy environment. Typically VDR is a blockchain. However, there are no strong requirements, and VDR may be implemented using a distributed file system like IPFS or even centralized storage.

VDR is expected to be used as a storage for:[75]

1. **DIDs**, regardless of their subjects, if they are intended for use with an unknowable number of parties.
2. **Credentials schemas** as they should be permanently available to enable systems to recognize their properties.
3. **Public keys**.
4. **Credentials revocation** lists.
5. Other **predominantly public** data that is necessary for the ecosystem to work properly.

75 W3.org. 2021. Verifiable Credentials Data Model 1.0. [online]. [Accessed 05 August 2021].



Chapter 4

SSI Governance

Casper

The Diversity of Governance Methods

Every complex system needs governance. Like a state, SSI ecosystems need a set of rules regulating how that system should work and how its participants should behave. Good governance is at the heart of SSI adoption. The beauty of information systems is that the governing rules may vary essentially and are not limited only by legal regulations. In many ways, governance in SSI is performed technically, being incorporated directly into solutions architecture.

Governance for SSI is not a single, well-established process but a set of ideas and concepts that are likely to be applied in combination, and each of them will cover its own domain. We envision this to be a combination of centralized and decentralized methods, although the latter seems to be more appropriate for decentralized trust ecosystems.

75 W3.org. 2021. Verifiable Credentials Data Model 1.0. [online]. [Accessed 05 August 2021].

Trust Frameworks

Trust framework may be defined as "a common set of best practice standards-based rules that ensure minimum requirements are met for security, privacy, identification management, and interoperability through accreditation and governance."[76] They are the set of business, legal, and technical rules that allow digital trust ecosystems of any scale to exist.[77]

Such frameworks can exist on different levels:

1. **Domain-specific** trust frameworks.
2. **National trust** frameworks.
3. **International trust** frameworks.

The governance trust triangle added to the basic Trust Triangle concept described in Chapter 3 clearly reflects the essence of such a governance method.[78]

76 Learn.mattr.global. 2021. Trust Frameworks. [online] [Accessed 6 August 2021].

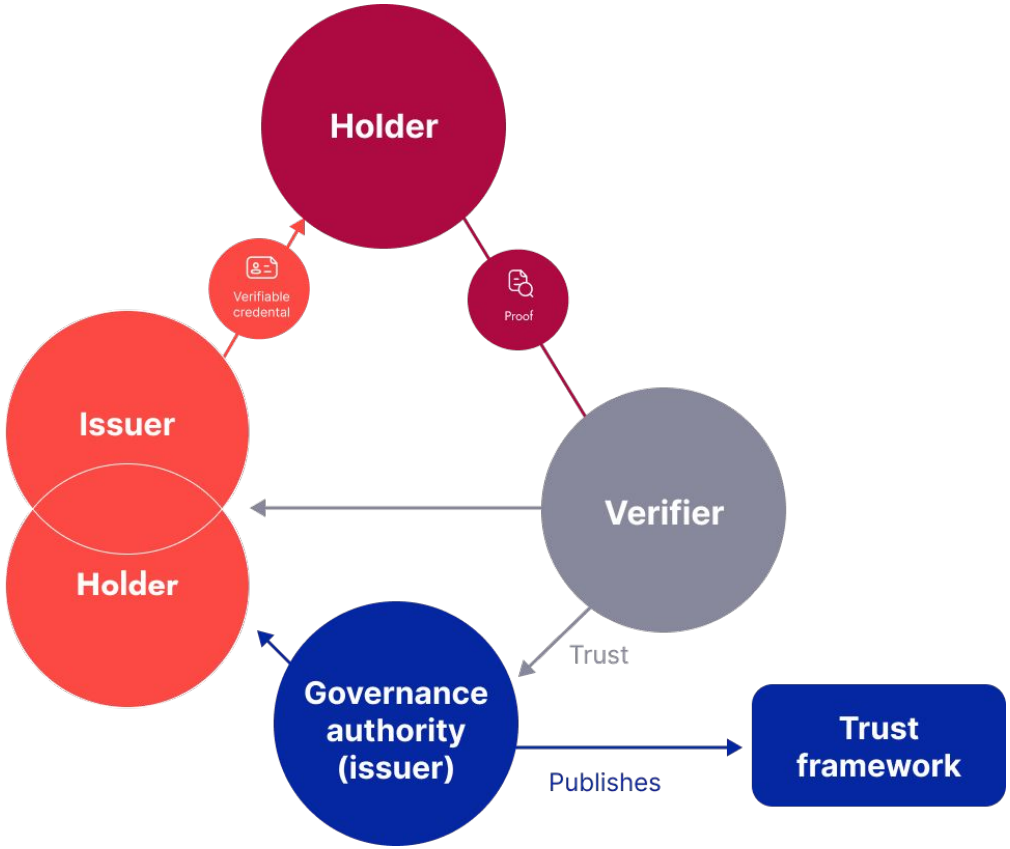
77 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 36

78 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 251

Centralized Governance

79 Trustoverip.org. 2020. Introducing the Trust over IP Foundation V1. [online] [Accessed 6 August 2021]. p. 19-22

Trust frameworks can cover all the aspects of the SSI ecosystem from the very bottom to the top layers. Speaking about the VDR, they specify the policies under which it's implemented and operated in such a manner that it can be trusted by the higher layers. In addition, the frameworks may set requirements for mobile wallets and agents, as well as for the exchange protocols of different levels. Finally, the requirements for the ecosystem participants — Issuers and Verifiers — may be specified.[79]



Certificate Authorities

The PKI + CA model is aimed to solve the problem of binding a public key to a certain identity, which means ensuring that the entity actually owns the public key that it declares. Hence a trusted third party called a certificate authority (CA) issues a digital certificate containing:

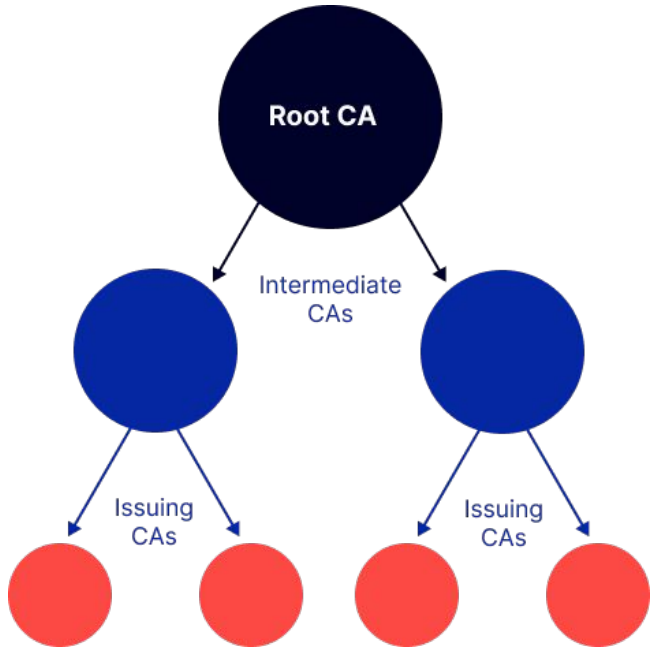
1. **The information** about the subject.
2. **The public key**.
3. **The expiration date** of the certificate.
4. **The signature** of the CA.[80]

Before issuing a certificate, the CA validates the subject's identity. In this regard, when it comes to relations with this subject, the counterparty must trust the CA, and this is the weak point of such a model. In addition, the services of CA are not costly and are likely to be needed again over time, as certificates have a limited validity period.

Another potential issue is this concept is not likely suitable for the system which aims to be widespread globally. Mutual recognition and acceptance of e-signatures have been a real problem even for highly integrated international entities such as the EU.

The above reasons determine that certification, being applicable to SSI, is likely to have a limited scope rather than being the core PKI model. For instance, Issuers of state credentials (IDs, birth certificates), as well as Issuers subject to state licensing and authorization (medical centers, insurers, etc.), can be certified by the state.

80 2021. PKI: The Role of Certificate Authorities in PKI Certificate. [online] Savvy Security. [Accessed 6 August 2021].



Assurance Communities

An SSI Assurance Community (SSI-AC) is a formal or informal, temporary or permanent organization made up of several components (individuals, businesses, and governments) whose mission is to, at the very least, administer the SSI-AC while also supplying one or more of the products/services it regulates. The SSI-ACs are concerned with assurance amongst community members, as the name implies.

A group of individuals does not aim to establish norms or standards that should be followed globally. Because the nature of a community is that its members have some common ground, this goal may be accomplished by exploring that existing common ground.[81]

Here are some functions that an assurance community may contemplate of performing the following duties:

1. **Govern a set of credential** types.
2. **Maintain credential catalog** in which its members can advertise the credential types they issue and specify the assurances and other data that parties may need in order to decide whether or not to take that member upon that offering.
3. **Provide service** for searching an Issuer of credentials of a certain type
4. **Govern and document** accreditation schemes.[82]

81 Joosten, R., den Breeijen, S. and Reed, D., 2021. Decentralized SSI Governance, the missing link in automating business decisions. 10.13140/RG.2.2.35491.68640 [online]. [Accessed 6 August 2021]. p. 11-13

82 NGI — eSSIF-Lab. 2021. SSI Assurance Community (SSI-AC). [online]. [Accessed 6 August 2021].

The Power of Smart Contracts and DAOs

In simple words, a smart contract is a computer program that is intended to execute and control legally relevant events and actions.[83] As to non-technical vision, then often parallels are drawn with the law, considering a smart contract as an agreement between the parties but in the form of code.

Although the theoretical concept was proposed much earlier, only the emergence of blockchain allowed to bring the technology to life, blockchain has become a kind of independent and transparent environment for the execution of smart contracts, which are difficult to imagine in centralized systems.[84] The first smart contract platform — Ethereum network — went into life in 2015.

Since then, our digital world has changed rapidly. The DeFI sector has become the most notable innovation, which by combining peer-to-peer (P2P) networks, algorithmic automation, and community incentive structures enhance existing and create wholly new financial products free from costs predetermined by current middleman-based systems. However, it's obvious that the technology application goes far beyond the world of finance.

Smart contracts, in turn, led to the emergence of a new idea of collective interaction and management — decentralized autonomous organizations (DAOs). And although the first implementation — The DAO — failed and became defunct after an attack which became possible because of engineering flaws, the core concept has demonstrated its advantages as a new technical way of coordination that potentially solves some of the management issues existing for decades.

83 Igi-global.com. 2021. What is Smart Contract | IGI Global. [online].[Accessed 6 August 2021].

84 Gemini.com. 2021. DeFi Governance in Action. [online].[Accessed 6 August 2021].

Decentralized Governance

Technically, a DAO is nothing more than a set of smart contracts. The bottom line is that analog trust typical for traditional organizations is largely replaced by trust in DAO code and its execution environment that are transparent and verifiable by any stranger.

In the context of SSI, one can also find a use for DAOs. In particular, we can fantasize about DAO-based Issuers and Verifiers. This, along with the power of the semantic web, allows to build up continuous trustless processes with understandable and automatically applied governance abolishing the traditional centralized approaches in many aspects.

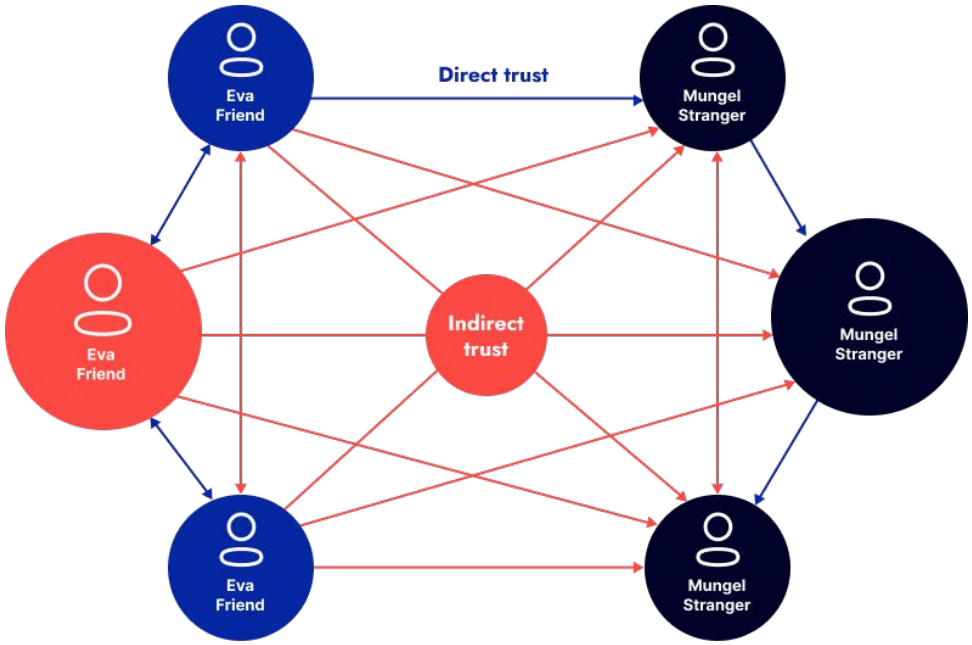
The Web of Trust Concept

As previously noted, the type of PKI currently dominating the Internet strongly relies on a hierarchical system of CAs — trusted third parties that have been designated to manage identifiers. The **Web of Trust** (The WoT) concept was proposed first about 30 years ago by PGP creator Phil Zimmermann to rethink that approach. The idea is a peer-to-peer attestation of public keys so that the task of key-to-identity binding is shifted from CAs to the community, eliminating the centralized dependency:[85]

"As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys."[86]

85 Learn.mattr.global. 2021. Web of Trust 101 Introduction. [online]. [Accessed 6 August 2021].

86 Zimmermann., P., 2021. Protecting Public Keys. [online] HFC Portal. [Accessed 6 August 2021].



That original vision of the WoT was never implemented and has not been universally used by now. Currently, with the decentralized web3 birth, the problem of independent PKI is again relevant, but blockchain solves it in another way, acting as the root of trust and eliminating the need to rely on anybody.[87]

So at the current stage, the WoT is interesting not as a narrow solution to the PKI problem but as an abstract concept of social interaction in the network to cover various tasks, including governance. Experiments on digital identity based on the social graph concept are being carried out (see the **BrightID** project as an example).[88] Besides, the PKI domain still has a place for WoT concept heritage: for instance, if we consider the ideas of social recovery of lost identity.

87 Habr.com. 2019. DPKI: Addressing the Disadvantages of Centralized PKI by Means of Blockchain. [online]. [Accessed 6 August 2021].

88 Brightid.org. 2020. Whitepaper Universal Proof of Uniqueness. [online]. [Accessed 6 August 2021].

Sovrin Ecosystem

Sovrin is a global utility for self-sovereign identity. Technically, Sovrin comes from Hyperledger Indy stack, using the Sovrin Governance framework as the legal foundation of the **Sovrin Network**.[89] The purpose of the Sovrin Foundation is "to administer decentralized governance for Sovrin Infrastructure on behalf of all Identity Owners."[90]

It is obvious that governance cannot encompass the entire planet because each region/jurisdiction has unique features that are frequently contradictory with others. With its **Sovrin Governance Framework (SGF)**, Sovrin attempts to provide a single basic governance layer while allowing particular sectors to define their own regulations. When the section is under SGF, the participants are guaranteed that the basic principles are followed, as the network is obliged to adhere to them.[91]

One of the most important elements of Sovrin's governance is that it is constructed on a permissioned blockchain. Because it is still a public ledger, anybody may join. However, the ledger is managed by Stewards, trusted organizations within the ecosystem that have committed to follow the criteria of the SGF and are in charge of running the nodes that keep the Sovrin distributed ledger running.

SGF's governance covers not only the business and legal but also the technical aspects of the ecosystem. That means it defines which code should be run by the nodes and how that code should be architected. In addition, all the changes are subject to review by the Technical Governance Board and the Stewards.[92]

89 GitHub. 2019. Sovrin Identity for All. [online]. [Accessed 6 August 2021].

90 Gleif.org. 2018. Sovrin Governance Framework V2 Master Document. [online]. [Accessed 6 August 2021].

91 Windley, P., 2018. Decentralized Governance in Sovrin. [online] Windley.com. [Accessed 6 August 2021].

92 Windley, P., 2018. Decentralized Governance in Sovrin. [online] Windley.com. [Accessed 6 August 2021].

Token-curated Registries. Token-curated Attesters

Token-Curated Registries (TCRs) were introduced in 2017 as the concept of decentralized lists independent from any single list owner, which by means of economic incentives and the wisdom of the crowd aimed to provide truthful information that cannot directly be verified. List curators collectively decide via a voting system whether or not a list should be populated with a certain item. To prevent malicious behavior, when curators vote on a list application, they stake tokens for or against a list application so that the winning side gets a part of the losing side's stake.[93] [94]

After examining the TCRs solution, **Botlabs** — the organization responsible for **KILT blockchain** development — evaluated some of the drawbacks of the concept and proposed their solution that originates from the analog world.

When speaking about solving complex subjective problems (for that purpose TCRs were proposed), KILT's team found the original concept unsuitable and turned to our ordinary world, where usually, qualified persons — experts — are involved. Good choices and decisions have a positive impact and offer opportunities to reward experts, but bad decisions harm experts' reputations and may result in their losing their jobs. This is a type of economic incentive that attempts to persuade specialists to do tasks correctly.

In many cases, VC Issuers are seen as trustworthy by default, as they are authoritative in society for one reason or another (large enterprises, governments). However, often the trust should be built from scratch. For those cases, the team tried to apply the ideas described above to the VC issuance process and introduced the concept of **Token-Curated Attesters (TCAs)**, responsible for claims legitimation.

93 Tepot, C., 2019. What are Token Curated Registries and decentralized lists? | Hacker Noon. [online] Hackernoon.com. [Accessed 9 August 2021].

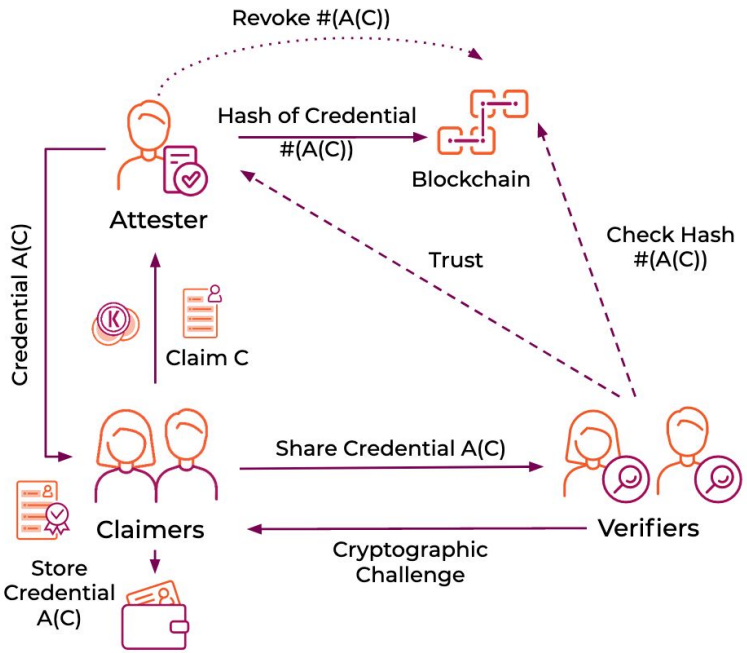
94 Medium. 2019. Rethinking TCRs: KILT's concept of the Token-Curated Attester (TCA). [online]. [Accessed 9 August 2021]

The attestation flow is the following:

1. **The Claimer sends** his attributes to the TCA.
2. **TCA replies** with the price of attestation.
3. The Claimer sends signed **claims with funds to the TCA**.
4. **The TCA involves Experts** who take all the necessary to check if the Claim is legitimated to get certified.
5. **If they found that's true**, a corresponding VC is issued to the Claimer.[95]

The concept is an interesting example of trying to build so-called **"bottom-up" trust** in the SSI ecosystem, keeping the idea of cryptoeconomic incentives for fair decisions inherent in TCRs.

95 Medium. 2019. Rethinking TCRs: KILT's concept of the Token-Curated Attester (TCA). [online] [Accessed 9 August 2021]



Chapter 5

SSI for Casper Network

Benefits of SSI and Blockchain Synergy

Since Satoshi Nakamoto first presented Bitcoin to the world in 2009, the reach of blockchain technology has expanded well beyond currency. The first attempts at using blockchain to issues of digital identity were made in 2015 at the Internet Identity Workshop.[96] This marked the beginning of an active movement towards the decentralized identity: "SSI was born because blockchain technology introduced an exciting new option for implementing a decentralized public key infrastructure."[97]

In addition to the charm of decentralized identity itself, there are some points explaining the mutual benefits of SSI and any blockchain network:

1. **SSI permits value** to be transferred out of the chain. There are a number of case-specific blockchain networks. However, unless there is a universal means of transferring the final result to other places: networks, apps, and storage, the end result stays locked in within the network. The use of VCs as a global standard appears to be a viable option.

2. While **VCs are transferring utility** across multiple blockchain networks, the utility of the whole SSI ecosystem is growing. SSI is of little interest to anyone when it covers only one information system, organization, or governing body.

3. **SSI opens a huge number of use cases**. Currently, blockchain is predominantly the area of anonymity, which initially limits the scope of its application given the potential of the technology. SSI protects anonymity while also adding a degree of trust to digital relationships that encourage collaboration and progress.

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

97 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 89

Blockchain + SSI Architecture Components

The potential blockchain uses for SSI are numerous. We will focus on the most important aspects, knowing that the blockchain's potential is far from exhausted.

Having decomposed the SSI concept into its primary building blocks in previous chapters, we can now summarize the sample list of blockchain network applications for the SSI ecosystem, supplementing it with a couple of not touched upon in the text but essential components:

1. **Ledger-based DID method** originated decentralized public key infrastructure, replacing the administrative root of trust, typical for centralized systems, with algorithmic one.

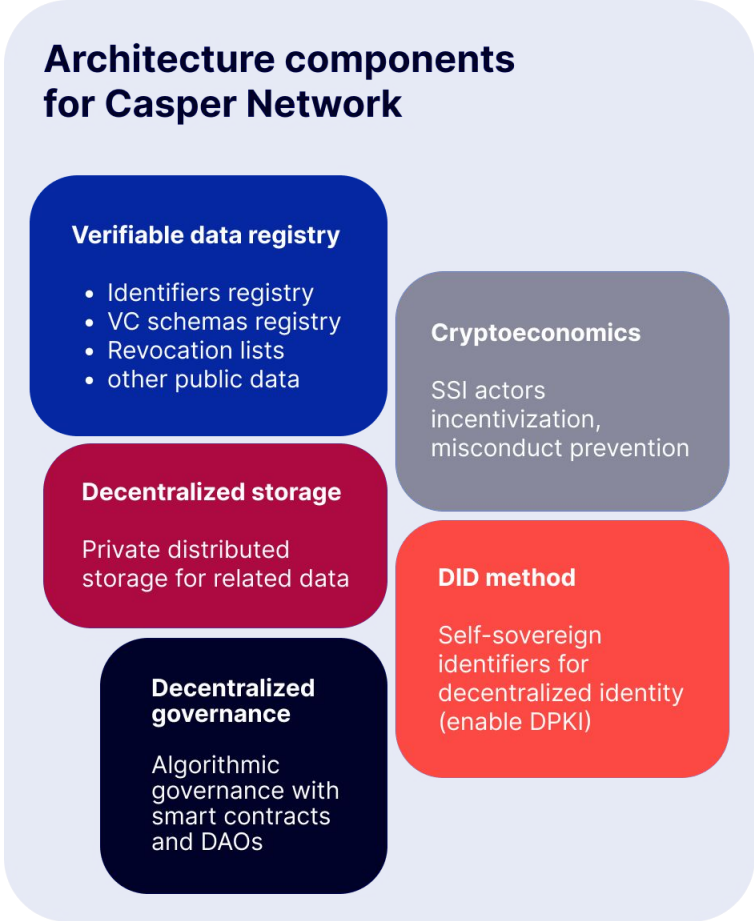
2. **Verifiable data registry**. The role of VDR as the root of trust has already been described in Chapter 3. In this chapter, we will explain why exactly blockchain has become the standard for VDR today.

3. **Decentralized governance.** Smart contracts and DAOs working on-chain can play a significant role in the algorithmic governance of decentralized ecosystems, as discussed in the previous chapter.

4. **Cryptoeconomics** rooted in the blockchain network has a regulatory and stimulating function in the SSI ecosystem.

5. **Decentralized storage** hits the problem of trustworthy data storage in decentralized systems.

In this chapter, we will focus on ledger-specific aspects of some of the building blocks, explaining how they can foster digital trust being implemented on the blockchain network.



Ledger-based DID Method

DIDs, as previously mentioned, are thought to function with any network and may be produced virtually anywhere, including in centralized systems. So, what are the benefits of using blockchain? What are some of the advantages?

First of all, blockchain may act as an algorithmic root of trust for DIDs.[98] For that purpose, once the public/private key pair is generated, the private key is used to digitally sign the transaction in blockchain so that DID is recorded. An identity (no matter a thing, a person, or an organization) needs no centralized registration. From now on, Verifiers should check the ledger to verify the public key. The vast majority of DID methods at the current stage are blockchain-based.[99]

Standardizing bodies do not insist that this DID be used in all connections. Instead, for the purpose of unlinkability and privacy, the subject may have thousands of DIDs each for one encrypted relationship. However, blockchain-based DIDs are the right solution for anywise relationships as they must be resolvable by anybody. Blockchain-based DIDs may be used to reference their subjects without establishing a relationship (for example, the Issuer property of a VC may be represented by DID value, making it easy for people and systems to check their status and attributes).[100]

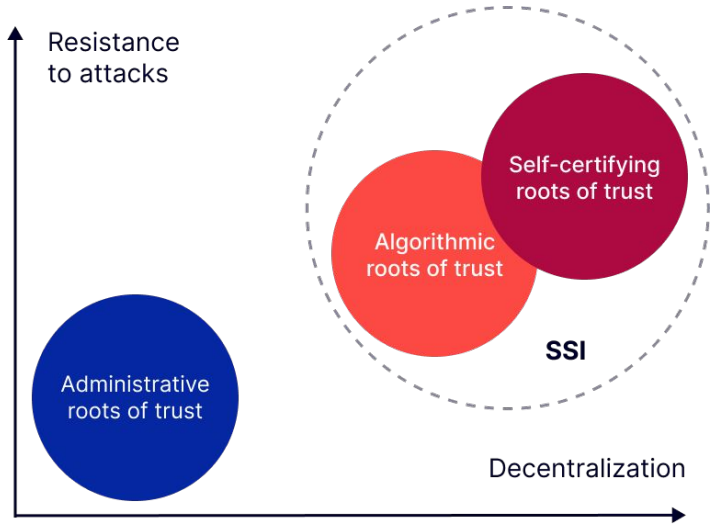
98 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 230

99 Steele, O. and Sporny, M., 2021. DID Specification Registries. [online] W3.org. [Accessed 6 August 2021].

100 Identity.foundation. 2021. Peer DID Method Specification Peer DID Method Specification blockchain-independent decentralized identifiers. [online]. [Accessed 6 August 2021].

Blockchain + SSI Architecture Components

Decentralized key management is one of the most complex features that blockchain-based DIDs provide, as SSI would not exist without it. Within the DPKI the requirement for CAs is replaced with a distributed ledger, distributed database, or distributed file system that support DIDs. Thus, algorithmic root of trust replaces the administrative one.[101]



As a result, blockchain-based DIDs, as well as blockchain as a verifiable data registry, marked a fundamental shift in key management, allowing CAs to be abandoned as a weak part of PKI infrastructure.[102] The right behavior of miners/validators and the consensus process form the foundation of trust.

Governance systems that provide punishments or rewards, as well as the restricted scope of their functions in the ecosystem, prohibit misbehavior.[103]

101 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 225

102 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 224

103 Huang, Y., 2019. Decentralized Public Key Infrastructure (DPKI): What is it and why does it matter? | Hacker Noon. [online] Hackernoon.com. [Accessed 6 August 2021].

Blockchain + SSI Architecture Components

When establishing blockchain-based DID infrastructure, there are a few common concerns to address. Although key management is becoming independent of centralized systems, which is one of the blockchain's primary attractions, the blockchain's weaknesses emerge (compromised consensus algorithm, 51 percent attack). For system architects and developers, complying with GDPR-like legislation (particularly in the context of the right to be forgotten) might be added complication.[104]

How to start implementing DIDs in the Casper network? Start from the **Casper DID method specification** defining at least the DID scheme (the formal syntax of DID) and how CRUD operations on DIDs and DID Documents are performed on the Casper network. Additionally, other implementation, security, and privacy considerations may be outlined in this document.[105]

104 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 230

105 Sporny, M., Longley, D., Sabadello, M., Reed, D., Allen, C. and Steele, O., 2021. Decentralized Identifiers (DIDs) v1.0. [online] W3.org. [Accessed 5 August 2021].

Verifiable Data Registry

The same question arises: why should we use a blockchain since VDR may be represented by any storage according to the W3C definition? The solution is the key feature that made it a groundbreaking breakthrough just over a decade ago.

First and foremost, we must remember what type of data VDR is required to process. These can include IDs, public keys, VC schemas, presentation definitions, and credential manifests, revocation lists, and so on, depending on the system's design.

They are all linked by the notion that it should be publicly accessible data. Second, because this data is important to the system's operation, it should not be entrusted to any centralized entity and should be secured from unauthorized modifications and deletion based on the trusted nature of SSI. For example, keeping the Issuer's public key in a public location makes logical since it may be used to validate his digital signature when a VC is given to a Verifier. At the same time, we must be certain of its identity and invariability, as it is the key that verifies the document's legitimacy.

To satisfy these needs, blockchain is the best option. It is, first and foremost, a decentralized network. Decentralization creates a trustless environment in which no network member must trust another. Simply said, because each node has a copy of the ledger, if a member's copy is damaged or hacked, a certain number of other nodes will reject it.[106] While no one has direct authority over the ledger, each peer may trust it. Furthermore, the ledger's transaction history is immutable. That implies that anyone may rely on it and, if required, examine the full history of data transmission.

106 Amazon Web Services, Inc. n.d. What is Decentralization? [online]. [Accessed 6 August 2021].

Decentralized Private Storage

Not all information should be stored on the blockchain, even considering its advantages over centralized systems for the following reasons:

1. **No encryption** algorithms can be considered secure forever, while the data placed in the ledger will remain there for a long time.

2. **Even if the data** is secured at the moment, the knowledge about its movement in the registry constitutes a threat to privacy.

3. **Transaction history** persistence may conflict with regulatory rules when it comes to storing personal data.

Thus, any private data should not be stored inside the ledger. This is especially true for VCs, although there have been attempts to store them directly on the blockchain.[107] This is partly owing to financial reasons, as VC exchange operations may necessitate several transactions being recorded in the ledger.

What can we do if we still require a secure remote storage system that is not dependent on a third-party provider? What if consumers don't want to rely on Dropbox, Google Drive, or other opaque systems to keep their sensitive data outside of a mobile wallet? Decentralization will assist here as well, but not in the same way that blockchains would.

107 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 92

Blockchain + SSI Architecture Components

One of the most important elements for a scalable decentralized network is storage. In the perspective of privacy, we may talk about the following important criteria for such a decentralized storage solution:

1. **Data protection**. Since the storage of non-public data is implied, the information must be protected from prying eyes.

2. **The possibility of data revocation**. This feature is extremely important, especially if data sharing is implied. At the same time, this is a non-trivial challenge in a distributed network.

The concept of decentralized cloud storage has been worked out for a couple of years and has resulted in such projects as Filecoin, Siacoin, Storj, Solid, etc.[108] In general, the key idea of such decentralized storage is that data is kept in a non-custodial way utilizing blockchain technology. No party other than the owner of the data can erase or damage it. As the data is stored in a distributed manner, it is potentially physically located on hundreds and thousands of devices on different continents, which makes this storage method even more reliable compared to the redundant data centers of large cloud providers. So, the primary benefits of decentralized storage are their privacy-preserving design and resistance to center-level failures.

As with centralized data repositories, economic incentives may exist for the party responsible for data storage, although it is distributed in this case. For instance, within the Filecoin network, thousands of storage providers (miners) may exist, and all of them are rewarded with fees for file placement on the network, as well as for reading operations when required.[109]

108 Gillam, A., 2021. Five Uses of Blockchain That Aren't Cryptocurrency — Pod Group. [online] Pod Group. [Accessed 6 August 2021].

109 Medium. 2021. What is Filecoin?—A Descriptive Guide. [online] [Accessed 10 August 2021].

Cryptoeconomics Incentives for the Ecosystems

Appropriate incentives for all the parties of the Trust triangle seem to be an essential aspect of technology adoption. If in the case of the Holder, there may be enough of the advantages that SSI technology brings itself, economic measures may be effective to make Issuers and Verifiers reconsider their traditional views of things.

Given the significant role that blockchain plays in the SSI ecosystem, it would be foolish to ignore the mechanisms of crypto-economics embedded in its architecture.

The possibilities of cryptoeconomics enable systems to incentivize participants dynamically in real-time, that is, immediately after the transaction (e.g., VC transfer) is performed. Those instruments are aimed to ensure balance within the economic model where VC providers are on the supply side while Verifiers and Holders generate demand on the market.

Cryptoeconomic mechanisms embedded into smart contract algorithms can help to attract to the market those Issuers and Verifiers are not presumed to be trusted. Staking mechanisms with slashing as negative responsibility when platform rules are broken stimulate correct behavior. At the same time, the proper performance of their role in the ecosystem is rewarded.

To summarize, that's what cryptoeconomics can actually provide for SSI:

1. **Economic incentives** for all the actors of the supply chain in a trustworthy manner.
2. **Barriers and negative responsibility** for rule-breakers while preventing misbehavior.

Chapter 6

Legal Aspects of SSI Implementation

Regulating digital environment

The foundations of digitization of all commercial and non-commercial processes online are laid by regulation. Regulation provides the legal tools required for remote contracts, clarifies the rights and obligations of the various actors involved in digital transactions, and establishes a framework that promotes users' trust in digital markets, even if the consumer does not know the service provider or their location is remote. In the modern world, the Internet is fundamental to commerce and social interactions. Both require robust systems of identity so they can function, but the identity was not built into the Internet's original design. This section will provide a brief overview of the global regulatory trends that cover digital and electronic signatures, digital identity, data protection, and SSI.

Adopting the SSI principles implies, overall, a rise in trust management complexity and a shift away from hierarchical or federated trust assurance frameworks – such as the current eIDAS Regulation for electronic identification means immediately informed for cross-border transactions– and toward network-based socio-reputational trust models or accumulative trust assurance frameworks that use quantifiable met criteria methods to aggregate trust on claims and digital identities.[110]

As SSI relies on the use of public/private keys associated with DIDs for verification, the link between the DID and the actual identity can be easily achieved by using the pair of keys corresponding to a qualified certificate as the pair of keys associated to the DID (instead of keys self-generated in the user agent), thus creating a cryptographic connection between the DID and the certificate. Additionally, the use of the keys of the qualified certificate as the keys associated with the DID implies that anytime something is signed with the private key of the DID (which is the same as the one of the qualified certificate), the signature will have the status of an advanced signature produced with a qualified certificate according to the eIDAS Regulation.[111]

110 Domingo, I., 2020. SSI eIDAS Legal Report How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. [online] Joinup.ec.europa.eu. [Accessed 5 August 2021].

111 Ec.europa.eu. n.d. EIDAS SUPPORTED SELF-SOVEREIGN IDENTITY. [online]. [Accessed 10 August 2021].

Electronic Signatures

Electronic signatures or digital signatures are one of the services that confirm authenticity online, just like we do in real life with paper documents.[112] In international business and trade, electronic signatures are crucial. E-signature technology is used by businesses of all sizes all over the world to complete large transactions on a regular basis. E-commerce would most certainly come to a standstill if national regulatory authorities could not ensure the legality of electronic contracts and online transactions. Many countries have passed legislation governing electronic signatures and digital transactions. This expansion, though, is only getting started. Every year, the number of nations that have enacted some sort of e-signature law increases.[113]

According to the United Nations Convention on the Use of Electronic Communications in International Contracts, e-signatures can fulfill a legal necessity for a signature if they match specific criteria. It also provides criteria for the creation and validity of electronic contracts, as well as standards for the attribution of data messages, acknowledgment of receipt, and defining the time and location of data message dispatch and receipt.[114]

A Model Law from the United Nations (MLES) provides equivalence standards for electronic and handwritten signatures based on a "two-tier" approach, as well as responsibility regulations for parties engaged in the signature process. In theory, technology is neutral, yet it may favor one technology over another. MLES contains provisions favoring the recognition of foreign electronic signatures based on a principle of substantive equivalence that does not take into account the place of origin. It is adopted in at least 30 States. MLEC and MLES are both model laws, or "soft laws," such as the allow states to change their provisions as they see fit.

112 Citrix.com. 2021. E-Signature Laws in Every Country — Citrix. [online]. [Accessed 6 August 2021].

113 Citrix.com. 2021. E-Signature Laws in Every Country — Citrix. [online]. [Accessed 6 August 2021].

114 D. Gregory, J., 2015. The United Nations Electronic Communications Convention. [online] Unctad.org. [Accessed 6 August 2021].

Electronic Signatures

Electronic signatures and associated trust services are regulated in the European Union by the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). In the United States, e-signatures are regulated by Electronic Signatures in Global and National Commerce Act (E-SIGN) of the United States, found in 15 U.S.C. 7001. The legislation allows for the use of electronic signatures in a variety of contexts and explicitly exempts numerous state regulations that would otherwise restrict their use.[115]

Electronic signatures are especially significant in business transactions between companies, especially in a worldwide or regional value chain. While e-commerce transactions involving final consumers are typically one-time purchases of discrete goods or services that can be fulfilled with a simple click of a button, cross-border deals involving firms often entail a long-term business relationship involving the production and delivery of customized goods or services, the terms, and specifications of which must be agreed to in advance. At the very least, a regulatory framework should acknowledge that electronic signatures are a legally acceptable method of recognizing a document's requirement or provisions. Furthermore, the framework should ensure that, like a handwritten signature, when an electronic signature fulfills specific standards, it is fully recognized as legitimate and enforceable.[116]

E-signatures may constitute a component of the digital identity. For individuals and electronic gadgets, digital identity is the digital version of real-world identification. It is based on a collection of qualities and characteristics connected with its carrier. Just like an identification document, only these are electronic data.[117] Certificates may be used to create digital identities, ensuring security and reducing the danger of fraud. The regulation of digital identity is critical in today's society, and the next part will evaluate the present state of play in terms of digital identity laws and policies.

115 Govinfo.gov. 2000. [106th Congress Public Law 229] [From the U.S. Government Printing Office]. [online]. [Accessed 9 August 2021].

116 Worldbank.org. 2020. Digital Trade in MENA Regulatory Readiness Assessment. [online] [Accessed 9 August 2021].

117 Rojo, S., 2018. Brief glossary about digital signature and identity so as not to get lost. [online] vintegris.com. [Accessed 9 August 2021].

Digital Identity Regulation

According to the World Bank Group

"a Digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. A digital identity system refers to the systems and processes that manage the lifecycle of individual digital identities. A person's digital identity may be composed of a variety of attributes, including biographic data and biometric data as well as other attributes that are more broadly related to what the person does or something someone else knows about the individual. These attributes, along with credentials issued by the service provider, can then also be used as authentication factors to answer the question "are you who you claim to be?". The attributes and authentication factors used in a digital identity may vary from one context or country to the next depending on the type of identity system."[118]

Businesses and individuals throughout the world were compelled to transfer their daily operations to online platforms as a result of the COVID-19 epidemic and following government initiatives. According to the World Economic Forum, digital identification might play a crucial role in reducing the pandemic's dangers to health, mobility, travel, and trade. The fact that identity fraud has increased as more activity goes online is one of the most obvious of these threats.[119] In light of these conditions, states are attempting to push through legislative reforms relating to digital identity legislation. Thus, in the EU, The European Commission announced in June 2021 a framework for a European Digital Identity that would be available to all EU citizens, residents, and companies. With the touch of a button on their phone, citizens will be able to confirm their identity and exchange electronic documents from their European Digital Identity wallets.[120]

118 Gsma.com. 2016. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper. [online] [Accessed 9 August 2021]

119 Global-counsel.com. 2021. Will 2021 be the year that digital identity finally takes off? | Global Counsel. [online] [Accessed 9 August 2021].

120 Commission proposes a trusted and secure Digital Identity for all Europeans. 2021. Press corner. [online].[Accessed 9 August 2021].

Digital Identity Regulation

Trust in the online world is critical to an effective shift to a digital society. Citizens and businesses are hesitant to engage in digital transactions in the absence of trust. Electronic identification (eID) and electronic trust services, such as electronic signatures, are critical facilitators for European residents managing their digital identities.[121] Member States will be allowed to provide people and companies digital wallets that will allow them to link their national digital identities with verification of other personal qualities under the new eIDAS Regulation, such as diplomas, bank account, certificates, etc. Public agencies or commercial companies may offer these wallets, as long as they are recognized by a Member State. The new European Digital Identity Wallets will allow all Europeans to access online services without having to utilize private identification mechanisms or provide personal information unnecessarily. They will have complete control over the data they disclose with this service.[122]

The European Union's eIDAS legislation provides remedies to this problem. Legal certainty across national boundaries is provided by eIDAS, as is a predictable regulatory framework for smooth cross-border recognition of eID and trust services. For government, businesses, and consumers, eIDAS improves trust, security, and online ease. If an organization gets its digital identity right, it leads to more efficiency, revenue, and transformational benefits with an enhanced user experience and a differentiating digital journey for customers or citizens.[123] In addition, eIDAS establishes a European internal market for trust services, such as electronic signatures, electronic seals, timestamps, electronic registered delivery, website authentication. eIDAS assures that: trust services will be available beyond national borders. Traditional paper-based processes will have the same legal standing as trust services. People and companies can use their own national eID schemes (eIDs) to identify themselves when using digital services in other EU nations, thanks to eIDAS.[124]

121 Digital-strategy.ec.europa.eu. 2021. Building a Trusted and Secure European Digital Identity — Brochure | Shaping Europe's digital future. [online]. [Accessed 9 August 2021].

122 European Commission — European Commission. 2021. Press release. [online]. [Accessed 9 August 2021].

123 van Es, G., Vanhaecht, J. and Wyatt, M., 2021. The Future of Digital Identity. [online] Deloitte. [Accessed 9 August 2021].

124 Shaping Europe's digital future. 2021. eIDAS Regulation. [online] [Accessed 9 August 2021].

Digital Identity Regulation

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. For this, trusted and secure interactions are essential. The objective would be to ensure appropriate and interoperable identification and authentication frameworks. Current digital identity reforms are often aligned to SSI for their objective to create user-centric data sovereignty.[125] Although SSI has been scoped, architected, and built as technology, it is not merely technology. By definition, it's sociotechnology (involving the application of insights from the social sciences to design policies and programs).[126]

In addition to the eIDAS, the European Union has also been developing a Digital Finance Strategy, which states that "by 2024, the EU should create a strong legislative framework enabling the adoption of interoperable digital identification systems," according to the "Digital Finance Strategy for the EU."[127] Customer/user identification and authentication by financial institutions would become more technologically standardized, interoperable, and secure. The eIDAS Regulation is the basic trust framework for natural and legal person agency on the Internet in the European Union and the European Economic Area.[128]

The European Digital Identity will assist in accomplishing a number of objectives and milestones set forth in the Commission's 2030 Digital Compass. By 2030, for example, all important government services should be available online, all citizens should have access to electronic medical data, and 80% of people should be using an eID solution.[129]

125 Giannopoulou, A. and Wang, F., 2021. Self-sovereign identity. Internet Policy Review, 10(2).

126 Sheldrake, P., 2020. The dystopia of self-sovereign identity (SSI). [online] Generative Identity. [Accessed 9 August 2021].

127 Eur-lex.europa.eu. 2021. EUR-Lex — 52020DC0591 — EN — EUR-Lex. [online]. [Accessed 9 August 2021].

128 Eur-lex.europa.eu. 2021. EUR-Lex — 52020DC0591 — EN — EUR-Lex. [online] [Accessed 9 August 2021].

129 Commission proposes a trusted and secure Digital Identity for all Europeans. 2021. Press corner. [online]. [Accessed 9 August 2021].

Digital Identity Regulation

On June 30, 2021, Congressmen Bill Foster (D-IL), John Katko (R-NY), Jim Langevin (D-RI), and Barry Loudermilk (R-GA) introduced the bipartisan Improving Digital Identity Act of 2021 in the United States. The bill aims to improve the country's outdated digital identification infrastructure. Additionally, the bill would create a grant program under the Department of Homeland Security (DHS), enabling states to update their digital identity verification systems, such as those used to issue driver's licenses or other forms of identification credentials.[130] The challenges of a digital ID system are numerous. The foundations of a unified ID system in the United States would have to meet the country's distinctive federalist system, as well as difficult privacy and security concerns and the role of the private sector.[131]

For 2020, the United Kingdom, just like several other if not most states, has also underlined the growing reliance on internet services. Both companies and governments require identity verification. The Financial Action Task Force (FATF) proposed to its member nations in 2020 that legal professionals and real estate agents be subject to anti-money laundering measures. As a result of the Covid-19 outbreak, the UK's Financial Conduct Authority (paywall) accepted selfies and scanned ID papers as evidence of identification, following FATF rules.[132]

In February 2021, the Department for Digital, Culture, Media & Sport of the UK and Matt Warman MP proposed a set of regulations to stimulate the usage of digital IDs in the future. This is part of a larger strategy to make it faster and simpler for individuals to verify their identities using contemporary technology and to establish a procedure that's as reliable as using passports or bank statements. Once finalized, the framework[133] is anticipated to be enacted into law. It contains particular rules and regulations for businesses that supply or utilize digital identification services.[134]

130 Congressman Bill Foster. 2021. Foster, Katko, Langevin, Loudermilk Introduce Bipartisan Digital Identity Legislation. [online]. [Accessed 9 August 2021].

131 Ahmed, U., Gorfine, D., Lau, I., Sturtevant, M., Stephen, K., Jeong, S., Minhas, S. and DiNapoli, R., 2021. The U.S. Digital Identity Crisis | The Regulatory Review. [online] The Regulatory Review. [Accessed 9 August 2021].

132 Klenk, M., 2021. Council Post: Three Predictions For Digital Identity In 2021. [online] Forbes. [Accessed 9 August 2021].

133 GOV.UK. 2021. Policy paper The UK digital identity and attributes trust framework. [online] [Accessed 9 August 2021].

134 GOV.UK. 2021. Press release Government sets out new plans to help build trust in use of digital identities. [online]. [Accessed 9 August 2021].

Following the Financial Systems Inquiry, Australia established the Trusted Digital Identity Framework (TDIF), which established the rules and accreditation requirements against which suppliers of Digital Identity services are recognized, thereby constructing a federation of agencies and systems working together to ensure an Australian Digital Identity system. The TDIF currently includes a number of system-specific privacy and consumer protections for users, such as limitations on the formation and the use of a single identifier across the system, limitations on data profiling, limitations on the collection and use of Biometric Information, and requiring express consent before enabling User authentication to a service. The privacy of Australians is a big concern. Identity theft and fraud were regarded as the most serious privacy issues by 76% of respondents to the Office of the Australian Information Commissioner's 2020 Australian Community Attitudes to Privacy Survey.[135]

The sort of information that data protection and privacy regulations cover is information linked to our physical, psychological, or behavioral qualities that are registered, kept, or gathered. However, we must not misinterpret personal data with identity attributes: while all identity attributes are personal data, personal data is not always an identity attribute: for example, the address is a component of personal data, but because multiple people can have the same address, this segregated data is not an element of identity and can only be considered when combined with other components.[136]

As has been seen from the above, the trend toward digital activities and services, especially in the healthcare sector, has heightened the demand for improved digital identification tools to prevent fraud and improve the efficiency of online transactions.[137] Some analysts[138] have made the case that existing methods to digital identification frequently fail to adequately address data privacy concerns.[139]

135 Congressman Bill Foster. 2021. Foster, Katko, Langevin, Loudermilk Introduce Bipartisan Digital Identity Legislation. [online]. [Accessed 9 August 2021].

136 Ahmed, U., Gorfine, D., Lau, I., Sturtevant, M., Stephen, K., Jeong, S., Minhas, S. and DiNapoli, R., 2021. The U.S. Digital Identity Crisis | The Regulatory Review. [online] The Regulatory Review. [Accessed 9 August 2021].

137 Nyst C, Makin P, Pannifer S, Whitley E and Birch D (2016) Digital Identity: Issue Analysis. Guildford: Consult Hyperion and Omidyar Network.

138 Beduschi, A., 2021. Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. Data & Policy, 3.

139 Beduschi, A., 2021. Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. Data & Policy, 3.

Data Protection Issues in the Context of Digital Identity

The creation of a more data privacy and human rights compatible framework for digital identification might be a potentially beneficial result of the current situation with fighting adapting to the COVID-19 reality. However, for such a framework to succeed, two requirements must be met: (1) respect for and protection of data privacy, regardless of the architecture or technology used, and (2) consideration of the larger implications of digital identity on people human rights. Regardless of the architecture or technology used, data privacy must be prioritized in the design, development, deployment, and assessment of digital identification systems.[140]

The necessity of privacy and data protection is becoming increasingly acknowledged as more social and commercial activities take place online. The collection, use, and disclosure of personal information to other parties without knowledge or consent is also a source of concern. The collection, use, and disclosure of personal information to other parties without knowledge or consent is also a source of concern. 128 of the 194 nations have enacted legislation to provide data and privacy protection. Africa and Asia have comparable adoption rates, with 55 percent of nations adopting such laws, including 23 least developed countries. Noncompliance with relevant data privacy regulations may result in penalties, litigation, and even the restriction of a site's usage in some areas.

There is no privacy law at the federal level like the EU's GDPR in the USA. Instead, there are numerous federal privacy laws that are vertically focused, as well as a new generation of state-level consumer-oriented privacy legislation. The Federal Trade Commission Act (FTC Act) has wide jurisdiction over business companies to combat unfair or "deceptive trade practices, "The Federal Trade Commission does not specify what information should be included in website privacy policies. To protect consumers' privacy, the FTC issues regulations with enforcing privacy laws and takes enforcement actions.[141]

140 Beduschi, A., 2021. Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. Data & Policy, 3.

141 Federal Trade Commission. n.d. Federal Trade Commission Act. [online]. [Accessed 9 August 2021].

California's Consumer Privacy Act (CCPA) does not address consumer data privacy, at least for California residents. However, it does come close to addressing the issue and is a great exercise to compare and contrast with Europe's General Data Protection Regulation (GDPR). The Californian Consumer Privacy Act, on the other hand, comes close to GDPR to addressing consumer data privacy, at least for California residents.[142] In addition, The California Privacy Rights Act, which is modeled on the CCPA, was approved by voters in 2020. The CPRA creates a new privacy authority. The California Privacy Protection Agency will be given the authority to fine violators, hold hearings on privacy violations, and clarify privacy policies. It is a five-member body that will begin the enforcement six months after the CPRA takes effect on July 1, 2023.[143] In contrast, GDPR Regulation has covered all EU Member States.

The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights[144](Article 8)[145], and the European Charter of Fundamental Rights (Article 7). Human dignity is recognized as an absolute fundamental right in the EU. To be independent, in charge of information about yourself, and to be left alone is crucial in this concept of dignity, privacy, or the right to a private existence. Privacy is a communal value as much as an individual right.

Data protection stems from the right to privacy, and both are important in protecting and advancing fundamental values and rights, as well as exercising other freedom and rights, such as free speech and the right to assemble. Data protection refers to the safeguarding of any information belonging to an identified or identifiable natural person, such as names, birthdates, photos, camera footage, email addresses, and contact information.[146]

142 Osano. 2021. Data privacy laws: What you need to know in 2021 | Osano. [online]. [Accessed 9 August 2021].

143 Green, A., 2021. Complete Guide to Privacy Laws in the US | Varonis. [online] Inside Out Security. Accessed 9 August 2021].

144 Eur-lex.europa.eu. 2012. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION C 326/391. [online]. [Accessed 9 August 2021].

145 Echr.coe.int. 2021. Guide on Article 8 of the European Convention on Human Rights. [online] [Accessed 9 August 2021].

146 Edps.europa.eu. 2021. Data Protection. [online] [Accessed 10 August 2021].

Data Protection Issues in the Context of Digital Identity

In April 2016, the EU adopted a new legal framework — the General Data Protection Regulation (GDPR) and the Data Protection Directive for the law enforcement and police area. Fully applicable across the EU in May 2018, the GDPR is the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age.[147] Among other important legal implications, GDPR provides a definition of "Privacy by Design."

Ann Cavoukian coined the phrase "Privacy by Design" in the 1990s to address the ever-increasing and systemic implications of information and communication technologies, as well as large-scale networked data systems. The objectives of Privacy by Design — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles.[148] Cavoukian's principles also advocate for transparency and visibility, as well as user-centered approaches to system design, operation, and administration.

"Privacy by Design" and "Privacy by Default" have been commonly discussed data protection concepts. The original ideas for "Privacy by Design" were presented in the 1970s and were integrated into the RL 95/46/EC data protection directive in the 1990s. According to this Directive's recital 46, technical and organizational measures (TOM) must be considered to preserve data security at the time of planning a processing system. The phrase "Privacy by Design" simply means "data protection through technological design."[149]

147 Edps.europa.eu. 2021. Data Protection. [online] [Accessed 10 August 2021].

148 Cavoukian, A., 2011. Privacy by Design The 7 Foundational Principles. [online] Ipc.on.ca. [Accessed 10 August 2021].

149 General Data Protection Regulation (GDPR). n.d. Privacy by Design | General Data Protection Regulation (GDPR). [online]. [Accessed 10 August 2021].

Design is the greatest method to ensure privacy in a rapidly changing digital environment. As a result, industrialized nations are boldly implementing SSI systems in their digital identity management projects. By providing data owners total control over their identity data, SSI intends to undermine the federated digital identity model. SSI systems are decentralized systems based on blockchain-based (not necessarily!) trust and transparency platforms. By design, these technologies protect anonymity and eliminate the identity triangle's third-party identification organizations. Additionally, SSI systems allow data owners to share identity data with organizations with ease and have the option to revoke data access.[150] The next section will specifically describe the existing SSI regulatory frameworks.

150 Medium. 2020. Self-Sovereign Identity: Achieving privacy by design. [online]. [Accessed 10 August 2021].

SSI specific regulation

SSI is a relatively new idea, and many technological difficulties must be overcome before it can be used for its present and future objectives in identifying and addressing global economic crises. Intergovernmental organizations and governmental unions, such as the ID2020 Alliance and the EU, have emphasized its development, highlighting the need to provide legal identity to all invisible and vulnerable individuals by 2030 in order to make them visible and reintegrate them into society.[151]

At the EU level, the eIDAS Regulation established a trust structure.[152]eIDAS sets the degrees of assurance for electronic identification and the basis on which any EU Member can recognize the credentials of other EU Members. These categories are designed to be applicable to a variety of identity management systems. The Regulation also allows for the use of electronic signatures and seals by assuring their legal effect and enables approved companies to serve as "trust service providers." [153] Since its inception in 2018, the European Blockchain Partnership has brought together 29 countries (all EU member states, Norway, and Liechtenstein), as well as the European Commission (EBP), to work together to maximize the potential of blockchain-based services for the benefit of residents, community, and the economic system.[154] The European Commission recently[155] proposed a framework for a European Digital Identity that would be available to all citizens, residents, and businesses in the EU. Citizens will be able to confirm their identity and trade electronic documents from their European Digital Identity wallets with the push of a button on their phones.

151 Un.org. 2021. ID2020 Summit 2016. [online] [Accessed 13 June 2021].

152 Shaping Europe's digital future. 2021. eIDAS Regulation. [online]. [Accessed 11 June 2021].

153 UNHCR Blog. 2018. Bridging the identity divide – Is Portable User-Centric Identity Management the Answer? – UNHCR Blog. [online]. [Accessed 13 June 2021].

154 CEF Digital. 2021. EBSI. [online]. [Accessed 13 June 2021].

155 Press release. 2021. Commission proposes a trusted and secure Digital Identity for all Europeans. [online]. [Accessed 13 June 2021].

Chapter 7

SSI Use Cases

Casper

Potential SSI Application

The benefits of SSI solutions were described earlier in the paper. The areas of the current and potential use of the technology are vast and include the public and private sector, expansion of the use in the digital world. As a result, SSI may have a genuine value that may be acquired by both individuals whose personal data is at play and companies. The possible applications of SSI are numerous, ranging from the public sector to banking, commerce, and healthcare. An SSI wallet could be used to prove one's qualifications and identity when applying for a job, opening a bank account, issuing a driving license, securing a mortgage, or making a purchase in an online store. SSI also means no more registration across different platforms using various usernames and passwords, and hence no need to maintain multiple personal accounts. SSI translates to reduced administrative burden and improved customer experience.

An increasing number of SSI platforms, business actors, and technical teams are dedicated to creating and strengthening the SSI and decentralized identity architecture.

ID Services

Government-issued digital identity documents are frequently eIDs that are either a "smart" document/chipcard with some cryptographic/electronic equipment (as in Estonia, Germany, and a few other countries) or a centralized IT system without a physical eID (as it is the case in the Blockchain Usage for Government-Issued Electronic IDs: A Survey 159 Aadhaar system in India). Aadhaar uses biometric "keys" to match them to the system-stored data; a person may receive a "printout" as non-binding evidence of identity, but the printed copy cannot be used for identification by itself. As a result, the use cases of government-issued eIDs differ per nation and serve to identify residents in order for them to access services offered by the respective government.[158] In Europe, the digital identification environment is changing rapidly, and innovation is accelerating. In addition, there is a lot of fragmentation, so unification is both inevitable and crucial for digital identity to fulfill its promise.

In the meantime, dedicated service providers that aggregate identity methods for relying parties can help improve the reach of individual methods on the side of the relying party. The role of governments varies and ranges from the full-fledged identity provider (for example, Estonia) through creating a concrete legal framework (for example, Switzerland, Sweden, Norway, and the Netherlands) to a more passive stance (for example, Germany). Either way, broad and interoperable digital identity is necessary as data transactions between economic actors increase exponentially, all of which need to be enabled and secured by trusted digital identities. Building on regulatory efforts formed under eIDAS, private and public sectors need to strengthen collaboration toward a more harmonized and interoperable landscape of digital identity in Europe.[159]

158 Kuperberg, M., Kemper, S. and Durak, C., 2021. Blockchain Usage for Government-Issued Electronic IDs: A Survey. [online] Dbsystel.de. [Accessed 2 June 2021].

159 Wirecard.com/. 2019. Digital Identity: Concepts, State of Play, and Its Role in the Data-Sharing Economy. [online]. [Accessed 9 August 2021].

Public Sector

Europe is most likely the world's most developed and diversified area for digital identification systems and solutions. One explanation for this high level of maturity is that virtually all nations have successfully digitized their official identity services.[160] On July 5, the European Union called for the creation of the ESSIF, which may serve as a safe European eID. ESSIF will provide a standard self-sovereign identity (SSI) capability, allowing individuals to construct and govern their own identities across borders without relying on centralized authority. Some nations, such as Estonia, have had high adoption rates, while others, such as Germany, continue to have low adoption rates.[161]

In Switzerland, **Zug**, popularly known as the "crypto valley," has collaborated with uPort to develop an SSI solution for its people that runs on the Ethereum blockchain. Users in Zug can use the SSI to pay parking fines, register for elections, and access e-government services online. Zug collaborated with the city of Zug, the Institute for Financial Services Zug (IFZ) of Lucerne University, platform integrator TI&M, and voting platform Luxoft to build the world's first live implementation of a self-sovereign government-issued identification project on the Ethereum blockchain.[162]

In Belgium, a project named **"Blockchain on the Move"** is experimenting with SSI and its municipal application. Following multi-month market research, the Blockchain on the Move collaboration chose Jolocom as its technical partner to build SSI software during the project's starting step.[163] It examines how SSI can be utilized in e-government applications as well as how state-issued credentials can be used in private industry B2B and B2C transactions.[164] **Jolocom** has developed an open-source protocol for the decentralized sharing of digital identifying data in Germany, in addition to Belgium. Jolocom has also created an application that allows users to maintain their personal information in a mobile wallet in a safe manner.

160 Wirecard.com/. 2019. Digital Identity: Concepts, State of Play, and Its Role in the Data-Sharing Economy. [online]. [Accessed 9 August 2021].

161 Little, K., 2021. Data Sovereignty and Trusted Online Identity — IEEE SA. [online] IEEE SA. [Accessed 8 August 2021].

162 ConsenSys. n.d. Government Issued Blockchain Identity: Zug Case Study | ConsenSys. [online] [Accessed 9 August 2021].

163 Jolocom. 2021. About — Jolocom. [online] [Accessed 9 August 2021].

164 Wirecard.com. 2019. Digital Identity: Concepts, State of Play, and Its Role in the Data-Sharing Economy. [online]. [Accessed 9 August 2021

Public Sector

In Finland, a research project called **"TrustNet"** is exploring the use of SSI in a network of research institutions and industry partners.[165] TrustNet is a study and pilot project for decentralized personal data management that includes members from the Finnish digital services industry as well as three research organizations (Aalto University, University of Oulu, and the Tampere University of Technology) where the sandbox environment is also provided by the **Sovrin Foundation**.[166]

Digital identities are likewise high on the German government's priority list. The **IDunion** network's second project phase began on April 1, 2021, and will last three years. SSI technology will be used in more than 40 pilot applications throughout this time. Bosch is sending a team from its Economy of Things division to the event. Werner Folkendt and his colleagues are working on a globally deployable SSI application that is already benefiting businesses in the areas of corporate identification and master data management.[167]

In Canada, **the Digital ID and Authentication Council** (DIACC) is a partnership of public and private sector organizations dedicated to providing Canadians with a secure digital identity experience. The Pan-Canadian Trust Framework (PCTF), led by DIACC, is a framework consisting of agreed-upon legal, business, and technological principles for identity, authentication, and authorization agreed on between participating public and private sector organizations across Canada.[168]

165 GlobeNewswire News Room. 2017. Sovrin Foundation and Finland's TrustNet Join Forces to Build a Trust Network for Distributed Personal Data Management. [online]. [Accessed 9 August 2021].

166 Wirecard.com/. 2019. Digital Identity: Concepts, State of Play, and Its Role in the Data-Sharing Economy. [online].[Accessed 9 August 2021

167 Bosch Global. 2021. Self-sovereign identities. [online] [Accessed 11 August 2021].

168 Diacc.ca. n.d. Interoperability: Digital Identity You Can Use. [online]. [Accessed 9 August 2021].

Public Sector

SecureKey, for example, works with government, business, and consumer-focused groups to constantly enhance **Verified.Me,** a mutually beneficial network that assists individuals with their digital identity needs, such as online access to financial or health information.Employment and Social Development Canada's (ESDC) adoption of Verified.Me. ESDC, a public sector entity, is now able to receive verifiable credentials from users through Verified.Me securely streamlines the process by allowing users to use their private-sector credentials for this registration and verification. Verified.Me has been adopted by Employment and Social Development Canada (ESDC). ESDC, a public sector institution, may now accept VCs from users.[169]

The US Department of Homeland Security's Science and Technology Directorate has invested in the development of SSI standards. The Science and Solutions Directorate (S&T) of the Department of Homeland Security has granted $1.3 million to 13 small firms for the development of innovative cybersecurity technology.[170]

The **Illinois Blockchain Initiative** is collaborating with Evernym on a birth register pilot in the United States, where self-sovereign identities are generated, and government agencies make "verifiable claims" for birth registration features such as legal name, date of birth, sex, or blood type.[171]

In early 2016, Australia Post teamed up with The Boston Consulting Group (BCG) to conduct a study of consumers, small company owners, and employees of major corporations and government agencies on the topic of digital identification. Researchers discovered that while these groups considered identity management to be time-consuming, repetitive, and tedious, they struggled to envision a society that was better suited to deal with it.[172]

169 Boyson, A., 2021. The Future of Digital Identity in Canada: Self-Sovereign Identity (SSI) and Verified.Me | Verified.Me. [online] Verified.Me. [Accessed 8 August 2021].

170 Dhs.gov/. 2016. News Release: DHS S&T Awards $1.3 Million to Small Businesses for Cyber Security Research and Development. [online] [Accessed 9 August 2021].

171 Nascio.org. 2017. The State of Illinois Blockchain Initiative. [online]. [Accessed 9 August 2021].

172 Soltani, R., Nguyen, U. and An, A., 2021. A Survey of the Self-Sovereign Identity Ecosystem. Security and Communication Networks, 2021, pp. 1-26.

MATTR[173] solutions provide the foundation for solving and removing the historical difficulties of digital security, privacy, and data verification, ushering in a new era of trust. Mattr is an SSI platform that uses DIDs and verified credentials.

The aim of the **LifeID Foundation**[174] is to provide every individual with a self-sovereign digital identification that will be known as their "lifeIDTM." The lifeID Platform will be used to build LifeID, which will be an open, permissionless, and highly secure blockchain-based identity service. The self-sustaining, self-funding lifeID Foundation will install and maintain this platform, which is an identity-as-a-service (IDaaS) layer for the blockchain ecosystem that enables a wide range of identity-specific transactions.

SelfKey is a self-sovereign identity technology stack that includes an open-source identity wallet for the identity owner, a marketplace with real products and services, a JSON-LD protocol, connectivity to third-party identity microservices, and a native token called "KEY" that allows the SelfKey ecosystem to exchange value and data.[175]

Healthcare

The necessity to advance and digitize our lives has become apparent as a result of the COVID-19 outbreak's limits and restructuring of society's functioning. Thus many technological solutions have evolved since the start of the global pandemic in early 2020. Electronic health records (EHR) systems abound on the market, and their number continues to rise. Motivated by industrial regulations, automation processes, paperless efforts, privacy and security risk mitigation, and the desire to improve the health and wellbeing of people, academic research is moving toward these issues and investigating technological advances and ways to solve them.[176]

173 Mattr.global. 2021. Restoring trust in digital interactions. [online]. [Accessed 9 August 2021].

174 Lifeid.io. n.d. An open-source, blockchain-based platform for self-sovereign identity. [online] [Accessed 9 August 2021].

175 SelfKey. n.d. Self-Sovereign Identity for more Freedom and Privacy — SelfKey. [online] [Accessed 11 August 2021].

176 SIQUEIRA, A., ROCHA, V. and F. DA CONCEIÇÃ,, A., 2021. Blockchains and Self-Sovereign Identities Applied to Healthcare Solutions: A Systematic Review. ACM Comput. Surv., Vol. 1, No. 1 Article 1.

The COVID Credentials Initiative (CCI) is an open worldwide community working to make open-standards-based privacy-preserving credentials and other related technologies compatible for public health reasons. The goal of this focus group is to bring together important stakeholders to discover trustworthy and scalable strategies to combat the worldwide COVID-19 epidemic. They are working to inform and empower Public Health Authorities (PHA) by assisting them in identifying and formulating an approach for the adoption of VCs to enhance their implementation of the COVID-19 vaccine administration. To do so, they will form jurisdiction-specific subgroups with the goal of gaining momentum with PHAs and establishing POC or pilot programs in their respective countries. The United States is the first grouping.[177]

The International Civil Aviation Organization (ICAO), the World Health Organization (WHO), and other international institutions are working with businesses to develop technological advancements to reduce the potential risk of travel during the pandemic. Players in the travel sector ecosystem should consider how DLT may be utilized to revitalize travel by making it easier for individuals to establish their COVID-19 immunity status to airport authorities, airlines, immigration offices, and other relevant institutions. The importance of self-sovereign identity and VCs is central to this innovative solution. This combination would enable hospitals and testing institutions to provide digital COVID-19 immunity certificates to patients, which could subsequently be shared with and confirmed by the relevant authorities.[178]

177 Covidcreds.org. 2021. COVID-19 Credentials initiative : Home. [online]. [Accessed 10 August 2021].

178 Covidcreds.org. 2021. COVID-19 Credentials initiative : Home. [online]. [Accessed 10 August 2021].

Education

Higher education has long been a technological study area for blockchain identification. Nevertheless, a wide range of industries and organizations are already investigating the prospects of SSI, with live student solutions being examined. **Evernym** has identified three key areas of SSI benefit as a result of discussions regarding lifelong learning:

1. **Student lifecycle.** "Know your student," onboarding, and authentication.

2. **Study credentials.** Qualifications, micro-credentials, and learner records.

3. **Life beyond studying**. Getting a job, moving home, opening accounts.

They cite Canada as an example, claiming that the governments of British Columbia and Ontario kicked off the **VON** program by issuing millions of organizational credentials. This, according to Evernym, may mean that the same technology that authenticates student credentials could also be used to authenticate communications between institutions and other organizations.[179]

Receivers should be able to control all aspects of their credentials in a truly self-sovereign ecosystem, notably where they are stored, who they are shared with, and how they are recognized as individuals in the credential. They should be able to own, control, and choose to disclose all or portions of their digital credential records in return for services and information they want—without having to rely on a third-party middleman to validate or match such information or identities to other data all of the time.[180]

179 Covidcreds.org. 2021. COVID-19 Credentials initiative : Home. [online]. [Accessed 10 August 2021].

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

Pilots in credentials and infrastructure are the focus of blockchain and education practice in 2021. [181] Blockcerts is an open standard for creating apps that issue and validate authentic blockchain records. Certificates for civic records, academic qualifications, professional licenses, workforce development, and other items may be included. Blockcerts is dedicated to ensuring that all participants have self-sovereign identification and that recipients have control over their claims through simple tools like the certificate wallet (mobile app).[182] **Blockcerts** is likewise dedicated to ensuring that credentials are always available, with no single point of failure. Some authors[183] point out that The Government of Malta, the Caribbean Examinations Council, the Federation of State Medical Boards (FSMB), and the MIT Media Lab have all launched high-profile blockchain certification projects based on the Blockcerts standard since 2017. In addition to Blockcerts, the authors highlight another project.

Qualichain is a centerpiece KMI project funded by the European Commission to better understand the interplay of blockchain technology, semantics, and data analytics. It serves a dual purpose of storing and issuing credentials as well as providing a comprehensive set of innovative technology such as career counseling, intelligent profiling, and competency management. The utilization of the QualiChain platform and services to support and streamline public sector recruiting and competency management procedures is the focus of this pilot use case.[184]

There is also the **Digital Credentials Consortium (DCC)**, which is a global collaboration of twelve institutions with the intent of developing a centralized platform or standard for academic credentials across universities and other educational establishments so that students can easily receive store, and share their credential records. Admission committees and companies will be able to verify credential accuracy, detect counterfeit credentials, and conduct a comprehensive evaluation of a student's talents using this one-stop solution.[185]

181 NuWireInvestor. 2021. The Role of Blockchain Technology in the Education Sector — NuWireInvestor. [online]. [Accessed 9 August 2021].

182 Blockcerts. n.d. Blockchain Credentials. [online] [Accessed 9 August 2021].

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

184 Kontzinos, C., Markaki, O., Kokkinakos, P., Karakolis, V., Skalidakis, S. and Psarras, J., 2020. Decentralised Qualifications' Verification and Management for Learner Empowerment, Education Reengineering and Public Sector Transformation: The QualiChain project. [online] Semanticscholar.org. [Accessed 10 August 2021].

185 MIT Open Learning, 2021. Digital Credentials Consortium: Evaluative User Research. [online] Medium. [Accessed 10 August 2021].

The **EBSILUX project**[186] was developed in collaboration with Luxembourg's Ministry for Digitalisation, Infrachain, the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), and the Luxembourg Institute of Science and Technology (LIST) in response to a call for projects issued by the European Union in 2020. The EBSILUX Project, which is co-funded by the European Union, connects Luxembourg to the European Blockchain Services Infrastructure (EBSI) and implements a European EBSI use case at the national level.

This improves the internal market operations and boosts the European economic resilience. EBSI employs blockchain technology to create cross-border services that will help public administrations and their ecosystems to validate the information and increase the trustworthiness of services. EBSI developed a distributed blockchain node network across Europe to assist applications focused on specific use cases. By hosting one of EBSI's servers, the EBSILUX project helps EBSI's overall resilience and security. Luxembourg places a high value on student mobility, multilingualism, and international collaboration. EBSI's Diplomas use case is being implemented by EBSILUX. The use case offers digital academic certificate records in Luxembourg for the sake of openness and confidence between schools/universities, students, and employers.[187]

Atala PRISM[188] is an open-source, linear blockchain solution based on the Cardano system, a technology developed by IOHK. Its implementation consists of a mobile app, a web wallet, a management panel, as well as SDKs and APIs. Education, health, government, enterprise, finance, travel, and social are some of the use cases for Atala. They are collaborating with the Ministry of Education and universities in the Republic of Georgia. Students may use Atala PRISM to receive, save, and submit their achievements directly from their cellphones. Immediate credential verification eliminates the need for background checks, saving institutions and companies precious time and resources.

186 Infrachain. 2021. Launch of the EBSILUX Project and the Diplomas Use Case in Luxembourg — Infrachain. [online]. [Accessed 10 August 2021].

187 Infrachain. 2021. Launch of the EBSILUX Project and the Diplomas Use Case in Luxembourg — Infrachain. [online]. [Accessed 10 August 2021].

188 Atalaprism.io. n.d. [online]. [Accessed 10 August 2021].

Smart cities

"A smart city is a framework, predominantly composed of Information and Communication Technologies (ICT), to develop, deploy, and promote sustainable development practices to address growing urbanization challenges."[189]

MyEGO is a Germany-based platform for SSI management. Their solution focuses on the user, rethinking and developing data management and processes. They created the Smart City project, which attempts to promote the digitization of analog operations in cities. The smart city, on the other hand, brings with it new challenges that must be addressed in order for the digital transition to be effective for all stakeholders. Digital transformation necessitates the creation of new interfaces that: put individuals at the center and give them control over their personal data; are open to (new) economic and municipal business operations; and simplify existing structures and procedures in businesses and government.[190]

Kokosioulis and Stockburger (2020)[191] suggest and investigate the usage of SSI in a Decentralized Identity Management for Public Transportation system. They point out that the SSI environment and ecosystem of applications are always expanding. Public transportation in conjunction with Self-sovereign Identity appears to have a bright future. Respecting privacy, data protection rules, and interoperability, allows the sector to integrate with any other form of application. The ecosystem as a whole might improve its usefulness by extending application integration. Private transportation services, such as car-sharing or scooter-sharing, might, for example, link with public transit services to provide a combined solution.[192]

189 Thales Group. n.d. Secure, sustainable smart cities and the IoT. [online]. [Accessed 10 August 2021].

190 myEGO English. n.d. SSI in the smart city – a part of the digitization in the modern city.. [online]. [Accessed 10 August 2021].

191 Kokosioulis, G. and Stockburger, L., 2020. Decentralized Identity Management for Public Transporation. [online]. [Accessed 10 August 2021].

192 Kokosioulis, G. and Stockburger, L., 2020. Decentralized Identity Management for Public Transporation. [online]. [Accessed 10 August 2021].

Traveling

The IATA Travel Pass is a digital credential system that allows airlines, governments, and other organizations to immediately validate travel and health documents (such as COVID-19 test results) in a highly secure and privacy-protecting way. The International Air Transport Association (IATA) created Travel Pass, which makes use of Evernym's Verity, Verity Flow, and Mobile SDK technologies.[193]

ShareRing's[194] travel app will provide a more seamless customer experience by consolidating all necessary activities and bookings into a single ecosystem, including hotel check-ins, flights, visa and tourist applications, COVID-19 tests, SSI cards, mobile wallets, payment solutions, and vehicle rentals. The app is part of the company's larger ecosystem of blockchain solutions. ShareRing's application is already linked with over 2.6 million hotel and activity providers worldwide, and they offer a sharing marketplace that eliminates intermediaries like Uber and Airbnb. SharePay is their stablecoin, which 'hides' the end-user from the complexities of cryptocurrencies.[195]

The architecture of the German project **GAIA-X** is based on key ideas such as sovereignty, distribution, and federation and must adhere to EU rules such as GDPR and eIDAS. As a result, GAIA-X members have complete control over their identities and trust decisions thanks to a decentralized identity management system based on SSI standards.Furthermore, the identities utilized are self-owned and maintained.

193 Evernym. n.d. IATA Travel Pass: Getting Started — Evernym. [online]. [Accessed 10 August 2021].

194 ShareRing.Network. 2021. ShareRing.Network | Open the world with ShareRing ID. [online] [Accessed 10 August 2021].

195 Amoils, N., 2020. ShareRing Uses Blockchain To Solve Self Sovereign Identity And Proof Of Health Simultaneously. [online] Forbes. [Accessed 10 August 2021].

Finance

Mastercard's[196] digital identity strategy is based on a distributed, user-centric paradigm. Mastercard is looking towards a decentralized digital identity for financial transactions, government interactions, and online services verification. It is a well-known truth that digital identification might allow those without physical documents or credit histories to access banking and other services.

CULedger, a Denver-based company providing self-sovereign identity capabilities for credit unions, recently celebrated the launch of its first production credential. For high-risk transactions, CULedger granted its first production credential to a California-based credit union's contact center. Depending on the amount of risk involved, members initiating high-risk transactions or suspected of fraudulent behavior require an average of 40-80 seconds. The credit union UNIFY was able to cut the time it took to authenticate members to less than 10 seconds after using MemberPass.[197]

Banking institutions are also getting on board. One of the major Dutch banks, Rabobank[198] has been investigating Self-Sovereign Identities for KYC and mortgage applications. **TietoEVRY**[199] also helped **Infopulse** launch a banking KYC system, powered by Hyperledger Fabric, for collecting, storing, and operationalizing customer information in a secure, auditable manner.

196 Mastercard.us. n.d. DIGITAL IDENTITY March 2019 Restoring Trust in a Digital World. [online] [Accessed 10 August 2021].

197 Goldfarb, S., 2019. Six ways self-sovereign identity is transforming financial services — Evernym. [online] Evernym. [Accessed 10 August 2021].

198 Lamers, D., 2019. The universal ledger agent: a logical result of Rabobank's journey in blockchain based self-sovereign identity. [online] GitHub. [Accessed 10 August 2021].

199 Infopulse. n.d. Know Your Customer (KYC) System on Blockchain for Banks | Case Study. [online]. [Accessed 10 August 2021].

Property rights

For property rights, the most fundamental use of SSI is to give people identities that they may use to interact with land administration services. In the absence of official documents such as a signed survey plan or a notarized will, SSI can assist clients in establishing evidence of their property ownership. SSI credentials are highly versatile, and they don't have to be digital copies of old paper papers. SSI is an emerging technology, and although it has been employed for purposes like distributing food and energy aid and establishing an economic identity for refugees, it has not yet been used for land and property rights.[200]

Gaming industry

Gamers in the traditional virtual world are represented by their own characters, who have behavioral data and records, as well as equipped goods that players create on the platform. Such involvement is recorded and controlled by a single game publisher in a centralized or conventional database structure. More virtual identity autonomy necessitates the integration of SSI infrastructure into gaming.

Liquid Avatar,[201] a company headquartered in Canada, has begun to build the base for a world of virtual personas and self-managed identities (aka self-sovereign identities or SSI) by making its offering attractive to a new generation that's growing up on online games. When a user sends their avatar to anyone, the icon will contain more than just a picture of a cartoon character. It carries within it three other layers of information that help the user to manage and share only the information he or she wants with third-party applications.[202]

200 New America. n.d. Self-Sovereign Identity and Property Rights. [online]. [Accessed 10 August 2021].

201 Liquidavatar.com. n.d. Liquid Avatar. [online] [Accessed 10 August 2021].

202 Brekke, J. and Alsindi, W., 2021. Cryptoeconomics. Internet Policy Review, 10(2).

Digital use cases

In recent years, SSI has become one of the most widely utilized concepts in the Identity Management context. Many supporters believe that we are on the cusp of a technology breakthrough that can be utilized to create a SSI Management System as a result of a few recent creative technological developments. Many people believe that the arrival of blockchain technology will provide the technological foundation on which the concept of SSI may be restored.[203]

In the past few years, a number of networks have developed that allow for general-purpose computing as well as easy smart contracts and token creation. This layer 2 crypto economics includes the development of ostensibly important economic assets that are unrelated to the network substrate's underlying security characteristics, such as ERC20-type Ethereum tokens, Non-Fungible Tokens (NFTs),and more recently Decentralised Finance (DeFi) synthetic tokens.[204] DeFi, unlike other centralized financial systems, does not provide an identity layer, which is often implemented through KYC procedures.

Alternatively, DeFi connects directly to smart contracts, removing the requirement for a legal identity verification procedure. As a result, the platform does not need to engage with user identity to conduct trades.[205] DeFi prioritizes decentralization and anonymity in addition to decentralization.Users of decentralized apps (DApps) are drawn to the concept of being able to borrow, sell, swap, and lend without the other party knowing anything about them.[206] The disadvantage of this structure is that users are unable to make educated judgments about how much to lend, interest rates, and loan terms, resulting in excessive collateral requirements. As a result of treating all users the same, DApps are unable to provide individualized services and non-collateralized borrowing, resulting in a poor user experience.[207]

203 Ferdous, M., Chowdhury, F. and Alassafi, M., 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access, 7, pp.103059-103079.

204 Brekke, J. and Alsindi, W., 2021. Cryptoeconomics. Internet Policy Review, 10(2).

205 Gataca.io. 2021. Decentralized Finance & Self-sovereign Identity: A tale of decentralization, a new paradigm of trust.[online] [Accessed 12 August 2021].

206 Gataca.io. 2021. Decentralized Finance & Self-sovereign Identity: A tale of decentralization, a new paradigm of trust.[online] [Accessed 12 August 2021].

207 Raphael, D., 2021. How Bloom is Bridging the Gap Between DeFi and Decentralized Identity [online] Bloom.com. [Accessed 12 August 2021].

Digital use cases

While the marketplaces for decentralized financial and decentralized identity are both rapidly developing with new and innovative technologies, they are currently mostly fragmented. Whereas the identity record or credential is generated off-chain, it can be swiftly transferred onto the blockchain and converted into a digital identification solution utilizing technology developed by a number of companies, including **Sidetree and Bloom.** The inventors explain that despite the fact that decentralized identification systems are chain-adjacent, they require an intermediary to permit the transmission of chain-adjacent data to on-chain requestors like DeFi apps. Such "bridges"come in a range of shapes and sizes, and can be utilized to provide decentralized access to DID systems. **Oracles**, for example, can connect to data vaults to have access to information that is specific to them.[208] However, there is a trust issue with the majority of popular Defi lending apps. Because there is a current need and demand for decentralized identity solutions, DeFi is highly adapted to be integrated with such platforms. Because of its urgent requirement from both a customers' needs and a regulatory obligation, it is a strong first-mover fit with current DID solutions.[209]

Another crypto economy component that can tremendously benefit from the adoption of SSI is NFT. Lack of NFT verifiability also leads to intellectual property and copyright infringements. In addition, the chain of custody may be tracked back to the creator's public address to see if the same artist has created identical artwork at that location.Consequently, there is no simple or efficient method of checking an NFTs developer's trustworthiness. Nonetheless, there is no easy or foolproof technique to check an NFTs developer's legitimacy. In case verification is not included in the NFT, it will just verify ownership of that NFT.[210]

208 Raphael, D., 2021. How Bloom is Bridging the Gap Between DeFi and Decentralized Identity [online] Bloom.com. [Accessed 12 August 2021].

209 Raphael, D., 2021. How Bloom is Bridging the Gap Between DeFi and Decentralized Identity [online] Bloom.com. [Accessed 12 August 2021].

210 Raphael, D., 2021. How Bloom is Bridging the Gap Between DeFi and Decentralized Identity [online] Bloom.com. [Accessed 12 August 2021].

Digital use cases

Because it was created for blockchain-based IDs, SSI is the best solution for bringing identity to NFTs.

"SSI applications can be used by the creator or artist to prove that a digital or physical item was created by them. Buyers can then double-check that they're getting an artist-made NFT. SSI is what gives NFTs immutable, cryptographically linked "value beyond the token itself."[211]

SSI is a brilliant notion that can be used in any digital actor, including IoT devices, businesses, and digital agents. Of course, in order for it to work, they'll all have to agree on standardized technologies and formats that will allow for seamless integration in any area of the internet that demands a digital identity. SSI relies heavily on blockchain and other distributed ledger technologies. With the evolution of blockchain-based technologies, SSI has the ability to fill in the identity layer that is missing. The focus of this study is on reputation and how it can be developed and placed in the context of SSI and creation of a functional and user-friendly ecosystem. The following chapter will provide readers with further use cases, as well as a more detailed description and study of reputation in digital scenarios.

211 Tanner, J. and Roelofs, C., 2021. NFTs and the need for Self-Sovereign Identity — Gimly Blockchain Projects. [online] Gimly Blockchain Projects. [Accessed 12 August 2021].

Chapter 8

Decentralized Reputation and SSI

Basic Issues in the Field of Reputation

In general, when it comes to human interactions, reputation is the total of all our activities that are mirrored by the society around us in how people behave or interact with us. It is human nature to be concerned about one's reputation. A person's or organization's reputation is a measure of its social status.[211] It is an indirect result of anything and everything that we do.

We may all agree that the social nature of reputation differs from one person's personal view of another. Each reputation value is determined by the audience or algorithms that comprise it. As reputation is a changeable and frequently local phenomenon, one person may have many domain-specific reputations.[212] Reputation is a context-specific phenomenon, and a person may have reputations in multiple contexts simultaneously.[213] The context is essential as past behavior may be a better predictor of future behavior when applied to similar contexts.[214]

Reputation fixes those characteristics of the identity that are significant in the situations of social interactions: qualifications, performance, consistency, etc., which are assessed under conditions of uncertainty before entering into the relationship.[215] "Almost any social or business interaction is established on the basis of the perceived reputation of both the involved parties."[216] Additionally, the existence of reputation itself has a socially corrective impact, as positive or negative social assessment of reputation encourages good behavior over the longer term.[217]

211 Medium. 2018. The Importance and Psychology of Reputation In Human Lives. [online] [Accessed 11 August 2021].

212 Shashkova, 2015. Reputatsionnyi potential v kontekste upravleniya scialnymi sistemami. [online] Cyberleninka.ru. [Accessed 11 August 2021].

213 Randall Farmer, F., 2010. Building Web Reputation Systems. [online] O'Reilly Online Learning. [Accessed 11 August 2021].

214 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021].

215 Shashkova, 2015. Reputatsionnyi potential v kontekste upravleniya scialnymi sistemami. [online] Cyberleninka.ru. [Accessed 11 August 2021].

216 Borderless Technology Corp., 2018. The Importance and Psychology of Reputation In Human Lives. [online] Medium. [Accessed 11 August 2021].

217 Hendrikx, F., Bubendorfer, K. and Chard, R., 2015. Reputation systems: A survey and taxonomy. Journal of Parallel and Distributed Computing, 7, p. 2

Basic Issues in the Field of Reputation

The major difficulty with reputation is that there is presently no way to measure it as an objective value. When reputation becomes measurable, it becomes simpler to assess identification before engaging, resulting in higher trust and better interaction outcomes.[218]

Why do people and businesses seek a good reputation? Actually, a greater reputation is rewarded in the society providing new opportunities and revenues.[219] A good reputation is virtually everything for individuals. Globally, it defines their social standing, the range of available roles, and their capacity to engage in specific social connections. In the case of businesses, a high reputation enhances business value and brand awareness, gives greater chances for maintaining client loyalty, and therefore lowers marketing expenditures.[220]

We believe the society as a whole also benefits from clear reputation calculation and determination. Healthier relationships are built from the start. As defective relationships can be evaluated only ex post facto, trustworthy reputation metrics also avoid the additional costs caused by malicious behavior (e.g., litigations, restarted hiring process, fraud costs). Fair reputation-based decision-making also raises the bar for all the members of society, forcing them to improve.

218 Borderless Technology Corp., 2018. The Importance and Psychology of Reputation In Human Lives. [online] Medium. [Accessed 11 August 2021].

219 Campbell, K., 2021. Why reputation is important for people and business. [online] Blog.reputationx.com. [Accessed 11 August 2021]

220 One eleven web design. 2021. 5 Key Benefits of Having a Good Reputation for Your Business. [online]. [Accessed 11 August 2021].

The Role of Reputation in Building Digital Trust

The Internet has opened up new avenues for human contact. However, with its popularity has come the issue of digital trust. Digital trust is the level of certainty and confidence that two entities have in each other while engaging in and completing digital transactions. With the commercialization of the Internet, the problem grew serious, giving rise to the notion of a sovereign identity. This is how SSI was born.

Despite the fact that more and more transactions are taking place online, faith in technology has dropped by six percentage points by 2020. This is due to a variety of factors. Others are irritated by the absence of direct human interaction, while some depend on their prior unpleasant experience. Some people are worried about the rise in personal data breaches.[221]

SSI is a breakthrough in digital trust. The numerous advantages of the technology are outlined by us in the first chapters, so we will not repeat ourselves. Definitely, DIDs and VCs provide incredible opportunities, but even after them, there are directions to evolve. Imagine the context where SSI is already adopted across numerous regions, jurisdictions, and organizations. You have to make contact with the business. For example, you are going to buy an apartment and contact a real estate agency.

Given that SSI exists, you do this without even leaving your apartment. It seems that everything you need is on your phone. You check the certificate of state registration of the agency and other documents in the VC form. You are convinced of the authenticity of the digital signature after your wallet application has accessed the blockchain. You also check the VCs of your personal manager, confirming his relationship with the agency and authority. Can we stop there and trust the agency completely?

221 Miteksystems.com. 2021. Create digital trust with digital identity technologies | Mitek. [online] [Accessed 11 August 2021].

The answer is no. Are they really as professional as they describe themselves in their promotional materials? How quickly and efficiently do they work? Will you have any problems with documents during the transaction? Will the staff be polite?

The problem is that you will never get a 100% accurate positive answer to such subjective questions. With regard to the future, this is impossible due to the huge number of factors that determine the behavior of people and systems. But the likely outcome can still be assessed. For this, mankind, throughout its entire existence, turns to the record of past events. This is exactly about the phenomenon of reputation.

Before the Internet, reputation was determined by the information that circulated within the community, transmitted from person to person. This is a proven method, and it can even work in e-commerce today. But it should be borne in mind that there were ten times fewer players then, and of course, there were not many ways to mislead a person, which are typical for the Internet. The problem was solved with references provided by vendors and employees. Also, some kind of compliant registry existed for this purpose.[222]

With the advent of the Internet and the rise of e-commerce in the 1990s, the situation has changed. Now users are forced to trust so-called review-based reputation systems. Such a reputation system collects, distributes, and aggregates direct feedback about someone's past behavior. These systems help parties to decide whom to trust, as well as encourage trustworthy behavior without direct knowledge of the parties about each other.[223]

These feedback aggregation systems are the standard to this day, differing in implementation details.

222 Miteksystems.com. 2021. Create digital trust with digital identity technologies | Mitek. [online] [Accessed 11 August 2021].

223 Resnick, P., Zeckhauser, R., Friedman, E. and Kuwabara, K., 2001. Reputation Systems: Facilitating Trust in Internet Interactions. [online] Presnick.people.si.umich.edu. [Accessed 11 August 2021]. p. 1

Basic Issues in The Field of Reputation

One of the most well-known systems is Amazon's reviews. After reviews are left, they are additionally filtered by users with the "Was this review helpful?" button.[224] Moreover, Amazon calculates a star rating using machine-learning instead of a simple average. Several factors are used to ensure the authenticity of the feedback, such as how much time has passed since the review, whether the purchase has been validated, and so on.[225]

eBay's feedback score is based on the number of transactions performed by a buyer or a seller. Hundreds and thousands of individual purchase transaction ratings are used to aggregate the score. E.g., if a seller has a score of 99.5%, it means that 99.5% of the buyers who left feedback for them had a positive experience.[226]

224 Randall Farmer, F., 2010. Building Web Reputation Systems. [online] O'Reilly Online Learning. [Accessed 11 August 2021].

225 Amazon.com. n.d. Amazon.com Help: How Are Product Star Ratings Calculated?. [online] [Accessed 11 August 2021].

226 Randall Farmer, F., 2010. Building Web Reputation Systems. [online] O'Reilly Online Learning. [Accessed 11 August 2021].

Current Problems of Digital Reputation

So, what is the problem with reputation systems? It is stated that every reputation system, regardless of the content kind or audience, would encounter the same types of issues as the community expands:

1. **Problems of scale**. The number of users' contributions to the reputation system may be extremely significant.

2. **Problems of quality**. That's the problem of separating proper events from malicious ones.

3. **Problems of engagement**. Incentivization and rewarding users for contributions may be necessary.

4. **Problems of moderation**. The problem of dealing with malicious behavior quickly and efficiently.[227]

When it comes to the feedback-based systems mentioned above, certain critical issues and shortcomings are evident:

Lack of incentives. In reality, consumers are not rewarded for providing feedback to platforms. Only a small percentage of customers will return to the marketplace after getting the items to post a review. Even if they do, they frequently confine themselves to generalities rather than detailing the object's advantages and disadvantages in depth. Additionally, platforms are trying to stimulate customers in different ways, but sometimes it affects the honesty of reviews. In particular, they may offer bonuses to customers for leaving good reviews.

227 Randall Farmer, F., 2010. Building Web Reputation Systems. [online] O'Reilly Online Learning. [Accessed 11 August 2021].

It should be emphasized that consumers are especially hesitant to provide negative reviews. Parties always bargain, and unhappy customers may just remain silent about their unpleasant experiences in order to avoid tedious inquiries.

Fake reviews. This is one of the main diseases of current reputation systems, which continues to grow. Not too long ago, the study has shown that in some categories on Amazon, about 60% of reviews are fake.[228]

Motivation and the source of feedback vary. Businesses buy fake positive reviews or obvious motivation to extract benefits for themselves or negative reviews to spoil the reputation of their competitors. Disgruntled customers or laid-off workers may give false feedback simply because of their dislike of the company.

Platform lock-in. Thousands of platforms exist where the reputation of people, organizations, and things is formalized. However, there are no mechanisms to share the reputation across them. Although it is technically possible to import reputation from one platform to another, this approach is not large-scale. Often the formats for counting and expressing reputation themselves will be incompatible.

The possibility of manipulation. Like any proprietary code, current systems are like a black box. Thus, nobody can provide assurances that the reputation model is fair as a third party controls the whole process from receiving feedback from users to displaying the results and further system processing based on this result (for example, hitting the top).[229] [230] [231]

We outlined the issues with reputation systems based on explicit feedback (so-called user-driven reputation systems[232]), but this is a very narrow aspect of the problem.

228 Sterling, G., 2018. Study finds 61 percent of electronics reviews on Amazon are 'fake'. [online] MarTech. [Accessed 11 August 2021].

229 Dhakal, A. and Cui, X., 2019. DTrust: A Decentralized Reputation System for E-commerce Marketplaces. [online] [Accessed 11 August 2021]. p. 2

230 Resnick, P., Zeckhauser, R., Friedman, E. and Kuwabara, K., 2001. Reputation Systems: Facilitating Trust in Internet Interactions. [online] Presnick.people.si.umich.edu. [Accessed 11 August 2021]. p. 4

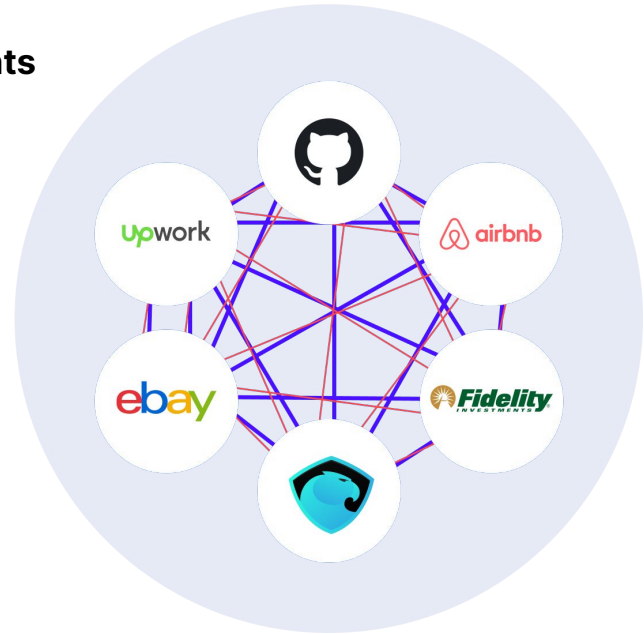
231 Sterling, G., 2020. Fake reviews problem is much worse than people know. [online] MarTech. [Accessed 11 August 2021].

232 Kulshreshtha, A. and Adler, B., 2010. Reputation Systems for Open Collaboration ∗ ABSTRACT. [online] Citeseerx.ist.psu.edu. [Accessed 11 August 2021]. p. 2

Basic Issues in the Field of Reputation

Along with **collective reproduction** — the reputation of the store on the platform, your reputation in the company or DAO, the reputation of an expert on the Q&A service, etc. — which aim to stimulate behavior in a specific community, there is a different one — **individual reputation.** Individual reputation is a combination of collective judgments. It's rather a global assessment of the entire set of qualities of the subject, formed on the basis of a certain set of collective reputation values. In turn, individual reputation may be valued in a new context, either bound to another collective or not. Independently, it regulates the behavior of the subject only in a general sense.

Individual reputation is a combination of collective judgements



Basic Issues in the Field of Reputation

What about the individual reputation in a digital environment? Actually, it **doesn't exist in any aggregated form** on the Internet. That means all the events affecting individual reputation in one way or another take place within scattered platforms. In many cases, one remains anonymous. In others, users act under various pseudonyms with varying degrees of anonymity.

Reputation is formed everywhere: entertainment platforms, professional networks, social profiles, etc. **It is difficult to analyze this data automatically**, and everyone, if interested, is forced to independently wander through all the sources and draw their own conclusions.

Another issue with an individual reputation on the Internet is that in many cases, this data will be **self-asserted** by the subject without any guarantees of its accuracy. Thus, the pieces of data intended to provide additional trust to a relationship in a specific context cannot be trusted by themselves.

The above issues and gaps explain why, as soon as it became technically possible, people began to think about a different approach to reputation. We'll take a closer look at it further.

Decentralized Reputation and SSI

The emergence of blockchain technologies gave new opportunities for building reputation systems. The immutability of blockchain data can act as a barrier for malicious online behavior as data stored placed on-chain can't be removed from there.[233] Blockchain provides transparency on all the transactions, interactions, and assessments so that the reputation system becomes clear and auditable and therefore becomes trustworthy. In addition, it doesn't require trusted centralized authorities to be operated so that lock-in effect and manipulations by owners are avoided.

The freedom that decentralization provides requires caution. The number of attacks that such reputation systems can be exposed to remains possible primarily because of the chain anonymity.

A number of projects focused on certain aspects of decentralized reputation are already in development. Some of them are focused on credit scoring. **Bloom** is trying to provide a blockchain-based cross-border credit scoring and risk assessment platform based on Ethereum and IPFS.[234] **Colendi** is a decentralized credit scoring and microcredit protocol that aims to provide the possibilities of microcredits, installment shopping, and p2p financing to a wide range of people.[235]

Boardroom governance platform for Web3 uses the reputation layer as governance requires continuity across repeated social interactions. They transfer identity systems and user profiles management to the IDX identity protocol, which is used to aggregate on-chain and off-chain transactions into a unified, cross-platform reputation.[236]

233 Lee, S., 2018. A Decentralized Reputation System: How Blockchain Can Restore Trust In Online Markets. [online] Forbes. [Accessed 11 August 2021].

234 van Rijmenam, M., 2018. Why a Decentralised Reputation-Based Society is a Sensible Approach. [online] Linkedin.com. [Accessed 11 August 2021].

235 Colendi. n.d. Colendi. [online] [Accessed 11 August 2021].

236 The Ceramic Blog. 2021. Boardroom is bringing context to Web3 governance. [online] [Accessed 11 August 2021].

Basic Issues in the Field of Reputation

Why did we decide that SSI will come in handy here, leaving attempts to implement a pure blockchain-based solution? An SSI-based reputation system has the following features and benefits:

1. **Portable repudiation.** With SSI stack, reputation state becomes decentralized and isn't stored on any single centralized platform. We remember that it's the Holder who actually owns the data and decides where to store the credentials. All this becomes applicable to the reputations of the subjects.

   What distinguishes the SSI scheme from the simple blockchain-based ones is its independence from this registry. We have already described the benefits of SSI in part of cross-chain utility transfer, and this is exactly the case.

2. **Persistent reputation.** In Web 2.0, all the reputation is scattered across the hundreds and thousands of services the user has ever interacted with. There is no guarantee of their existence in the future. The lifespan of VCs (provided that they are valid) depends only on their responsible storage by the Holder.

3. **Same data can be used across multiple contexts.** Self-sovereignty and portability of reputation means that the same reputation data can be used and reused in an infinite number of services and applications. SSI works across blockchains and merges reputation built on either of them in a single pseudonymous identity.

4. **Privacy by design.** SSI-based decentralized reputation inherits all the privacy-preserving features of SSI like selective disclosure, ZKP, etc. SSI allows one to choose the level of anonymity within a certain context, as well as does not interfere with hiding under a pseudonym when needed. In some cases, the level of disclosure will be essential: higher disclosure will result in a higher reputation score.[237] According to Samuel Smith, "public disclosure is one way to build reputation because it puts the disclosing party at risk to the degree that consequences may arise from the association of their behavior with their identity."[238]

5. **Reuse of ready-made solutions.** Hundreds of brilliant minds have worked and are still working on the problem of identity. Any reputation system will face an identity problem anyway as reputation is incompatible with anonymity. SSI takes care of all the related issues (strict identity binding, anti-sybil measures, unlinkability) since there is no point in trying to reinvent the bicycle.

   What is perhaps the most promising is that SSI provides an opportunity to build a layer of individual reputation on the Internet. The whole set of facts, qualifications, activities will now become a set of VCs.

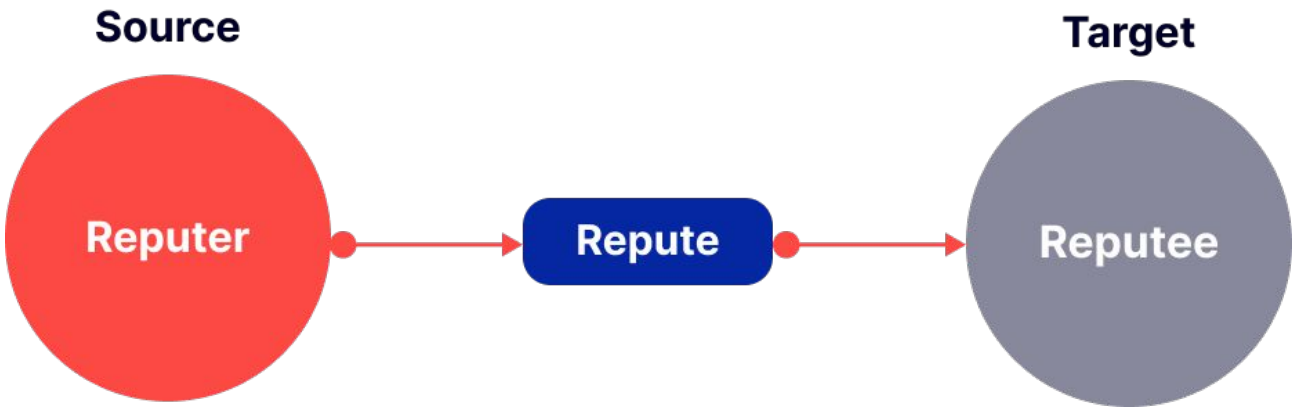
237 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 9

238 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 28.

Reputation Decomposition. Terminology.

Decomposition is a method of scientific cognition that replaces the consideration of a complex, composite concept — an object or phenomenon with the study of its parts of a smaller size. So, when starting exploring a new phenomenon, such as a decentralized reputation, it is extremely important to decompose the phenomenon initially.

Speaking of reputation decomposition, we are sympathetic to the conceptual apparatus and set of primitives that Samuel M. Smith proposed in his paper “Open Reputation Framework” (2015).



Reputation Decomposition. Terminology.

1. A **reputation** is a value based on past behavior based on the processing of pieces of information called reputational events.[239]

2. A **reputational event (or a repute)** is the basic primitive of a reputation system. A set of reputes is the ground of further reputation calculation, that is, to generate reputation scores in specific contexts. It is important to note that a repute is just an objective event, and it does not provide a subjective reputational evaluation by itself. In this sense, It can only be assessed by the scoring model.[240]

   What data can become a repute? Almost any event if there is a possibility to uniquely ascribe it to the subject: your successful deal on eBay, a contribution to an open-source project, or the fact that you were banned from Facebook.

3. A **reputable entity (or a reputee)** is an identity that is the target of reputational events. A person, a collective or organization, a place, or a computational agent — all these entities may become reputees if they are uniquely identifiable.[241]

4. A **reputer** is the primary source of the content of a repute about a reputee. The repute is about a distinct reputational activity of the reputee. One entity may be the reputer and the reputee for a given repute. Additionally, outgoing reputes may affect the reputation of the reputer itself.[242]

5. **Reputation scoring** is primarily the process of retrieval and evaluation of reputes provided to the scoring engine. The reputee in this context is the target of the repute.[243]

239 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p.1

240 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 4-5

241 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 3

242 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 5-6

243 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 4-5

Model Parameters

Reputation is not a one-fits-all term. There can be many reputational interactions of a different nature, completely different from each other, and all of them will be denoted by the same word, "reputation." Significant differences are noticeable even with the example of user-driven centralized systems. Thus, decomposition and systematization are essential to streamline reputation interactions.

As we mentioned previously, we have used Samuel Smith's apparatus for decomposition. The proposed systematization is a set of reputes, reputees, and reputors models. Such models are helpful to describe any reputation system in a standardized way for further:

1. **Analysis** (including searching for scenario's flaws).
2. **Comparison** with other models.
3. **Composing** own scenarios in an optimal way.
4. **Implementation considerations**.

Repute Parameters

Verification. The basic repute parameter is **verifiability**. Verifiability is the possibility to reliably verify a repute's authenticity with the help of cryptographic proofs.

1. **Verifiable**. Verifiable reputes or verified credentials usually refers to decentralized systems as it requires a verifiable data registry to be registered. The advantage of such is trustless and transparent. In a decentralized environment, the trust is delegated to the consensus mechanism, which relies on cryptography and logic of the underlying protocol. This means that any peer is able to verify any authorization against an independent registry. That approach also serves for advanced data privacy as all the data is stored in the registry without relying on a third party. Verifiable events are also highlighted as open-loop systems.[244]

2. **Unverifiable.** Unverifiable reputes refer to centralized systems. Centralized systems imply trust to a third party that creates and stores all the reputational events, credentials, etc. In order to verify the authorization, any user must communicate back with the third party. As the centralized registry could be easily manipulated, there's no reliable way to verify the events. Unverifiable events are also highlighted as closed-loop systems.[245]

Tethering. Tethering is the reputation event's dependence on the qualitative characteristics of the Issuer, i.e., reputer.

1. **Tethered** repute is issued by a single unique issuer. In a sense, it's similar to an ancestral affiliation. An example of tethered repute is a university diploma.

2. **Non-tethered** reputes are not connected in any sense to any issuer. That also means that the repute could be issued by different entities.

244 Smith, S., 2021. Authentic Chained Data Containers (ACDC). [online] GitHub. [Accessed 11 August 2021].

245 Smith, S., 2021. Authentic Chained Data Containers (ACDC). [online] GitHub. [Accessed 11 August 2021].

Model Parameters

Measurability. Measurability is the ability to quantify the reputation event. A repute could be both quantitative and qualitative at the same time.

1. Repute is considered as **quantitative** if a quantitative estimation is possible. Examples are the number of tokens held or exams assessment.

2. Repute is considered **qualitative** if a quantitative estimation is senseless. A driver's license is an example of a qualitative credential.

Event anonymity. Event anonymity is the possibility of public disclosure of a repute's metadata. Event anonymity allows complex business logic across reputational systems, including common cases in medicine, finance, and other domains.

Full anonymity implies that the repute's metadata is not accessible by the broad public. At the same time, repute and reputer that corresponds to the given repute could be visible.

1. **Selective anonymity** implies that the repute's metadata is partly hidden or accessible to a strictly restricted list of peers. Such cases increase reputational systems' flexibility and provide higher levels of privacy for users.

2. **Public events** do not imply any hidden repute's details. All the information about public events is transparent and accessible to all network peers. Although public events do not hide any metadata, a corresponding repute or reputer could be private or pseudonymous.

Model Parameters

Connectivity. Connectivity is the connection between reputes.

1. **Linkable reputes** could be linked to others. Repute could be linked to other reputes. The connectivity, in that case, is just a link to some other repute or reputes that refers to some logical connection between the reputational events. Imagine a second-level certificate that is obtained only after a first-level certificate was obtained. That could be bachelor's and master's university diplomas or security access rights.

2. There could be standalone or **independent reputes.** Such reputes can not be linked to any other reputes. In that case, repute is an autonomous event that is often evaluated without a context of other events.

Uniqueness. The uniqueness of the event is the quality of a reputational event to be distinguishable among other events issued by the same or other issuers (i.e., reputers).

1. **Unique events** are distinguishable from any other event. The uniqueness could be achieved through explicit indication of the Issuer and/or recipient.

2. **Common events** are not distinguishable among other events. A common event still has a unique identifier and might have a unique issuer or recipient, but there's no logical difference between common events.

Reputee Parameters

Type. According to Smith's model,[246] reputee is a potentially pseudonymous but uniquely identifiable entity. Repute refers to the concept of DID. Anything can be the subject of a DID: person, group, organization, thing, or concept.

1. **Person** type refers to an individual human acting according to its own interest.

2. A **group** of individuals is a separate reputee type. A group might have its own subjective goals that could differ from the goals pursued by individuals of that group.

3. A type called a **thing** refers to any non-human agent.

4. A **concept** is a type of reputee that represents any data model, algorithm, theory, abstract entity, etc.

Reputee type is the only parameter that is represented by an open list of types. The discovery of all possible reputee types is restricted in time by technological progress and is beyond the scope of the current paper.

246 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021].

Model Parameters

Privacy. Reputee's privacy is the ability of a reputee to choose the level of its identity disclosure. Notice that a single real-world entity might have several DIDs and act on its behalf.

1. **Anonymous reputees** imply that the repute's recipient remains completely uncovered for all other peers. In contrast to pseudonymous reputee, there are no technical or mathematical means to reveal the reputee's identity.

2. **Pseudonymous reputee** remains uncovered due to its own unique identifier, e. g. DID. All the actions are made on behalf of a DID while the real entity remains unknown to other peers. However, there's no guarantee that there is some way to reveal the reputee's identity by comparing the behavior of a pseudonymous account and the corresponding real-world entity.

3. In the case of **real identity**, the identity of the repute is known to other network participants. Notice that once an anonymous or pseudonymous entity was revealed, it becomes public forever, and there's no way to bring the anonymity back to the reputee.

Reputer Parameters

Type. A reputer is the originator or primary source of the information items in a repute.[247] In comparison to reputee's type, the list of possible reputer's types is limited.

1. A **human individual (peer)** could be a reputer. A human is able to supply facts to a data registry, evaluate reputees and express its own opinion. In all that cases, a human generates reputes that could be stored in a data registry.

2. An **organization** that consists of a few individuals or computational agents is also able to generate reputes. An organization could act according to a fixed set of rules that, in that case, should be considered as the rules of the game. As the organization is presented by human individuals, the rules could be denoted explicitly or could be even irrational in relation to other reputees.

3. A reputer could be represented by a **non-human computational agent.** Smart-contract, mathematical algorithm, oracle, etc., could be considered as an independent computational agent. In that case, the set of rules that generates a certain event is usually fixed but could be hidden from other reputees or could be uninterpreted in relation to humans.

Privacy. Reputor's privacy is the ability of a reputor to choose the level of its identity disclosure. Reputor's privacy is symmetric and has the same attributes as reputee's privacy:

1.Anonymous. **2.Real identity.** **3.Pseudonymous.**

247 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021].

Delegation of authorization. Delegation of authorization is the ability of a reputer to delegate its rights to issue reputational events to some delegate. The delegation might have a few rounds. In each round, the delegator delegates its rights to a new delegate, so each subsequent delegation goes to a new delegate. The final delegate of the authorization then presents the authorization back to the delegator, which verifies the issuance and, upon successful verification, provides access to the service.[248]

1. **Chained attenuable** reputes allow the delegation described above with **attenuation.** Attenuation provides a practical trade-off between issuing many fine-grained fit-for-purpose authorizations and a few but too permissive general authorizations. A delegate who in turn chooses to become a delegator may issue a more limited fit-for-purpose delegation that is an attenuation of a more general authorization it holds. This limits the risk to the delegator of the attenuated delegation while providing the flexibility to delegate.[249] In practice, some rounds of delegation of authorizations could bypass a limited set of rights of the original reputer, and some rounds could bypass a full set of rights.

2. **Chained unattainable** reputers do allow delegation of authorization but do not allow attenuation. In that case, only the full set of rights is inherited by a delegator and could be bypassed to another delegator.

3. **Unchained reputers** do not allow the delegation of authority. In that case, attainability is senseless.

248 Smith, S., 2021. Authentic Chained Data Containers (ACDC). [online] GitHub. Authentic Chained Data Containers (ACDC). [Accessed 11 August 2021].

249 Smith, S., 2021. Authentic Chained Data Containers (ACDC). [online] GitHub. Authentic Chained Data Containers (ACDC). [Accessed 11 August 2021].

Repute-based Scoring Models and Their Drawbacks

As it's said above, the repute does not have semantics by itself. The repute represents some fact about a reputee that could be interpreted by a third party. In this paper, the role of evaluator and interpreter is assigned to scoring models. However, in some cases, the reputee may perform the role of interpreter due to the self-assessment procedure. In this case, the reputee evaluates his own qualities and presents the result of his scoring model to the Verifier.

A **scoring model** is a mathematical model or an algorithm that receives reputes as an input and outputs the assessment mark that could be considered as a reputational score. The reputational score could be used in a decision-making process or etc. The model could take all or a subset of reputes that belong to the reputee. Moreover, the model might require reputes that were issued by a given reputee to access the same reputee or even reputes that are not explicitly connected to the assessed reputee. Under the hood, the scoring model might be a simple heuristic (e.g., if a reputee has a GitHub account, the model considers the reputee as a developer) or a complex statistical model (e.g., neural net).

In each given case, a separate model could be used. For instance, when accessing Alice's ability to play the violin, the model could require the reputes corresponding to Alice's musical education or the opinion of other violin players about Alice, etc. At the same time, when accessing Alice's programming skills, another model should be used. In that case, the model might require all Alice's GitHub commits, programming school certificates, etc.

Additionally, multiple scoring models may target the same area. Digital trust benefits from an open market of scoring models as fair competition allows Verifiers to select the most accurate ones.

Model Parameters

Scoring models output a quantitative or qualitative assessment of a reputee. For instance, Alice's programming skills are assessed as 5 out of 10, and Alice was rated as a good violin player. The assessment could also be binary (e.g., a particular bank rated Alice as a trustworthy borrower).

The model might consider each repute as positive, negative, or neutral. Reputes that were considered as positive (negative) in most cases increase (decreases) overall reputation score assigned to a reputee. Neutral reputes could be ignored. Note that the same repute might have a positive impact on a reputational score using one model and a negative impact using another model at the same time.

A scoring model that takes several reputational events (reputes) in order to assess a reputee might consider each event as independent or consider some logical connectivity between the reputes, although there are no explicit links between the reputes.

A scoring model might aggregate the reputes (e.g., the model takes into account the total amount of funds received by a reputee). In other cases, raw unaggregated reputes could be used for further evaluation.

A scoring model might weigh all reputes and outputs the reputational score that is a mathematical (e.g., weighted) combination of the reputes. That approach is most relevant to mathematical and statistical models. In opposite, a scoring model might produce a final reputational score by comparing the number of reputes that were considered as positive and the number of reputes that were considered as negative by a simple voting.

Model Parameters

Some reputes could have an expiry date which could be captured by a scoring model as well. For instance, the model considers a reputee as a developer if that reputee made any GitHub commit last month. Early GitHub commits are not relevant for that particular model. Model's score (which is actually a VC like a repute) can also (and will, most likely) have a half-life period during which it is trusted and valid.[250]

The latter aspect we must cover is that decentralization is not a panacea, although it does solve many problems. Scoring models as final value generators potentially suffer from numerous attacks that can target almost any link in complex reputes flow infrastructure (see "Proposed architecture" section further). Tassos Dimitriou, in his "Decentralized reputation" paper, highlighted some of the essential ones:

1. **Sybil attacks.** The Sybil attack damages a reputation system by means of contributing to the system under multiple fake pseudonymous identities.

2. **Self-promotion** reflects a reputee's malicious attempts to unfairly increase his own reputation.

3. **Whitewashing** means attempts to remove bad reputation by re-entering the system with a new identity

4. **Denial of reputation** updates reflects attempts to abort a transaction when its negative impact on reputation is known beforehand.

5. **Out-of-range values.** Provision of out-of-range values to the systems in order to inflate the reputation of collaborators or simply create erroneous values.

6. **Denial of service.** Attackers cause a denial of service by preventing the calculation and dissemination of reputation values.[251]

250 Rea, A., Kronove, D., Fischer, A. and du Rose, J., 2020. COLONY Technical White Paper.. [online] Colony.io. [Accessed 15 August 2021]. p. 14-16

251 Tassos, D., 2021. Decentralized reputation. [online] Eprint.iacr.org. [Accessed 12 August 2021]. p. 4

Model Parameters

We assume this is not an exhaustive list. Nevertheless, many of them are to be prevented by competent identity management, while others will become non-trivial issues for scoring strategy developers.

As SSI provides strong identity layers for reputees, many of them are likely to hit the border area between centralized and decentralized systems in reputes flow. Others may affect decentralized systems based on subjective assessment (for instance, DAO-based voting). While it's impossible to govern all the reputes sources directly, the protection is also the task of scoring models by giving an appropriate evaluation to the least trusted reputes based on the risk assessment.

Reputational Scenario Examples

As mentioned above, any reputational interaction could be digested via the proposed model. As an example, we have chosen to examine two cases. The first case describes the WikiTrust reputation system for Wikipedia,[252] and the second case describes the Indian lending model of Joint Liability Groups.[253]

WikiTrust

WikiTrust is a reputation system for wiki authors and content. The main **system objectives** are:

1. Incentivize users to give lasting contributions.
2. Help users, and editors, increase the quality of the content and spot vandalism.
3. Offer content consumers a guide to the quality of the content.

To achieve these goals, WikiTrust employs two reputation systems: one for users and one for content. Users gain reputation when they make edits that are preserved by subsequent authors and lose reputation when their work is partially or wholly undone. The text starts with no reputation, and it gains reputation when it is revised by high-reputation authors; the text can lose reputation when disturbed by edits. [254] Although both systems are similar in many terms, only user reputation is considered in detail in the given paper.

252 Kulshreshtha, A. and Adler, B., 2010. Reputation Systems for Open Collaboration ∗ ABSTRACT. [online] Citeseerx.ist.psu.edu. [Accessed 11 August 2021].

253 Studymaterial.com, 2021. Types Of MFIs In India – Joint Liability Group (JLG), Rural Cooperatives, Self Help Group (SHG) – Objectives And Features. [online] [Accessed 11 August 2021].

254 Kulshreshtha, A. and Adler, B., 2010. Reputation Systems for Open Collaboration ∗ ABSTRACT. [online] Citeseerx.ist.psu.edu. [Accessed 11 August 2021].

Reputational Scenario Examples

Text edit by a user is considered a **repute.** WikiTrust scenario implies:

1. **Unverifiable reputes**. As all the events are stored and processed on Wikipedia's servers, there's no reliable in terms of decentralized systems way to verify the events. Although Wikipedia might expose the history of all edits, the users' credentials are stored on the servers. That makes it theoretically possible for Wikipedia to manipulate the system and the reputation of a particular user or text.

2. **Tethered reputes**. Text edit is made over a particular text by a particular user. The events are considered as tethered as each event is tethered to the user and to the text.

3. **Qualitative reputes**. As a text edit is a qualitative event, the repute should be considered qualitative. In terms of the proposed model, quantitative repute's assessment is done by a scoring algorithm, i.e., WikiTrust system.

4. **No anonymity for reputes**. As mentioned above, all the events are stored on centralized servers. There's no event anonymity.

5. **Linkable reputes**. In order to assess a single repute, the WikiTrust engine compares it with other reputes (text edits).So the reputes should be considered as linkable because a particular text edit follows previous text edit and is followed by future text edits (in fact, it's linked to a few reputes and is followed by a few reputes).

6. **Unique reputes**. Each repute is unique as a certain user makes a certain edit in the text at a certain time.

Reputational Scenario Examples

The user that makes a text edit should be considered as a **reputee** as the user's reputation will be assessed. The scenario implies:

1. **Reputee is a human**. The user that makes text edits is a human owning some knowledge. Text edits are made due to that knowledge.

2. **Reputees are pseudonymous**. Reputee (i.e., a user) should be registered on Wikipedia in order to make changes. There are no KYC procedures when registering on Wikipedia, so users are pseudonyms.

Users' text edits are scored by a Wikitrust engine that serves as a **reputor**. The scenario implies:

1. **Reputer is a non-human computational agent**. Wikitrust engine is an algorithm that assesses text edits made by reputees.

2. **Reputer is a real identity**. The code of the algorithms is open-sourced.[255] As the history of all edits could be exposed, anybody can run the algorithm on top of it.

3. **Delegation of authorization is not possible**. The WikiTrust engine is the only entity that is allowed to assess users.

255 Kulshreshtha, A. and Adler, B., 2010. Reputation Systems for Open Collaboration ∗ ABSTRACT. [online] Citeseerx.ist.psu.edu. [Accessed 11 August 2021].

JLG Lending Model

The interest in alternative lending is growing. Loan history, as the primary criteria for generating traditional credit scores, is either incomplete or unavailable for a significant part of the population. This is especially true in developing countries, where many people not only face a lack of sufficient funds but also do not have the documents necessary to open a bank account and official work.[256]

For such people, the concept of Joint Liability Groups (JLGs) was proposed in India. A JLF is a homogeneous social group of 4-10 people of the same tribe or locality with the same socioeconomic background who mutually come together to form a group for the purpose of availing a loan from a bank without any collateral. All the members of a JLG are responsible for repaying the loan amount.[257]

The lending organization (i.e., a bank) makes loans to JLG members. The bank internally scores JLG members in order to filter out non-creditworthy clients. The scoring depends not only on JLG member's reputation but on the collective reputation of the whole JLG. That case becomes sufficient because each member of a JLG (i.e., a tribe) is responsible for other members' reputation, so each member is responsible not only to a bank but to other tribe members as well.

The concept could be considered as a simple DAO. Tribe members are the participants of the DAO who are interested in the best possible reputation of the tribe, i.e., their DAO. The whole system incentivizes DAO participants to behave in a way not only to increase their own reputation but to increase DAO's reputation as well.

256 Ifc.org. 2018. For Women in India, Small Loans Have a Big Impact. [online] [Accessed 11 August 2021].

257 Studymaterial.com, 2021. Types Of MFIs In India – Joint Liability Group (JLG), Rural Cooperatives, Self Help Group (SHG) – Objectives And Features. [online] [Accessed 11 August 2021].

Reputational Scenario Examples

Any tribe member's real-world action is considered a **repute**. Reputes affect both tribe's and reputee's reputation.

1. **Verifiable reputes.** As the repute is committed on behalf of a real entity that is known by the tribe, each repute could be verified. Though the decentralized ecosystem is not presented by a distributed ledger technology, the repute remains verifiable as all the reputee's actions are basically actions in the real world that are seen by other peers.

2. **Tethered reputes**. The repute is anchored to a specific tribe and a chosen member of that tribe.

3. **Both quantitative and qualitative reputes.** Reputes are considered as both quantitative and qualitative as there could be different repute types. Loan payback is definitely a quantitative parameter, while some reputee's real-world actions could have a quantitative measure. E.g., making your business prosper probably increases the reputation of a reputee across the tribe.

4. **Selective anonymity**. Some repute's parameters could be partly hidden from the other tribe members, which depends on a tribe setup. E.g., if a reputee makes a loan payment, the exact sum of the payment might be unknown to other tribe members.

5. **Independent reputes.** Each repute is logically independent of other reputes and should not be linked to other reputes in that case. Each repute impacts the overall reputation score, but reputes do not depend or rely on any other reputes.

6. **Common reputes.** The repute's uniqueness should be considered as common because there's no anything unique in a specific repute. All the reputes are similar in a logical sense though a single repute has its own unique characteristics.

Reputational Scenario Examples

The member of a tribe is considered as a **reputee** in the scenario, which implies:

1. **Reputee is a human**. The reputee is a human that owes money from a financial organization.

2. No **reputee's privacy**. As the reputee is a tribe's member, the repute is publicly known. Reputee also should pass KYC procedures in the financial credit organization, which does not correspond to a private reputee.

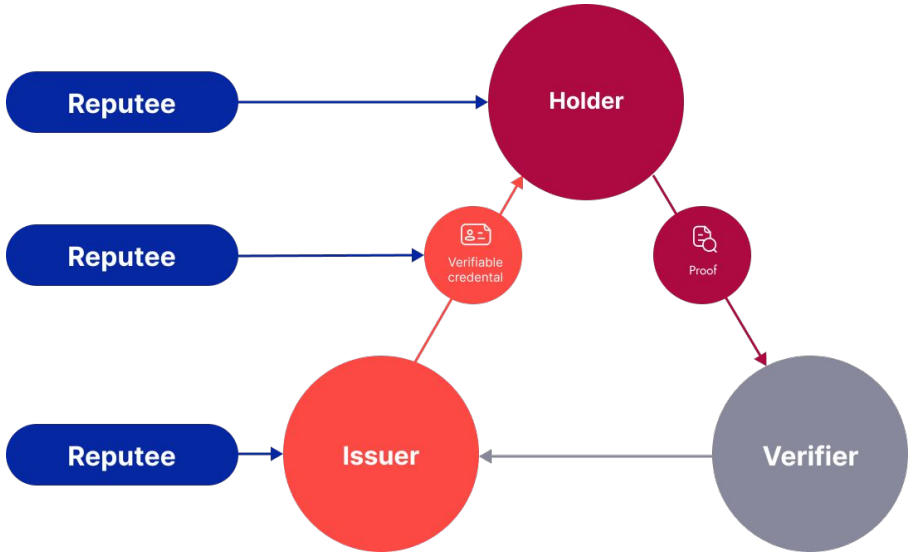
In a given scenario, the financial credit organization is a **reputor.** Reputers decide about reputees creditworthiness and make loans to them. The scenario implies:

1. **Reputor is an organization.** The financial credit organization scores the reputees and decides about the reputee's creditworthiness.

2. **Reputer is a real identity with no privacy.** As the financial credit organization is known by a reputee and a tribe there's the reputes are publicly known.

3. **Delegation of authorization is not possible**. The financial credit organization is the only entity that is allowed to assess reputees. However, the organizations might have brunch offices that are still the same entity.

SSI Stack for Implementation of the Concept of Decentralized Reputation



While reputes, reputees, and reputors constitute an abstract model suitable for analysis and conceptualization, there must be some kind of framework for practical implementations.

When Samuel Smith published his Open Reputation whitepaper, the work on SSI was still mainly at the stage of theoretical comprehension. In particular, there were still no decentralized identifiers that have changed a lot in this domain.

Proposed Architecture

If we overlay the SSI concept on the reputer-repute-reputee triad, finally we have the following picture:

1. **Reputes.** In the proposed architecture, reputes are presented in the form of VCs. We can think of VCs as secure tamper-proof data containers[257] that enable the secure transmission of reputational data. A typical repute must contain the primary information items to provide provenance of the repute.[258] This may include the identification of the repute, timestamping data as well as linking data to related reputee and reputer.his is exactly what the basic VC properties marked as imperative in the W3C standard do.

   The requirements for a repute serialization format, designated by Samuel Smith, are the following characteristics — flexible, nested, hierarchical, ubiquitous, simple, and human-readable — in the aggregate, and the JSON-LD format matches all of them, adding the power of semantic data to reputes.[259]

2. **Reputers**. As Issuers are the sources of verifiable claims, they are reputers in this system. In the case when the reputor and reputee coincide in one person, VCs will be self-issued.

3. **Reputees.** The Holder is a reputee who accumulates all the reputes with him as a subject. SSI allows the Holder to be the real owner of portable reputational events.

   Verifiers are not included in this triad. The role of the final reputable data consumers in this scheme will be described further.

257 Smith, S., 2021. Authentic Chained Data Containers (ACDC). [online] GitHub. [Accessed 11 August 2021]. p. 2,5, 7, 8.

258 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 32-33

259 Smith, S., 2015. Open Reputation Framework. [online] GitHub. [Accessed 11 August 2021]. p. 13-14.

General System Architecture

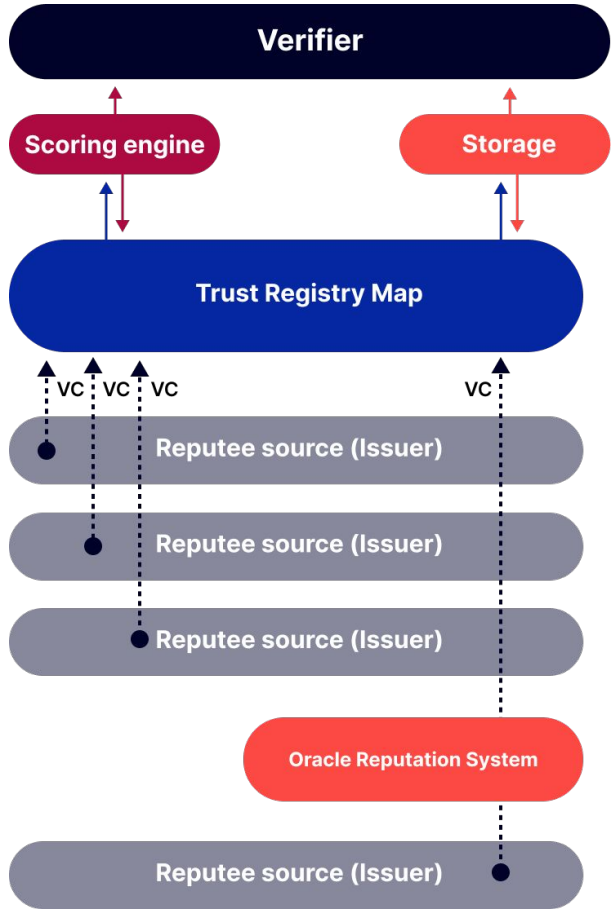
260 Smith, S., 2021. Authentic Chained Data Containers (ACDC). [online] GitHub. [Accessed 11 August 2021]. p.2 ,5, 7, 8.

Here is the general scheme of the SSI-based reputation system. We will describe the system along the reputes data path:

1. As we noted previously, reputes initially come from various Issuers of VCs. While VCs ensure only the data authenticity and not the data accuracy anyway,[260] their content part can contain absolutely any, even really corrupt information. That is why, in some cases, **the intermediaries** who will incentivize Issuers to provide truthful information and delineate untrusted sources of reputes are needed, especially in the cases when reputes are formed on the ground of off-chain online events from Web 2.0 platforms ("Oracle Reputation System" in our scheme).

2. **Trust Registry** is the following step in the data flow. Not only it allows to find the trusted counterparties for all the interested persons, but it also ensures that proper governance and technical standards cover the whole process.

Interoperability between the primary stakeholders of the Trust Triangle, which is essential within a comprehensive decentralized reputation, is a significant issue currently. Numerous separate trust ecosystems with their own Issuers and Verifiers present on the market. The number of non-equal governance models, trust frameworks, and regulatory systems is also not going to stop growing. Trust registry, being a cross-functional mapping component in our scheme, provides a bonding layer for end-users, giving the tools for the discovery of issuing rules, Issuers, and Verifiers, credential types, as well as user-friendly VC-management instruments.

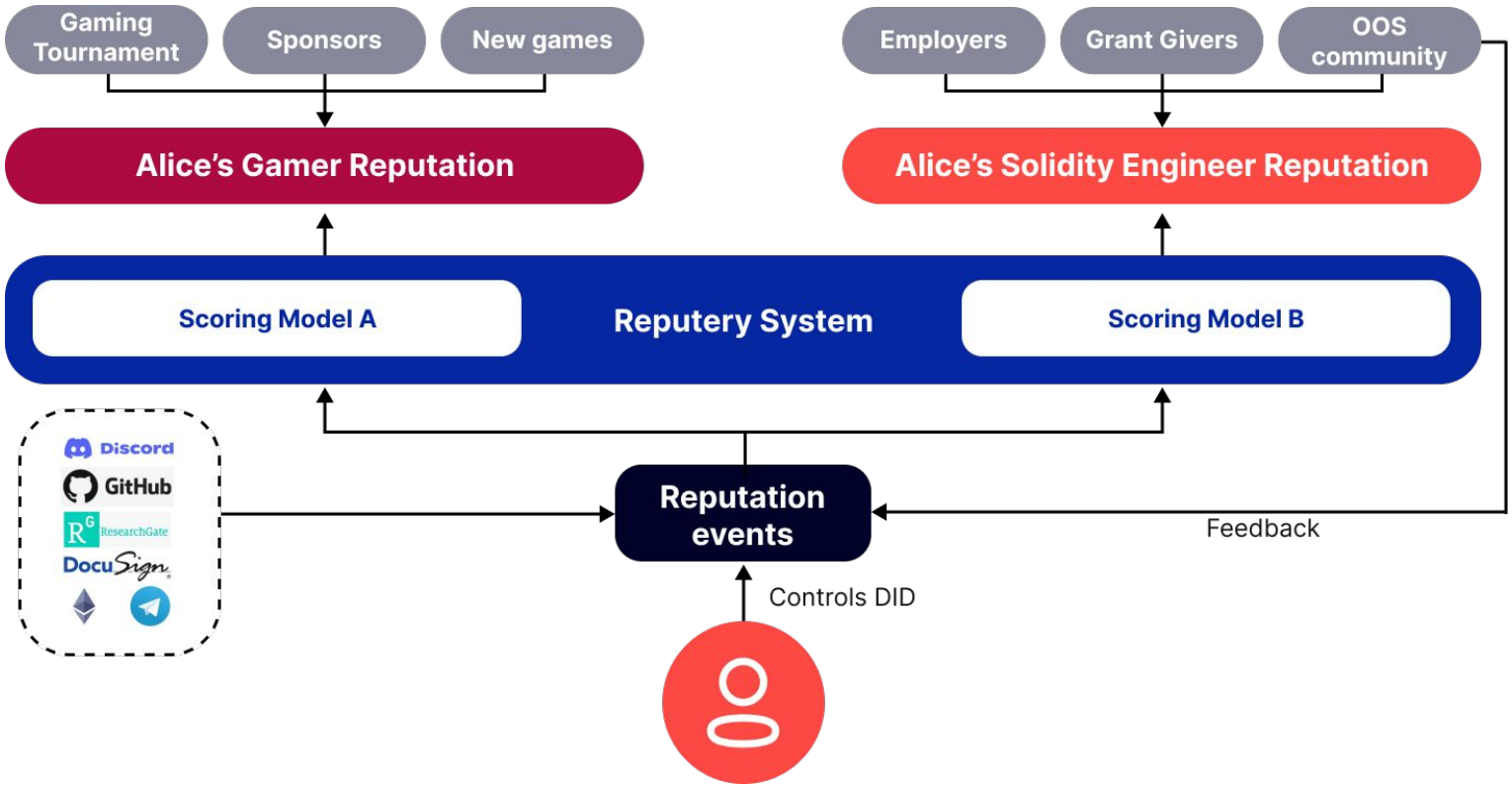


3. Then reputes can be shared with Verifiers directly (then this is just an ordinary VC exchange process), but a more promising approach is the use of independent intermediaries — **scoring engines** — generating the final domain-specific reputation scores based on the set of VCs from different origins.

Decentralized storage is a necessary module that acts as a trustworthy (i.e., independent from any trusted third-party) place where contextual data can be stored. First of all, VCs are not quite a suitable place for storing media and other heavy data. Instead, the JSON-LD format allows you to reference external resources. However, the involvement of a centralized resource, even in this aspect, can undermine the credibility of the repute at all, so that trusted storage is needed here. It should also be marked that any centralized thing is not permanent, while decentralized storage will provide data persistence. Hashing mechanism will ensure the verifiable authenticity of the data.

Use Cases

SSI-based decentralized reputation opens a huge number of use cases because of its portable nature and the ability to provide domain-specific reputational scores depending on the need. A common top-level concept demonstrating those aspects is shown in the scheme below.



Portable Reputation

The beauty of sovereign identity technology is that it enables users to become real owners of their data, no longer dependent on centralized platforms. Identity data portability was laid down as one of the initial principles of SSI, and all this became possible with the advent of DIDs and VCs.[261]

This feature is extremely important in the case of a digital reputation. Nothing is permanent on the Internet: even if it is a super reliable service from Google with multiple reservations, the world is too fickle to hope for. SSI shifts responsibility for the safety of data to the user. Being an additional responsibility in itself with no doubt, in general, this is seen as a blessing that gives new opportunities.

So what does a portable reputation give us, where all reputation events are VCs owned by the user? Decentralized reputation becomes cross-chain and cross-application. A collective reputation is easily imported into the individual one, while the latter opens up a huge range of use cases, which we will talk about further.

261 Preukschat, A. and Reed, D., 2021. Self-Sovereign Identity Decentralized digital identity and verifiable credentials. 1st ed. Manning Publications. p. 423

Reputation Score by Domain

Throughout his life, a person is permanently involved in various offline and online activities. As a result, it accumulates thousands of reputation events. What if we engage them to confirm the qualifications and skills of the user in a certain domain? Actually, it opens up great opportunities in the world where at the current stage, such a means of confirmation is academic diplomas, which do not always show the real level of competence. Without going deeply into the problems of modern education, we just note that, in addition, in the context of globalization and cross-border ties, residents of countries with diplomas from unauthorized universities remain overboard.

SSI allows you to aggravate all your reputational events into lifelong domain-specific reputations. Assume one is a software engineer. At the start, he most likely has a diploma, which he received as a result of offline education in the form of a VC. Then his reputation is formed through multiple activities: open source contributions, online courses, employment, participation in hackathons and challenges, etc. All this is more informative and reliable for a Verifier (for example, for a potential employer) than just a diploma.

There are many use cases for such a reputation outside the scope of professional qualifications. Investors can aggregate information about their experience on trading platforms and show additional qualifications for accessing high-risk assets instead of just passing[262] formal tests. Gamers can collect together all their gaming achievements plus their rating in gaming communities and receive additional bonuses. A driver provides all his driver's licenses. Confirms exemplary behavior without violations on the road (using ZKP, of course), as well as participation in the gas stations' loyalty programs, and receives a discount on travel on the toll road.

262 Hickey, S., 2021. FCA mulls online test for high risk investments. [online] Ftadviser.com. [Accessed 11 August 2021].

Use Cases

When reputes are collected, then scoring engines come into play. There may be many of them, but competition will determine the best and the most trustworthy. Decentralization opportunities (smart contracts and DAOs) and open source software will help here. Finally, the user is happy that all his activities now have added value and open new opportunities, while Verifiers enjoy trustworthy reputation scores provided by independent (e.g., DAO-based) scoring engines.

Meritocratic Voting

DAOs seem one of the most promising advances in blockchain technology and Web3. Theoretically, there is a huge potential behind them, although now the technology is still at an early stage, the stage of research and experimentation.

Originally, decisions in DAOs are governed by proposals and voting to ensure everyone in the organization has a voice.[263] We assume that this approach is far from ideal, especially if there are no additional mechanisms. Here are the core **issues with voting** if to speak generally:

1. Voters are not incentivized to vote at all.

2. Voters would not have to spend significant time analyzing the context.

3. Voters could be the subjects of malicious influence.[264]

The inefficiency of simple voting will ultimately lead DAOs to either implement hierarchical, centralized governance structures from the traditional world or seek other solutions. For instance, Ralph C. Merkle, in his "DAOs, Democracy and Governance" paper, proposed to use prediction markets as the core mechanism for making the key decisions.

Reputation is another solution preventing a DAO from turning into an authoritarian governance structure. Limited access to governance mechanisms (such as voting) based on fair and transparent reputation scores allows making meritocratic decisions, while SSI takes care not to violate the nature of DAOs with complete de-anonymizing of its members.

263 ethereum.org. 2021. Decentralized autonomous organisations (DAOs) | ethereum.org. [online] [Accessed 11 August 2021].

264 Merkle, R., 2021. DAOs, Democracy and Governance. [online] Merkle.com. [Accessed 11 August 2021]. p 4-5.

DeFi Credit Score

Blockchain technology opened up radically new opportunities in fintech. With blockchain as the root of trust, borrowers and lenders can conclude a loan agreement without the need for intermediates, which are typically banks. Automatically executing smart contracts frame the conditions of the deal instead of paper agreements.

But how to ensure human trust in peer-to-peer relations where parties are hidden behind pseudonyms at best? Actually, in the world of centralized finance, credit scores are used as the metrics of creditworthiness. Typically it's affected by the such factors as payment history, credit utilization ratio, length of credit history, credit mix (different types of credit utilized).[265] [266]

Hardly can we name them suitable for DeFI loans. Reputation may be the alternative again. Basically, not only financial metrics can show the level of a person's financial decency. Almost any good collective reputation can indicate your diligence and integrity. Staking/slashing may prevent the collective members from groundless score boosting.

An individual reputation can also say a lot. For instance, it can be informative to the lender that you always pay your rent payments on time.

265 Heming, T., 2021. WHAT AFFECTS YOUR CREDIT SCORE? Understand what causes your credit score to change. [online] Moneysupermarket.com. [Accessed 11 August 2021].

266 O'Shea, B., 2020. What Factors Affect Your Credit Scores? — NerdWallet. [online] NerdWallet. [Accessed 11 August 2021].

Hiring / Grant Giving Assessment

Provable professional reputation accumulating over the course of an individual's life may be more revealing to an employer than a job interview — especially given the general trend of moving work to the digital space.

Your professional reputation consists of a huge number of activities: employment records, badges, contributions, which reflect your competence in a certain area. All this allows the Verifier to at least make sure of your hard skills, thereby even eliminating the need for technical interviews in some cases. The same evaluation of your professional qualities and skills can serve as an objective criterion for assessing before giving a grant.

Community Rewards

Fair distribution of rewards in proportion to contribution is a rather old problem. The core idea of using reputation here is that reputation allows one to determine and evaluate the contribution of each party to a certain collective work ex post facto. For instance, if we talk about open-source projects, all your commits, open and resolved issues, pull requests, and other contributions for a given period of time reflect your usefulness for the project (which is your collective reputation for a given project). Ultimately, project participants are rewarded in proportion to their reputations.

Another big area for such a reward model is DAOs. Over time, when DAOs, as a new way of cooperation, begin to supplant traditional forms, for example, legal entities, they will cease to be just static collectives and begin to really frame human activity, the reputation of DAO members will become the core of selection mechanisms. This also applies to the rewarding of active members.

Spam Resistance

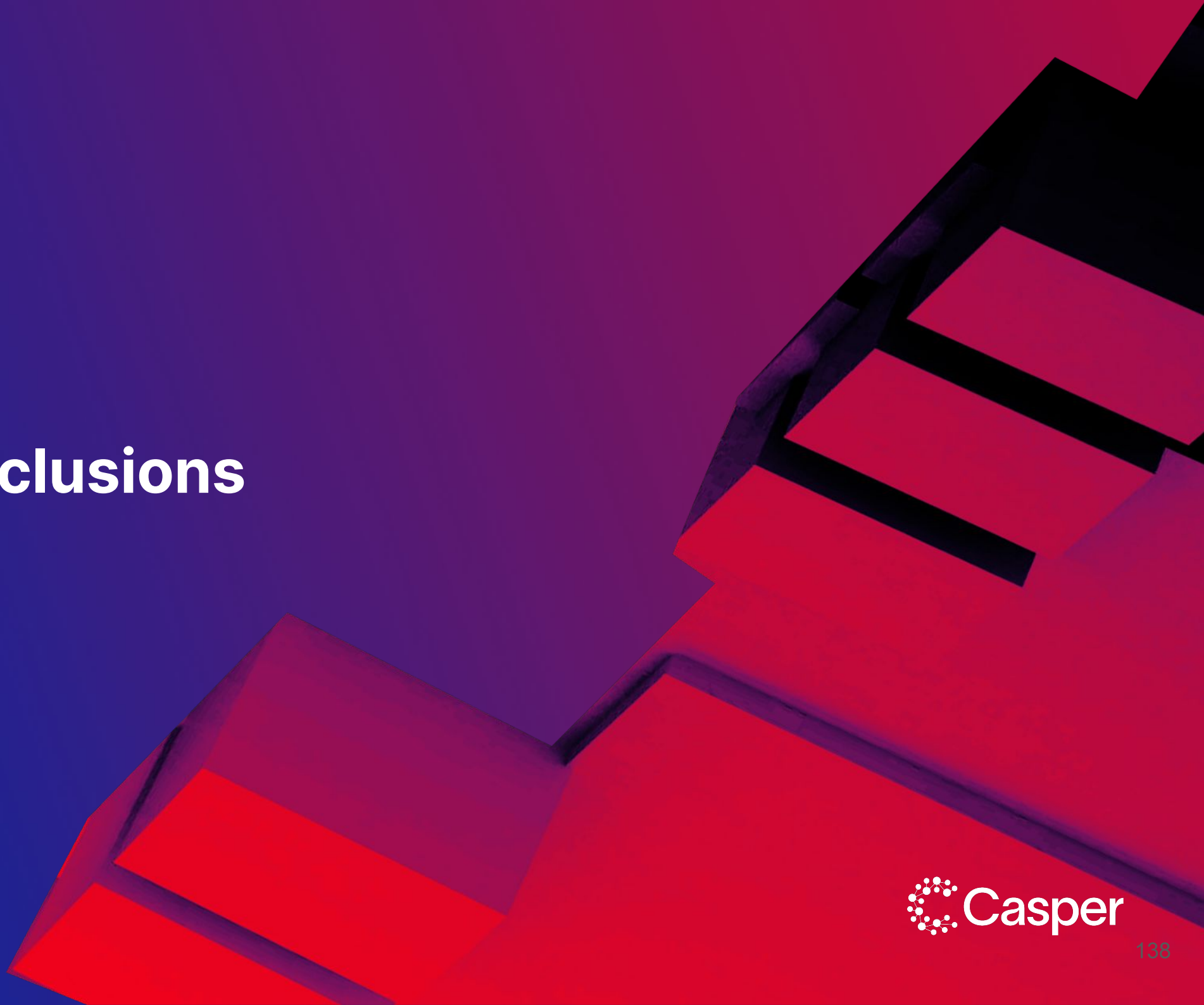
The problem of bots has become a real pain point for the Internet. According to various estimates, more than 50 percent of all traffic currently comes from automated programs known as bots.[267] There is no doubt that a significant number of them are aimed at malicious activities.

There is no doubt that in a decentralized web that will give the Internet back a little more anonymity and respect for privacy, the problem will be no less significant. The requirement for reputation disclosure before processing can become one of the tools to combat the issue. An Individual's reputation may constitute the likelihood that this is really a living person and not a bot. The sufficient value of this likelihood is determined by a specific use case. For less serious ones, just the user's activity on social profiles is suitable for cases requiring a high probability. More advanced cases requiring a higher probability may require more serious disclosure. For example, reputation based on transaction history can come in handy.

So, the seriousness of identity proofs vary from, obviously, less reliable (like connecting your Facebook profile to the service) to those that with almost 100% probability ascertain the existence of a person before you (like a video interviewing). SSI and reputation together allow not to go to these extremes and provide "I'm not a robot" proofs sufficient depending on the case instead.

267 Zilles, C., 2020. The Internet is Mostly Bots, and That Is a Problem. [online] Social Media HQ. [Accessed 11 August 2021].

Conclusions



Casper

Conclusions

The origins of the Internet identity can be traced back about 20 years.

In **Chapter 1**, we provide a brief historical overview of digital identity developments, including the evolution of digital identity models from anonymity to centralized, federated, and back to a more decentralized model with the development of blockchain technologies, among many other developments — SSI.

In **Chapter 2**, we join and share the vision of the fast growing community of SSI advocates, enthusiasts, and practitioners, as well as walk the reader through Christopher Allen's main concepts of SSI. The SSI vision is described, as well as its benefits to many sectors. This includes both the public and private sectors, but most importantly, what it means for individuals in terms of privacy and by putting users at the center of their data, thus safeguarding and promoting human rights.

Chapter 3 focuses on decomposition of the SSI stack into its primary building blocks. The concept of Trust Triangle as the relationship model of the parties in digital trust ecosystems is highlighted. Non-custodial self-sovereign identifiers — DIDs — covered in this chapter with VCs as portable authentic data containers allow users to become the real owners of their data on the Internet.

Chapter 4 outlines the landscape of governance methods for different layers of the SSI stack. There is no doubt that decentralized systems require even more governance than centralized ones based primarily on administrative methods. We assume that governance methods of different levels of decentralization will co-exist in the ecosystem.

Conclusions

In **Chapter 5** we marked the benefits of SSI implementation for a Casper blockchain. SSI provides a chain-independent value transfer layer that prevents lock-in effects and results in growth in the number of use-cases and transactions. All this ultimately increases the network's utility, as well as the utility of the SSI ecosystem as a whole. The primary architectural blocks for Casper Network are highlighted.

In **Chapter 6** we analyzed the current legal field surrounding digital identity, its components, like electronic signatures, with a brief overview of the current privacy and data protection laws, and we have seen that despite not having an SSI-specific regulation, based on its architecture the concept fits in many current legal developments in the field of identity, data privacy and basic human rights law too simply because it is based upon them.

In **Chapter 7**, we provide the reader an illustration of the recently presented solutions and the usage of SSI in the digital world and everyday reality.

In **Chapter 8** the concept of SSI-based decentralized reputation was presented and substantiated. While reputation is one of the primary social regulators, in the digital world reputational systems face trust, fragmentation and scaling issues. Additionally, individual reputation does not (and, probably., could hardly) exist in Web 2.0.

The term reputation has a context-sensitive meaning. As multiple completely different reputational interactions may exist, we resort to reputation decomposition and systematisation using Samuel Smith’s terminological apparatus of reputes, reputees and reputors. Being parameterized, these elements allow to compose models of reputational systems in a standardized way for further analysis, comparison and hypothesis testing.

Conclusions

The emergence of blockchain technologies and SSI allowed a different look at the digital reputation. SSI enables to build a layer of trustworthy reputation over the Internet, portable and persistent, cross-chain and cross-domain. Samuel Smith's three-link model perfectly fits the concept of Trust Triangle, where VCs serve as portable tamper-evident containers for reputational data (reputes), while Issuers and Holders correspond to reputers and reputees accordingly. Verifiers as final value consumers enjoy fair reputational scores and involvement of qualified leads.

Persistent and portable pseudonymous decentralized reputation is an especially important missing link in the context of continuous growth of the decentralized economy to provide effective and trustworthy coordination beyond just financial cases.