Self-Sovereign Identity Framework for freeTON Network

2021

Stepan Gershuni

gershuni.stepan@gmail.com

https://sgershuni.medium.com/

Introduction

There has been recent progress in decentralized identity development and adoption by community and major companies. There are recent studies such as the recommendation by the world wide web consortium for DID that prove the relevance and importance of DID in the future of the Internet and decentralization. DID allows individuals to prove their identity in centralized and decentralized applications and disclose only required personal information. That is crucial for future blockchain applications due to the fact that problems of identity theft and custody of digital assets are not yet fully solved in a decentralized manner in most blockchains. Blockchain protocols are heading from resource consuming PoW algorithms to PoS and PoA algorithms that add extra importance to the need of managing identity securely. For permissioned blockchains having the ability to generate, revoke keys and restore access to identity becomes important due to the fact that these authorities ensure integrity of the network. PoS blockchains also require functions of taking control of private keys because of slashing algorithms for misbehaving that can occur in case of identity theft. Individuals that are willing to invest in crypto are concerned with security issues that they face in both DeFi applications and centralized exchanges.

Despite recent progress in decentralized identity there is still room for improvement in terms of not only storing and proving identity but also using DID to take custody over digital assets. DLT protocols have to consider implementing decentralized identity and it creates an opportunity to improve transparency and security for individuals that would give a competitive advantage. Casper is on the leading edge of BFT development with flexible finality that especially relies on proper behaviour of participants that can be ensured using decentralized proof of identity of the network participants.

There has been recent progress in decentralized identity development and adoption by community and major companies. There are recent studies such as the recommendation by the world wide web consortium for DID that prove the relevance and importance of DID in the future of the Internet and decentralization. DID allows individuals to prove their identity in centralized and

decentralized applications and disclose only required personal information. That is crucial for future blockchain applications due to the fact that problems of identity theft and custody of digital assets are not yet fully solved in a decentralized manner in most blockchains. Blockchain protocols are heading from resource consuming PoW algorithms to PoS and PoA algorithms that add extra importance to the need of managing identity securely. For permissioned blockchains having the ability to generate, revoke keys and restore access to identity becomes important due to the fact that these authorities ensure integrity of the network. PoS blockchains also require functions of taking control of private keys because of slashing algorithms for misbehaving that can occur in case of identity theft. Individuals that are willing to invest in crypto are concerned with security issues that they face in both DeFi applications and centralized exchanges.

Despite recent progress in decentralized identity there is still room for improvement in terms of not only storing and proving identity but also using DID to take custody over digital assets. DLT protocols have to consider implementing decentralized identity and it creates an opportunity to improve transparency and security for individuals that would give a competitive advantage. Casper is on the leading edge of BFT development with flexible finality that especially relies on proper behaviour of participants that can be ensured using decentralized proof of identity of the network participants.

The Need for SSI framework

The Internet is one of the most important innovations in human history. It reimagined virtually every industry in the world: from communications and payments to transportation and education. To achieve that, it grew from a few thousands to billions of users in a span of two decades, and precisely due to this unimaginably rapid growth rate, the internet companies were forced to make quite hard compromises. Namely, they've been forced to consistently choose UX over privacy, simplicity of the business model over user sovereignty, high growth over long-term sustainability and "build fast, break things" over "build for the decades" approach.

This has proven to be the right decision at the time and in the given circumstances. However, as the Web matures and data is becoming more valuable than physical resources for so many of us, we're faced with the challenge of figuring out a truly decentralized system where the interests of a small number of corporations are aligned with our own.

The Internet, as pretty much any human invention, is not at its final stage. We can do much better. **The goal of this paper is to propose the path for the SSI framework and its implementation on top of the freeTON network**. In order to do that we will cover four key topics:

1. Identify existing problems

2. Offer technical solutions and building blocks for the Decentralized Web and highlight where does SSI fit it

3. Review business models of the decentralized services that are aligning value maximization with the goals of long-term sustainability, user convenience and sovereignty

4. Describe potential decentralized applications and provide reasons why they achieve superior economic efficiency over existing platforms.

Problems Overview

To begin with, we will look at the high-level components of the Web that result in billions of dollars in losses for Internet companies as well as their customers. None of these problems were consciously introduced by some malicious actor; rather they arose from a series of one-way decisions made in an attempt to solve pressing problems and figure out sustainable business models by the internet companies.

Data Storage

With almost 5 billion internet users there's over 40 zettabytes of information stored online. However, the majority of sensitive personally identifying

information (PII) is not directly controlled by the users. Instead, it's service providers, internet corporations and online businesses that custodially store, manage, aggregate, analyze and resell our personal information. Digital data storage services can take many forms: storage-as-a-service, like Google Drive or Dropbox; consumer data storage that e-commerce and social media platforms have to maintain in order to provide quality service and personalization; government data registries; location and search history maintained by search engines, telecom providers and mobile operating systems.

What is common across all of these cases is that data access is maintained by 3rd parties. And precisely due to this reason only those 3rd parties are responsible for security and privacy of our information. As a user you become more and more dependent on the service provider: if they are hacked, you lose all your data and might not even be notified about the incident; if their service is down, you lose an ability to access your information. Natural profit maximization optimization leads to the business models based on reselling customer data that forces companies to collect sensitive information about their users.

The attempt was made to introduce data protection regulation in the form of GDPR, CCPA and similar legislation. However, this does not solve the underlying business problem and, most importantly, not even always possible to fully adhere to. When signing up with a new web service users are greeted with "all or nothing" Terms of Service: you either agree with everything or don't use the service at all. There is no granularity or real control — just an imitation of compliance with the current regulation.

As a result, we end up with a situation where internet companies are liable for data breaches, forced to provide at least some degree of control over PII to their customers, yet have very little business incentives or technical capabilities to change the status quo.

One of the major reasons for such systems to evolve was utilization of switching costs competitive advantage by internet companies. Once you have a large amount of data stored with the particular provider you expect some value loss that would be incurred from switching to an alternative solution.

Identity Lock-in

When proving or creating a new digital identity we're usually faced with a few options: sign in with Google, sign in with Facebook, sign in with an e-Government account or sign in with login and password. Even in the last case it's still the identity service that is actually responsible for authorization and granting us access. What's missing is "Sign in as Yourself".

No matter what authorization method from above you choose, you can be censored and locked out single-handedly by the platform operator. Moreover, if Facebook or Twitter for whatever reason decides to ban your account, you're also losing access to any other service that you were signed up to using their single sign-on feature.

Second issue is that such an approach, no matter how privacy-preserving those companies claim to be, will inevitably provide grounds for surveillance. One can't be using 3rd party service as an identity provider without metadata and activity traces being recorded. User privacy in such systems is compromised by design and we, as users, are deprived from ability to set up granular permissions and desired level of anonymity. Moreover, identity is almost always strongly coupled with the data storage systems described above.

Data Portability

Digital platforms are heavily utilizing network effects, a strategic advantage where the value realized by the user increases with more users on the platform. Precisely due to this reason and not technical barriers those same platforms limit their users in ability to transfer data in and out of the platform. Let's take an example of reputation: you might spend years building a reputation in an online community, seller reputation on eBay, social media followership, taxi driver or passenger rating on Uber. Yet there is no way for you to transfer or re-use these attributes elsewhere, even though they actually describe your identity and nothing else.

Centralized computation

Computation results coming from a centralized system can't be trusted by multiple mutually suspicious parties. This becomes increasingly problematic in sensitive areas like finance, health care or B2B transactions. To give a few examples, we're not able to fully trust an exchange or gambling website to not manipulate computation results. Obviously there are compliance standards but what's missing is a way to directly prove that algorithms are honest and auditable. Centralized systems also exhibit a higher risk of systemic failure in comparison to distributed ones.

Information Gatekeeping

More than half of social media users call these platforms as their primary source of news. The stronger the network effects of centralized information providers, the more gatekeeping behavior they exhibit. In some cases it may be direct censorship in the form of a website banning one of their prominent users. In other cases censorship can be indirect and not even explicit: curation algorithms optimize towards engagement and advertising revenue and such optimization in turn leads to unintentional curation bias. And finally the platform might decide to abuse their curation and recommendation power to steer public opinion.

Another problem arises from the ability of centralized platforms to track their users. In repressive regimes this will mean that ISPs, social media sites and communication platforms are forced to limit or block access for specific citizens. It might even result in de-anonymization and – bloggers can be arrested or killed, and political opponents can be monitored.

Manual governance

Technological progress is synonymous with an increase in automation. However, we still heavily rely on manual and slow governance and bureaucratic processes that mostly consist of pretty simple actions, such as verification of authenticity, rule-following and compliance. This process not only costs trillions of dollars per year to the global economy, but also provides a potential for bias, corruption and random mistakes. Moreover, those systems are already seriously automated — it's not just a person but a software operated by a person that makes a lot of

administrative decisions. By replacing the middlemen that tend to manipulate and extract personal gain from the system with middlemachines which have no personal interest we're able to achieve higher level of trust in the governance system, increase transparency and auditability, reduce bias and discrimination. This is true for federal governments or international committees but also on a very practical level of corporate compliance, municipal governance, online community management or document processing at your local notary public office.

Building Blocks of the Self-Sovereign Identity and the Decentralized Internet

The system is as decentralized as its most centralized component. If we want to solve the problems outlined above in a sustainable way we need to keep a few things in mind:

1. The solution should be a decentralized stack, not just one single component. Otherwise, manipulation and censorship opportunities just shift up or downstream.

2. The solution should have a clear and scalable business model for the developers and entrepreneurs. Otherwise, market forces won't let it get enough adoption.

3. It should provide comparable or superior user experience.

Uncensorable Money

Cryptocurrency is the most mature technology of this whole stack, even though the idea itself is less than 30 years old and Bitcoin just hit its 12th anniversary. However, what is important for the decentralized web stack is not just a trustless monetary system but also ability to enable privacy-preserving payments, decentralized financial markets and funding mechanisms. The need for the decentralized monetary and financial system is not political, although that can be the reason for Bitcoin adoption. But for the purposes of our research we view

these components as means to enable the new decentralized web business models. We will examine each of those solutions separately.

1. Bitcoin is a native internet currency with no central authority or financial institution that controls it. Bitcoin is not the only cryptocurrency that currently exists, but definitely the one that has the highest adoption and rich infrastructure in the form of wallets, centralized and decentralized exchanges, and regulatory recognition.

2. DeFi, or decentralized finance, is an umbrella term for various financial services in a decentralized form: loans that are given out by smart contract, decentralized currency exchange or derivatives market, deposits, mutual funds, insurance and other services with no middlemen.

3. Appcoins, or utility tokens, a decentralized form of equity for DApps (decentralized applications and protocols). It is being used for two purposes: to fund products through token offerings and to enable circular economy within DApps. Key innovation of appcoins is that they are sold to anyone willing to buy and value produced by the network or application directly accrues to the token holders, therefore anyone can become an investor in DApp and they don't need to wait for liquidity events to take their profits back.

Decentralized Identity

Decentralized Identifiers (DID) is a new and prominent digital identity architecture introduced by W3C. The goal of this technology is to give every entity on the planet (including people, organization, smart things and no-so-smart things) a digital anonymous identity that doesn't rely on any centralized provider. This is the practical solution to lower the switching costs between service providers since. DID is also a privacy-protection mechanism since it is anonymous by default but you can always link a seemingly random cryptographic identifier with you real world identity or only reveal some partial information, like your country of origin without sharing the real name.

“I am large, I contain multitudes”

DIDs are free to generate and anyone can have a few dozens or even thousands of identifiers that are being used in different settings: for online shopping, for job hunting, for scientific research publishing or interacting with the government services. However, this does not mean DID owners have zero liability for their actions, as we will explore in the **Persistent Reputation** section.

Confidential Storage

The goal of Confidential Storage technology is to provide clear separation between application and data layers: applications are built, updated and maintained by businesses, but data is always in control of its owner. Instead of the world with your personal information scattered across Facebook (pictures), Twitter (tweets), Dropbox (documents), Docusign (contracts), you, as a user, have full control over personal data pods, which in turn are stored in some kind of decentralized network. All your data is always encrypted and you are the only person to decide who gets access to what information and for how long. In the end of the day, Confidential Storage aims to decouple *service* and *data* layers of the web and, by doing that, to enable user independence and autonomy to freely switch between service providers without the risk of getting locked out from their own personal data.

Now we can also see how these decentralized web layers play together: for example, DID technology mentioned above is needed to enable key management for Confidential Storage.

Distributed Computation

Distributed computation platforms are consensus-based decentralized state transition systems also known as blockchains. They provide computation services and compete in their speed, cost, throughput, degree of decentralization and censorability. Utility focused blockchains (Ethereum, freeTON, Polkadot) are quite different from cryptocurrecy-focused blockchains like Bitcoin in a sense that they are much less dependent on network effects and universal adoption. Hence, one can expect much higher interchangeability. Nevertheless, these platforms provide

a critical infrastructure for all of the other layers to perform computation in decentralized and provable manner via so called smart contracts, or DApps.

Verifiable Credentials

Highly connected digital world requires a new type of documents — the one that is open and free for anybody to use, natively digital, available on your phone or PC, permanent, provable and does not require vendor lock-in. Verifiable credentials can be a very simple piece of information like proof of email, phone number or address but it can also be a very complicated structure like a multi-party contract, full bank statement or travel history.

VCs can be considered as a "glue" that keeps the whole decentralized web stack together: Verifiable Credentials are usually issued by one DID to another, stored in a Confidential Storage data pod and verified by or through a smart contract in a Distributed Computation system.

Programmatic Governance

The goal of programmatic governance is to enable scalable, compliant, automated and verifiable legal processes. Programmatic governance tools reduce bureaucracy costs by lowering transaction costs through disintermediation and replacement of manual work with algorithms (also known as smart contracts). Not only does this technology help to automate legacy governance processes, it also creates a more efficient solution to the Principal-Agent problem. Company equity and employee compensation can be determined algorithmically. Moreover, such equity in a form of cryptocurrency or tokens provide instant liquidity and is not limited by the next liquidity event.

Decentralized governance is not only a solution for a governance inefficiencies in and between businesses, it's also a superior tool to establish fair and transparent governance for the public projects, such as charity, donation, non-profit organization, internet consortiums, public funding and even government. It includes a range of tools to carry out verifiable voting, democratic or meritocratic decision-making.

Governance is a living organism that is always adapting to external circumstances. Making this process an open sourced software achieves two major goals. First, it increases the rate and quality of improvements as different organizations can clone and build upon governance software and processes that are already available. Second, this governance becomes publicly auditable, thus it provides transparency and an efficient feedback instrument to all stakeholders.

Business Models of SSI and Other Decentralized Products

A business model describes the rationale of how an organization creates, delivers, and captures value. What's different about decentralized business models is not just a way to make money but also increased economic efficiency of value delivery due to disintermediation and increased trust.

Theory of the Decentralized Firm

First step of every economic transaction is to establish trust between transacting parties. Centralized, vertically integrated corporations were an effective mechanism to provide this trust by leveraging economies of scale, their brand image and arbitrage opportunity on the difference in the speed of information flow within organization and on the public market. In his seminal paper "Nature of the Firm", Ronald Coase argued that firms exist due to the difference in the transaction costs and information asymmetry. However, as the World Bank rightly observed in its 2019 report "The Changing Nature of Work" this statement is becoming less and less true due to ongoing technological progress and reduction in the cost of communication. The businesses are becoming less vertically integrated: Uber only does matchmaking without owning any cars, AirBnB doesn't own any real estate and yet successfully competes with the largest hotel chains. If we put this trend into perspective, we can see that what used to be the most optimal solution — maintaining middlemen and intermediaries to establish trust and reduce transaction costs — is now becoming a burden.

Coase Theorem states that in a market with no information asymmetry and zero negotiation costs, game-theoretic optimal outcome will be achieved. What was lacking since the 1960s, when this idea was originally published, was the practical

method to create such markets. In a centralized information exchange system the optimal profit-maximing behavior for the platform operator is (1) to withhold part of information and generate asymmetry or (2) to introduce fees in order to extract value from their exclusive hard-to-replicate position. With the introduction of a decentralized monetary system and distributed computation, we can now enable such markets in an open-source, provably unmanipulated way.

By eliminating or at least reducing the costs associated with establishing trust, exchanging information and bargaining we are able to create a more efficient market. Companies in such markets are replaced with networks, protocols and "personal assistants" aka Edge Agents. All the applications built on top of such a market are collectively bearing lower variable costs, therefore are more competitive in comparison with existing incumbents. In the last section of this paper we provide a detailed example of how a decentralized corporation can successfully compete with a centralized alternative.

Thanks to the instant propagation of information and decentralized web stack we're now able to construct decentralized organizations that achieve comparable or even superior levels of trust while completely eliminating the intermediaries whose profit margin generated through information asymmetry arbitrage.

Now we will examine practical models of building decentralized applications and network protocols in such a way, so that the incentives driving value creation for the network as a whole are aligned with those of its users.

Fat protocols

In his 2016 blog post Joel Monegro argued that unlike the current model of the web where most of the value is being captured by the application layer (Google, Amazon), in the decentralized web paradigm majority of the value will be created, captured and exchanged on the protocol level. By protocol we can mean any of the competing solutions for any of the six decentralized web stack layers described in this paper. By allowing multiple applications to leverage the same shared and open protocol for data storage, computation or governance, these

products are collectively more competitive compared to standard "fat application" model due to two fundamental reasons:

1. Network effects span across individual applications therefore create value for users to join an already rich and heavily used protocol. Metcalfe's Law is exponentially more beneficial for a shared protocol compared to standalone application.

2. Value captured by the protocol doesn't end up as revenue for a for-profit corporation, but rather accrues to the price of protocol native token which is usually freely traded from day one. This incentivizes application builders, individual and institutional investors as well as protocol developers to improve and enhance existing protocols rather than building a competing one.

What changed since 2016 is that now it's pretty clear that it won't be just a few dominant protocols like Bitcoin and Ethereum but rather hundreds and thousands of competing and complementary interoperable protocols. Just to give an example, one can choose to build fully decentralized web service using Solid as a confidential storage system, Ethereum as smart contract network, Bitcoin's Lightning Network for payments and DIDs anchored on Sovrin for user-controlled identity.

Let's now take a minute to better understand how the fat protocol business model works.

Cryptoeconomics

Cryptoprotocols described above do not behave as individual corporations, but rather their behavior can be best described as an online micro-economy. Such economies consist on three major groups of stakeholders:

- **Investor** side, people that initially fund the protocol by buying protocol tokens or equity in a foundation organization that is governing the network.

- **Developer** side, company or group of developers that are building the network.

- **Supply** side, users of the network that are providing value and get rewarded in a form of digital native currency: miners, content creators, liquidity providers, etc.

- **Demand** side, users that consume the service provided by the network: do cryptocurrency transactions, buy advertisement, consume content, play decentralized games, etc.

On top of that, most protocols decide to have their own currency or token to facilitate economic interactions and govern network evolution through applying mechanism design to control money supply and velocity of circulation in a form of inflation, deflation, staking, locking, burning and other mechanisms.

Since cryptoprotocols do not have a notion of revenue, it's not possible to use discounted cash flow analysis to estimate the current value. Instead the network value is paradoxically resemblant the Equation of Exchange from monetary economics which defines the relation of monetary supply and circulation velocity to the amount value created by the economic system.

Multiple competing UIs

Both strength and weakness of a cryptoprotocol is that it's not trying to solve for the full stack of internet applications. Unlike Facebook which owns data centers, backend code as well as frontend applications to provide seamless and integrated experience for its users, crypto network is usually only solving for one particular piece of the stack. This means that anyone is free to build an alternative frontend application on top of a protocol. The positive side of this is that by decoupling data, computation and UX layers we now can provide more granular control to the user. However, the short-term downside is that achieving optimal easy-to-use user experience takes time and typically is not instantly available to the users.

What we can deduce from this fact is that there will be multiple competing user-facing applications with comparable functionality on top of the same protocol. A good example would be cryptocurrency exchanges or wallets. Users can choose to use any single application and freely change them with almost zero

switching costs. This allows for close-to-perfect competition with no lock-in that benefits end users.

User experience, however, remains one of the biggest problems for all of the six Decentralized Web Stack layers and companies that are first to solve this problem efficiently will enjoy hyperlinear returns.

Self-sovereign Identity Use Cases

In this section we will bring it all together and take a closer look at hypothetical examples of applications that can be built using the decentralized Web stack. The goal of this section is to demonstrate viability, superior value proposition and economic efficiency and compare it with the internet incumbents.

Decentralized Social Media

Problem statement

We identified three major problems with social media applications today:

1. Centralized social media evolved to have user lock-in and high switching costs.

2. Centralized content display leads to curatorial bias, misinformation and discrimination.

3. Social media platforms but not the content creators are the ones who receive the bulk of the value generated by engagement on the platform.

Product Pitch

We propose a design and decentralized business model for a social network that is globally decentralized and owned by no one. The goal of this design is to resolve the above-mentioned issues while not compromising user experience.

Technical Feasibility

1. Each user has their own public DID. Anonymous for the outside observer but selectively linked to the real or virtual identity if the owner wishes so. In the DID document users can choose to specify service endpoints, such as blockchain addresses or email services.

2. No protocol-level censorship: each user is free to publish any kind of content. However, it's up to the UI to filter out any type of content that the developers don't see as a good fit. For example, one can choose to build a special social network for kids on top of a shared protocol and only PG-13 content to be displayed.

3. Semantic data is directly accessed through a pre-defined object structure, such as https://schema.org/SocialMediaPosting

4. Content is always available in a permanent storage network such as Arweave, or in the user-controlled personal data pod based on top of Solid or Filecoin protocols. This way the content is always provably censorship- and tamper-proof. In the first case it's also permanently available, while in the second case it's up to the data pod owner to hide or display a piece of content publicly.

○ Design of the locally stored Encrypted Data Vault is described in the paper by Michael Herman. While it is a very detailed description of potential implementation using existing standards, it doesn't include aspects of monetization, decentralized always-on agents and front-end applications.

5. Other users directly subscribe to the public DIDs, meaning that followership is transferable across applications.

6. Frontend applications take care of discovery, curation and monetization of the value created in the protocol

Business Viability

From a business viability standpoint we are interested in three distinct aspects of decentralized social media application, namely protocol economics, curation and funding.

In a protocol or Decentralized business model economic equilibrium is found when marginal revenue is as close as possible to the marginal cost. In the absence of for-profit corporations trying to maximize its shareholder returns, such a protocol is able to provide the same level of product quality and computational load at a lower price point. End customers are able to explicitly choose a social contract they enter with the protocol: one way would be to pay minimal fee in the native protocol token that covers data storage and computation or opt into a free model that is subsidized by advertisers. This is a win-win situation for users, developers and advertisers of the protocol at the expense of investor returns.

Curation and discovery is an important piece of value generated by any online media business. In our example curation is not happening on the protocol level, as all data (posts, likes, users) is treated as equal and no one except the data creator is in control of sharing or hiding it. However, curation platforms can be built on top without permission from the underlying network as part of one of the many competing user interfaces accessing the same data. The TCR algorithm implemented as a smart contract on the distributed computation layer creates a system where curators are monetarily incentivized to determine what is most relevant to us.

Lastly, an important aspect and key differentiator of a decentralized social network would be a more fair revenue distribution and compensation scheme for its users. Not only such a network can and is interested in providing fair compensation to content creators from advertising revenues, the model also allows for crowdsourced fundraising for popular or upcoming authors. Similar experiment recently happened on a decentralized publishing platform Mirror, where a user managed to raise almost 10 ETH to fund the writing of their essay: "Instead of publishing my work for free, or putting it behind a paywall, I'm doing something in between: raising funds to produce a new essay in exchange for ownership of the work."

Portable Persistent Reputation

Problem statement

People are status-seeking animals. Status and reputation is not easily portable across contexts, websites or online/offline settings. It's quite easy to pretend to be an expert while on the other hand it's hard to verify someone's credentials, expertise level and reputation. Existing reputation mechanisms are susceptible to manipulation (LinkedIn bots) or are not privacy-conscious (Social Credit in China).

Product Pitch

A decentralized protocol of building verifiable reputation for multiple contexts: education, work, scientific contribution, soft skills, personal integrity, credit score, reviews of goods on sale, corporate rating etc.

Technical Feasibility

To build a protocol that is dependable and trustworthy enough for building and verifying other people, things or organization's reputation we need to come up with a system design which is (a) privacy-preserving, (b) interoperable and standardized, (c) resistant to majority of attack vectors of existing reputation systems and (d) providing clear monetary incentives for protocol users to create network effects and value for the protocol.

In order to achieve interoperability we start with re-using already existing parts of the decentralized Web stack:

1. Blockchain-anchored decentralized identifiers (DIDs) to generate anonymous identities with an arbitrary number of unlinkable pseudonyms

2. Verifiable credentials as authentic data exchange layer enabled by the SSI protocols.

Business Viability

Pain points:

- Today, scoring is based on the "one size fits all" mechanism. It is designed to defend from the least common denominator and requires all customer to submit the same standardized set of data about themselves

- Businesses create overly complicated processes which leads to losing customers
- Customers are frustrated by the complex bureaucratic procedures

Solution: Persistent digital reputation that can be built by the customer over time and be used by service providers to progressively score their customers.

How it works:

1. Customer lands on the issuance portal and can start building up her reputation by getting VCs from various sources:
    - Proof of Phone number via Twilio
    - Proof of Address via Utility Bill
    - Proof of ID / residency
    - Proof of funds via bank statement
    - Proof of social media followership via Fb/Tw/Ig API
    - Proof of personhood via Zoom / Offline ceremony
    - Proof of employment
    - Proof of developer activity (HackerRank rank, GitHub # of commits/PRs/issues)
    - Proof of ownership (device, laptop, real estate, car)
    - Proof of crypto holdings
    - Proof of knowing someone (web of trust)
2. Business customers integrate the 5-liner API where they just need to select the reputation threshold during the customer onboarding process. E.g. A telecom operator can choose levels 1 thru 10 for different tariffs, where 1 is

required for pre-paid plan and 8 for long-term family contract with an iPhone and home DSL

3. Users build up reputation once, have confidence that it's in their control and can be re-used in the future with different service providers.

Decentralized Corporation

The existing trillion-dollar market opportunity for SSI is in replacing every centralized database of trusted records as well as every paper document with the Verifiable Credentials. An ambitious goal but at this point, it's becoming clear how to get there. However, the second (arguably, even larger) market is the one of building new governance structures, new decision-making processes, and eventually reinventing the notion of organization. This can't and shouldn't rely on SSI technology alone but rather on tight coupling of the Decentralized Stack. In this article, I'm talking about by far the most complex and the most important layer of that stack — the DAO.

According to the https://deepdao.io/ and https://defipulse.com/ there are at least 180 operational DAOs in the world at the moment with over US$ 50 billion in value controlled through them. Even though most of those organizations are still at their very early stages and considered experimental, these organizations were able to produce highly successful products that are wildly popular among their customers.

Problem statement

An organization (corporation, firm, company, or government) can be defined as a group of people authorized to act as a single entity to generate profits or social benefits. The reason for the structured organizations' existence can be described as transaction costs minimization from the economical point of view or as a coordination problem solution from a game-theoretic point of view.

However, within the centralized legally enabled corporations dominating the world today both of those problems are not solved efficiently. Coordination within firms is problematic due to the Agent-Principal Problem. And transaction costs

within firms are still suboptimal as with the growth of complexity corporate governance becomes expensive and is barely offset by the economies of scale or exclusive know-how. In traditional organizations incentives, the distribution of risk and decision rights, and the distribution of residual claims are all operationally managed by the use of both implicit and explicit contracts. [Morrison] Explicit contracts result in legal costs of negotiation, singing, and enforcing. Implicit contracts leave room for ambiguity and unneeded arbitration at the later stage.

Product Pitch

Decentralized Autonomous Organization (DAO) represents a set of linked smart contracts running on top of a public blockchain that enable governance run by stakeholders collectively rather than by managers selected by the shareholders exclusively.

The "The DAO" lesson taught us a lot. Modern DAOs are not just one gigantic smart contract. The modular approach proven to be highly effective in all other branches of software development and thus is being used in the development of governance tools.

The actual operational work in most DAOs is not done through blockchain-based coordination but rather using the more traditional means of communication like Telegram groups. It is an only financial, executive or high-level strategic decision that has to be made in an actual decentralized governance form. In addition, there's a reduced risk of making wrong non-financial decisions as an alternative is always a possibility through a fork, whereas for a competitor there's no more economically rational action than to fork an existing organization and experiment with their own approach or strategy.

Technical Feasibility

Before blockchain there was no way to make economic governance systems experimentally, all of it was purely theoretical. The key and by far the most important quality of the DAO is its openness: anyone can fork or build on top of the existing system. Moreover, if investors, founders, or developers of a certain DAO decide they want to extract more profits for themselves, this organization will

be most likely forked and launched in a more competitive and fair form. As we continue to experiment with billion-dollar businesses fully governed by the DAOs, we learn important lessons about:

1. Most efficient decision-making mechanisms: liquid democracy, pseudonymous or even anonymous voting, programmable meritocracy

2. Building systems that are trustless (no reliance on a single entity) yet reliable (have a fallback solution in times of crisis or hostile takeover)

3. Adopting law to the blockchain world. The legal system has been around for millennia and it's not a smart decision to completely scrap it all together and replace it with a Solidity program but to find an intricate balance between machine- and human-owned arbitration

4. Modeling of economic equilibria in the decentralized financial management systems. Something that isn't practically possible in the closed-source companies of today.

Business Viability

DAO is not about better corporate management or shareholder decision-making. DAO is about replacing old, incentives-incompatible, zero-sum, greed-powered organizations of the past with the decentralized inclusive alternative.

1. Centralized == closed. Any company is started with openness in mind as it struggles to get its first customers. However, as the business matures it focuses more and more on satisfying the shareholders' demands and increasing shareholders' value. Instead of cooperating with the market, it focuses on competition and defending its positions. In contrast, DAO is owned by all of its stakeholders, including developers, managers, customers, and investors.

2. It's not the token but actual ownership people are buying. DAO provides a natural way for token holders to actually benefit from the growth and actively participate in the governance and development of the projects they invested in without reliance on a centralized legal entity.

The Path Towards SSI Adoption

In this section we are going to explore ways to accelerate the rate of SSI adoption. We will start with discussing the value generation mechanisms in SSI and how the value realized by the end customers depends on the network effects created though standardized, portable and interoperable digital identities and credentials. We will discuss some key problems that slow down SSI adoption. Finally, we will propose a practical solution to expedite the build of truly interoperable marketplaces that are aligned with the incentives of SSI vendors, data issuers, services providers and provide superior end customer experience when compared with some traditional solutions.

Current situation

SSI is getting traction among governments, business customers and end users. The technology, governance systems and public specifications are becoming more mature. The regulatory support, awareness of SSI concepts and the number of theoretical use cases are growing every month. However, the rate of adoption can be higher across geographies and verticals. Solving the "chicken and egg" problem turned out to be a quite difficult task for a lot of SSI companies.

First and foremost SSI is a network technology, meaning the value is realized not by a single customer using the product but rather through the network effects. The value is created at the edges of an SSI network graph. SSI network utility, as with many other networks, can be described with the Metcalfe's Law stating that the value or utility of a network is proportional to the number of user's of the network.

Holders benefit from abundance of issuers, ability to choose different edge wallets and larger number of services offered by the verifiers. Verifiers are more likely to implement SSI flow once there's mature enough UX, a lot of holders with pre-existing or easy to get credentials. And so on.

But how can we build these network effects while preserving user's privacy and SSI vendors' autonomy to build a sustainable and defensible business model based on key company strengths?

First, let's structure and sum up the challenges that hold back SSI adoption.

Problems of Existing SSI implementations

SSI ecosystem is fragmented

This is both a challenge and a positive thing, as with more experimentation we're able to learn faster and build more tailored solutions for specific customer segments, jurisdictions and verticals.

- Today we have dozens of SSI network implementations (using permissioned, permissionless DLTs or ledgerless) and 82 did methods.

- it's hard to exchange credentials across networks and there's still no wallets that works across all of them

- Very hard and unintuitive to share a VP combined from multiple credentials issued on different SSI networks and by different SSI providers. One example would be COVID tests and vaccination certificates where dozens of companies and organizations create their own standards yet we still see very little interoperability.

- Number, complexity and differences among governance frameworks is growing. Today we see such frameworks being developed by non-profit organizations, governments and corporations.

What to do? Even though a lot of SSI standards are interoperable, there's still a missing link that will enable discovery, transactions and re-use of credentials across multiple SSI providers.

Customer education is suboptimal

The SSI ecosystem is quite often confusing for people who are working in it full-time. If we expect SSI to be as widespread the ease of use should become comparable to standards and protocols like PDF, SMTP or HTTP. We shouldn't expect customers to understand how exactly this works but we need to enable SSI software to provide similar seamless UX. One can use any search engine of choice using any device and browser to find and interact with any website.

An analogue of this would be an SSI Holder being able to discover and examine SSI credentials offered by the issuers, services offered by the verifiers and their respective governance models and compliance requirements. The Holder should not care about software used by either party and if they are part of the same network. Moreover, to create a truly open SSI ecosystem without the tendency to lock-in SSI applications should facilitate credentials re-use across ecosystems: why shouldn't I be able to use a vaccination VC issued by the German government to sign up with the scooter sharing app in Israel? In reality those two systems most likely will be using different Verifiable Data Registries, DID methods, SSI networks and software vendors which not only makes it complicated technically but also results in suboptimal frustrating UX.

What to do? It is not as much about educating customers but about lowering requirements through UX simplification. For the end customer, having a DID and a bunch of VCs should be as intuitive as owning a physical passport, not like a digital item that is only valuable on a single website.

SSI companies don't have a sustainable business model

SSI was created as an open interoperable set of standards, yet today we see very little collaboration between the SSI vendors and providers. All parties can benefit from the shared network effects yet the current business incentives force companies to build their own end-to-end solutions which often leads to the fragmentation problem described above. This leaves SSI vendors with two high level options:

1. Build the network effects between Issuers, Holders, Verifiers themselves which is a capital intensive and time consuming process. It requires building an

n-sided marketplace from scratch and also leaves an SSI provider to do all the education to shift customers' paradigm from centralized or paper-based approach to DID+VC mentality.

2. Resort to only building software which might not be a very sustainable model long-term as more and more open sourced solutions are created every day. This means that potential profit from building software for issuers or verifiers will be arbitraged out as more service companies and free software comes to the market.

What to do? Design and build an open protocol that will enable not only data transfer across SSI applications but also value transfer. This will stimulate SSI providers to join existing ecosystems and leave them with a sustainable business growth path. For example, two SSI healthcare or financial ecosystems in EU and NA would benefit from using a shared value transfer mechanism due to simplified UX, mutual benefits of network effects and overall better utility of the product.

Threat of centralization and de-anonymization

Lack of the interoperability on the level of network management and SSI software can potentially also lead to lock-in and centralization. Increased switching costs reduce competition and this just reduces the rate of innovation and creates suboptimal user experience which in turn hampers adoption.

Threat of fraud and impersonation

Siloed SSI ecosystems without shared governance practices and data registries can potentially lead to impersonation of SSI actors. When verifying an issuer's authority to issue a specific credential type ideally we shouldn't just trust the fact that the issuer is part of some sort of registry (such registry can be built and operated by a legit network provider as well as by a malicious actor). To solve this we need a marketplace model that unifies and cross-checks multiple governance and assurance systems (probably based on a centralized or decentralized reputation system).

Introducing VC Marketplace

Typical SSI go-to-market strategy involves building an n-sided marketplace of Issuers, Verifiers, Holders, Governance Authorities, Ecosystem Operators and so on. Many companies in the industry are doing exactly this. The key innovation of VC Marketplace allows SSI providers to collaboratively generate more value for their customers and provide seamless customer experience while preserving competitive advantage in software and target markets.

Let's examine a proposed VC Marketplace design:

VC Marketplace describes standard interfaces that SSI software uses to enable shared discovery of SSI actors capabilities. For example, issuers announce the governance framework they are following and what credential types they are offering. Verifiers in turn can announce Presentation Definitions for the exact VP that they require. This can happen across networks and ecosystems, therefore end customers have access to any other network participant that is valuable for them.

VC Marketplace includes a value transfer layer in addition to data exchange interoperability. This allows building cross-network business processes. For example, a bank in the US using Indy-based SSI software can request and pay for the KYC VC issued by the issuer in India who's using alternative software. Every network, issuer or verifier can publicly announce a price for issuing, sharing or storing a VC if they see it fit.

VC Marketplace is a protocol and should have multiple implementations. Due to the interoperable nature of SSI standards and especially recent work related to VC-HTTP-API, Credential Manifest, WACI and Presentation Exchange allows anyone to create their own implementation. VC Marketplace can be a standalone web or mobile application; can be integrated with the SSI wallets or directly accessed via API by any other software.

VC Marketplace should not store or force end users to share any PII. Marketplace needs to keep track of public schemas, issuer and verifier registries from different networks. However, all the data collected by the marketplace application must be explicitly shared. Primarily this data comes from issuers and

verifiers publishing their credential manifests, presentation definitions and other information needed to provide their services.

VC Marketplace can be centralized and run a single company or a decentralized application (like a smart contract). Marketplace can be built in either one of the following forms:

- Commercial application build by a for-profit company with internal business model (e.g. transaction fee paid by issuer or verifier after every successful marketplace match and transaction)
- Non-profit application build by a government or NGO
- Fully decentralized application with no direct owners, possibly enabled by circular cryptoeconomics and staking/slashing mechanism to fight fraud.

VC Marketplace acts as an SSI storefront for the Holder. It allows search and discovery of credential types, trusted issuers and definitions of what verifiers are asking for. For example, customers can use marketplace to find answers to the following questions:

- Who can issue me a VC of a certain type? What's the issuance process I need to follow to get it issued?
- How do I trust a particular Issuer or Verifier? What governance framework are they using? What regulation and jurisdictions are they compliant with?
- Who's accepting the VCs that I have? What services can I get with those VCs?

Every SSI provider and SSI network should be completely autonomous without the marketplace. The goal here is not to create another dependency but rather provide an option for SSI ecosystem builders to bootstrap adoption of their products.

Conclusion

In previous chapters we discussed the vision of the decentralized Web and how SSI plays an integral part to it. We covered the market problems that can be addressed by this technology stack and potential outcomes. Next up we covered the technical solutions for these problems. We also discussed business models that can enable sustainable growth of the SSI and decentralized applications and infrastructure protocols along with real world use cases that prove these business models to be viable. Finally, we discussed the key roadblocks that are present on the way to universal SSI adoption and how these can be solved.

To sum everything up, the area of Self-Sovereign Identity is proving to be a foundational technology to enable digital identity and decentralized web for the modern world. Most of the technical challenges with SSI are either solved or we have a clear path of how to get there, however the problem of adoption still exists.

In this paper we proposed a few immediate steps that can be done to pursue these two goals:

1. Provide real production use cases for the freeTON blockchain,
2. And increase the rate of SSI adoption.

We feel very confident and excited about the rate of innovation happening in this space (both from technical and regulatory angle) and expect to see many production applications to be built in the coming years.