How SSI Will Survive Capitalism

a white paper from Rebooting the Web of Trust VIII

by Adrian Gropper, Michael Shea, and Martin Riedel

ABSTRACT

The Self-Sovereign Identity (SSI) community has described several groundbreaking properties that arise from the adoption of its principles. Governance, as in business and financing structure, is arguably the most challenging of these properties, captured succinctly by Shoshana Zuboff as: "Who decides? Who decides who decides?" However, even though the technology has matured greatly over recent years, bootstrapping an SSI product within the existing capitalistic market environment is complicated and has not been achieved at scale within any functional domain.

A RWOT6 paper explored the challenges to a sustainable commons. In this paper, we apply the SWOT framework (Strengths, Weaknesses, Opportunities, and Threats) to identify potential paths to adoption. For example, what are the general implications of introducing a credential holder into existing issuer/verifier relationships? Our analysis leads to cooperative (in the legal sense) governance with focus on the holder (the wallet) as the key innovation, since issuers and verifiers already exist. The healthcare industry is used as an example.

Caelum Labs
Generalitat de Catalunya
DCO
Protocol Labs
VENN . AGENCY
Validated ID
PTBVENTURES

Sponsors for the Rebooting the Web of Trust VIII Design Workshop

INTRODUCTION

Over the past twenty years there have been a consistent wish that individuals would be able to control their personal information in a manner equivalent to the pre-internet age. There have been multiple "turns of the wheel" (OAuth, SAML) of technological standards that have attempted to enable this. Self-Sovereign Identity (SSI) is the latest attempt to do so. In each of the previous attempts, the technology and work that was supposed to strengthen the position of the individual was subverted and the result is the current situation of strong corporate players (Google, Facebook) leveraging convenience to further mine behavioral data on individuals.

There can be no argument that there is a ground swell around SSI currently; the real unknown is whether SSI will maintain its current trajectory of empowering the individual to regain control of their information. However there are still real challenges ahead around enabling adoption and countering attempts to hijack the sector and direct it in some unforeseen manner. This paper provides a strategic analysis (SWOT) of the SSI community and sector to reveal where we believe the threats may appear and to identify the best path to adoption.

SWOT ANALYSIS

This paper applies the SWOT Analysis, a strategic planning technique that can help an individual or an organization in determining Strengths, Weaknesses, Opportunities, and Threats ("SWOT") to identify possible paths to adoption around Self-Sovereign Identity concepts. SWOT analysis may be used in any decision-making situation when a desired end-state (objective) is known. It should take into account internal and external factors that contribute to achieving or failing to achieve a given end result. The results of the SWOT Analysis can inform about possible measures or counter-measures in order to support or prevent certain anticipated factors.

Strengths of SSI

- Avoids an enterprise sale: adoption can be decentralized, one doctor, one patient at a time. Separating the SSI strategy in this way avoids having to create both supply & demand (bootstrapping cost, typical in a platform)
- Ease of implementing Privacy by Default
- Transparency is controlled by principals (doctors, patients) not by intermediaries
- Non-sectoral: the same personal agent creates opportunities across industries/sectors
- No corporate data aggregation
- Builds on top of object capabilities and delegation framework
- An Identity-layered Internet allows for the development of new business models in a privacy-preserving way without expensive platform intermediaries (decentralized Uber, decentralized eBay, decentralized AirBnB).

Weaknesses of SSI

- A barrier or friction point in adoption is created by introducing the holder into an incumbent verifier-issuer relationship.
- Lack of upfront financing due to lack of platform leverage (chicken & egg problem)
- Risk of increasing transaction costs
- Every technology can be used for good or bad and in many instances the first 'commercial' successes are for illicit purposes; quacks and fraudsters, are going to rise, creaing the potential for social media hysteria and significant shifting of market perception.
- Correlation of agent endpoint (we need tunnels, Tor, ...)
- Cellphones, as a secure element, are not inherently SSI
- Walled garden App Stores are not inherently SSI

Opportunities of SSI

- The value (cost) of data brokers/intermediaries can be redistributed to the principals (issuer, subject/holder, verifier)
- Decentralization of policy making promotes diversity and resilience
- Competition for governance
- Authorization agent improves data quality: elimination of rekeying, provenance implicit, streaming, query, single of point of monitoring, policies stay private
- Use of Zero-knowledge proofs for reputation, nullification (e.g., vote only once), data minimization
- Globalization of medicine where the patient selects the jurisdiction of physician; decentralization of reputation and issuance (e.g., guilds vs states)
- AI cost is 80% data and data cleansing, 10% data science and technology, 10% verification/validation (elimination/reduction of data brokers does not remove/limit AI)
- Decentralization of AI to reflect SSI principles through Self-Sovereign AI-enhanced agents based on federated machine learning. Federated machine learning means that one AI can teach another AI without actually sharing the training data itself. Human-in-the-loop AI is another example of Self-Sovereign AI.
- Standardized data governance labeling (http://bit.ly/PPR-IGL), *Quinn Grundy et al. - Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis, BMJ2019*)
- Agent capability improves with greater API standardization within the market (API effectively defines the data model. Semantic compatibility makes the agent more reliable.)

Threats of SSI

- Data brokers and intermediaries will fight to keep their current roles.
- Platform mentality and political power of platform, through the vehicle of regulatory capture, can delay effective standards and raise regulatory barriers.
- Need for standards, and lead times for standards.

- Market inertia: data brokers are here and built into the value chain.
- May require governmental action (antitrust for oligopolies/monopolies, human rights of access and privacy)
- Requiring change by multiple stakeholder categories (issuer, holder, verifier) magnifies barriers.
- Existence of government regulation (NIST-regulated trust framework models), where stakeholders may be willing to change but regulatory inertia causes delay.
- Data brokers are very large businesses, like icebergs, 90% hidden.
- Crypto wallets that are not SSI get integrated natively into iOS and Android.
- Agents as a Service (AaaS) (Microsoft, Amazon, Google, Telco's, ISPs)
- Intel SGX favors platforms and centralization
- Elimination of data brokers requires an alternative for all of a particular data broker's roles. Solutions may be required in as many as six use cases (reputation, matchmaker, transaction convenience, data brokerage, mapping data for a common ontology, and record retention)
- Lack of business knowledge for tech-first SSI industry participants
- Collusion or Regulatory Capture: direction is taken over by a limited number of private corporations that organize in "community groups", that do not truly represent commons or effectively create a barrier to entry.

SWOT RESULT INTERPRETATION: "BARRIERS, PATHWAYS AND THE THIRD RAIL"

With the identified factors of the SWOT analysis we are able to deduce further implications around the adoption of SSI. Specifically, we want to point out possible barriers, pathways, and distractions that may arise.

Barriers

- Want to bootstrap use without single entity dominance.
- Non-traditional economic model; SSI model has by definition no equity upfront. All value is created in the Commons.
- A Commons does generate enough equity for traditional finance models.
- Platform tokens have security regulatory risk.
- Surveillance capitalism has very low friction.
- Cultural norms (China) resistant to full agency (want backdoors).
- India (Aadhaar) wants to centralize and maintain control of identifiers.

Pathway Choices

Desired End State

Open-source standards-based code in a cooperative-based financial model, with each co-op in control of their specific policies while agreeing to allow any individual or entity to exit the cooperative, start their own cooperative, or operate outside of any cooperative. See Rochdale Society and seven principles of cooperatives and Past, Present, Future: From Co-ops to Cryptonetworks.

Community-driven Wallet reference implementation

Given the novelty and importance of the introduction of holder responsibility, the community should strive towards providing a non-commercial wallet implementation to support this process and lower the barrier to entry.

AaaS First

Agent as a Service (AaaS) as an intermediate pathway before completely moving the responsibility of the agent into the User space (e.g., "access recovery via the centralized service, like people are used to"). However, these services would need to be tightly regulated and allow a seamless transition into a fully self-sovereign internet. Regulation should aim at removing them altogether as soon as a critical size has been reached.

The Third Rail

- A megamerger of platforms across hosting, telecom, and payment creates the universal identity based on transaction surveillance. Regulating data use instead of regulating aggregation itself is a prescription for disaster.
- Apple fails at privacy by default; Facebook privacy theater wins.
- Private telecom uses 5G to eliminate the opportunity for personal firewalls as agents. Alternatives, such as mesh networks and free community broadband, are not actively pursued. (Need regulatory measures to give control to the owner of 5G-enabled equipment, e.g. keys, triple-blind, etc.)
- Our children join corporate America with blind respect for authority and platforms. The SSI infrastructure need for diverse holders/subjects is seen as a risk.
- Private authority does not have the ability to deter bad behavior the same way that government can, but government is weak compared to private sector.

THE HEALTH CARE EXAMPLE

Healthcare (the industry) is large and more about personal data than most markets. Health care (the value transaction) is prone to decentralization because the principals, patients, and licensed practitioners are able to transact independent of any institution and in some cases independent of any particular jurisdiction. This kind of decentralization is reminiscent of public blockchains.

SSI, in this example, applies to the licensed practitioner as well as the patient. Each of them is a holder. The practitioner holds credentials issued by testing institutions and benefits from appropriate reputation mechanisms tied to their identity. The patient holds health records, including notes, diagnoses, and prescriptions, issued by the licensed practitioners. These two rather different holder technologies must interact with each other independently of institutional issuers and verifiers.

The healthcare industry is dominated by data broker intermediaries that aggregate practitioner licenses and reputation on one side and aggregate patient health records on the other. We call them hospitals. Under what circumstances would the hospital support the introduction of SSI holders on behalf of either the practitioners or the patients?

Competitive pressure will force hospitals to accept SSI, effectively driving them out of the data brokerage business if they wish to remain in the principal business of operating ERs, surgery suites, and other health care services. But for that to happen the data brokerage function of hospitals will need to shift to an SSI model that respects a diversity of standards-based holders. What institutions will organize the tech and support systems to provide holders to the practitioners and patients?

Patient and physician cooperatives could provide governance and support for SSI holders without need for a proprietary business model or private equity. Alternative structures for support of SSI holders could be government (as a public commons) or a not-for-profit collaboration by interested principals such as pharmaceutical and device manufacturers. Strategic support could also come from employers and other players that stand to benefit from reducing the cost of data brokerage in healthcare. Another possibility for support of SSI would be a new class of data brokers built around a fiduciary relationship with the subjects. These Agent as a Service models will pick and choose among the SSI principles and standards and possibly focus on healthcare to the exclusion of other markets in order to develop brand and platform economics with private equity support.

CONCLUSION

Adoption of SSI is dominated by the challenge to the data brokers and intermediaries that would be replaced by holder technology. Even if some data brokers are able to pivot to Agent as a Service during a transition to SSI, the highly redundant and hidden data aggregation business would be decimated. SSI can overcome these incumbents while staying true to its principles by developing and supporting holder technology through a cooperative model. Cooperatives can focus on the needs of issuers and verifiers in specific markets while at the same time adopting and supporting standards that will allow holders to operate seamlessly across diverse markets. Transitional states on the path to decentralized SSI could include holder services with a more or less fiduciary relationship to the subject. In the long-run, self-sovereign identity and individual agency require both Free software and standards with support through cooperative governance.

The disintermediation and destruction of current data broker business models provide very strong economic incentive to hijack and subvert the goals of the SSI community. This is something that community must be constantly aware of and be prepared to counter.

Additional Credits

Lead Author: Adrian Gropper

Authors:Michael Shea and Martin Riedel

Sample APA Citation:

Gropper, A., Shea, M., & Riedel M. (2019). How SSI Will Survive Capitalism. *Rebooting the Web of Trust VIII*. Retrieved from https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/final-documents/how-ssi-will-survive-capitalism.pdf.

About Rebooting the Web of Trust

This paper was produced as part of the Rebooting the Web of Trust VIII design workshop. On March 1st to 3rd, 2019, over 80 tech visionaries came together in Barcelona, Spain to talk about the future of decentralized trust on the internet with the goal of writing at least 5 white papers and specs. This is one of them.

RWOT Board of Directors: Christopher Allen, Joe Andrieu, Kim Hamilton Duffy

Silver Sponsors: Caelum Labs, Digital Contract Design, Generalitat de Catalunya, Protocol Labs, Venn Agency

Additional Sponsors: Validated ID, PTB Ventures

Community Sponsors: Blockchain Commons, Digital Bazaar, In Turn Information Management Consulting, Learning Machine, Legendary Requirements

Workshop Credits: Christopher Allen (Founder), Joe Andrieu (Producer and Facilitator), Shannon Appelcline (Editor-in-chief), and Carlotta Cataldi (Graphical Recorder)

Thanks to our other contributors and sponsors!

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rwot8/issues

The ninth Rebooting the Web of Trust design workshop is scheduled for September 2019 in Europe. If you'd like to be involved or would like to help sponsor the event, email:

rwot-leadership@googlegroups.com