SSI: A Roadmap for Adoption

A Journey from *huh?* to *DUH!*

Authors:

* Moses Ma, FutureLab
* Claire Rumore, FutureLab
* Dan Gisolfi, IBM
* Wes Kussmaul, Reliable Identities, Inc

**Abstract:** The self-sovereign identity developer community is fun and vibrant in thought leadership, but the community’s current direction will not lead to exponential adoption. The community needs to get serious about doing what it takes to insure success for the standard, applications and vision. The goals need to be made clear: (i) a better approach to communicating the core concept and its benefits, (ii) the production of tools to assist in the development of compelling applications, (iii) the deployment of products that produce WOWs that stimulate media interest and viral propagation, and (iv) which leads to the formation of a critical mass of end users.

## Goals

* Outline a better approach for communicating a crisp, cohesive and comprehensive vision of the core benefits of SSI.
* Justify the importance of streamlining the developer experience through tools that improve time to value and assist in the development of compelling applications.
* Shift the focus from longer term ad-hoc brainstorming towards a formal initiative to develop a set of minimum viable reference applications.
* Help find the WOW (the balance between low hanging fruit scenarios and instantly graspable killer app features) that inspires hope and stimulates media interest and viral propagation so that we can win the hearts and minds of a critical mass of stakeholders.

## Audience

This paper is targeted first and foremost at the SSI technical community who needs become a enabler and not a descration to broad adoption. There will always be hard problems to solve, but in order to have the opportunity to work on non-trivial and interesting technical problems we must come together as a community to define and execute on a roadmap that makes hides the technical complexity of our vision, addresses the needs for a seamless experience for both developers and users (citizens). Our discussion will tackles not only suggest best practices for businesses to create a SSI strategy but also help debunk some of the myths that have arisen due to a lack of understand which of course is a direct result of our failure to simplify and articulate the concepts and benefits of SSI for the masses. We will touch on the necessity for toolkits, minimum viable environments (MVE), and interoperable end to end exemplars.

Specifically, this paper is targeted at the early adopters within a minimal viable community of stakeholders:

* Incubation thought leaders at ground zero that are passionate about bringing Self-Sovereign Identity (SSI) to maturity.
* Participants in open standards organizations
* Participants working on open source code based on those open standards
* Early adopters within the developer community
* Change agents within the media, enterprise and public sectors
* University and research institutes
* Forward thinking venture capital investors and incubators

## Success Metrics

Crystallization of common community initiatives that are measurable via Key Performance Indicators which include:

* The community goal is to see one million DIDs published by March 2019
* The release of a handful of reference applications that provide a down payment on the promise of decentralized identity
* Formalized plans by year end 2018 for the foundational SSI specifications
  + W3C DID
  + W3C VC
  + Oasis DKMS
* Go to Market Resources to support developers by year end 2018
  + Glossary of Terms
    - SSI v. Self-Administered Identity
  + Convergence of technical primers (tutorials) into a central getting started kit
  + Common baseline talking points for SSI advocates
  + High impact videos
  + Portfolio of industry specific demonstrations
  + RWOT demo recordings
* Foundational catalysts for adoption
  + Creation of a realistic technology roadmap
  + Adoption of a formal agile project management approach to drive the roadmap
  + Recruitment of foundational partners for a social media platform
    - Operational recruitment of key technologists from Slack, Telegram and RocketChat
    - Ideological recruitment of influential leaders (i.e: Reid Hoffman, Fred Wilson, etc)
    - Get some traction on meaningful support from GitHub and Wikipedia

Reality Check

We are a community of very passionate and bright individuals who share a common vision about self-sovereign identity (SSI). We have as an open community established in the foundational building blocks for bringing the SSI vision to fruition. We are admits a perfect storm whereby fear of identity related hacks and thief are pervasive; decentralized identity and key management is now possible because of enabling technologies like blockchain; and governments and business are realizes the risks and liabilities associated with centralized identity systems. However, this perfect storm also comes at a time when non-SSI alternatives are also being considered at scale. For example, one of our core worldwide identity instruments, the digital driver license, is being considered by national and state governments worldwide. Unfortunately, the new mobile driver license (mDL) initiative that is being driven by ISO will yield technical debit within society that will make the adoption of SSI even more difficult. The time is now to get focused on an clear and achievable rollout roadmap for SSI technology.

An honest assessment of the state of our SSI initiative will yield the reality that we are “not ready for prime time”. If we can get the community That is actually

* + We need to set expectations so early adopters can develop plans
  + We need to hide the complexity for usage
  + We need to solve the Wallet distribution problem
    - Who are the wallet makers
    - Need secure wallets - http://www.links.org/files/nspw36.pdf

Myths to debunk

There is a perception that blockchain based identity solutions actually store personally identifiable information (PII) on the distributed ledger. This is utterly false. The SSI initiative not only advocates against such poor practices, the community has established several principles including that of *portability* that address this issue. The concept of a ID is essentially a globally unique [decentralized identifier](https://w3c-ccg.github.io/did-spec/#dfn-did) that is compliant with internet standard [Universally Unique Identifiers](https://en.wikipedia.org/wiki/Universally_unique_identifier) (UUIDs). A SSI solution would use a ledger to establish immutable recordings of the lifecycle of a DID that is associated with a person, place or thing. However, the verifiable credentials that capture ones PII and associated with a DID are never placed on a public ledger.

Another common misconception about the decentralized identity concept, stated by less technically adept analysts, is that participation in the system is somehow involuntary. Additionally, it has been said, erroneously, that a decentralized ID could “never be turned off or blocked” due to the immutability of the distributed ledgers that underlie decentralized applications. And finally, that it will be impossible to prevent anyone from publishing anything they want about you, and that the immutability of the ledger means a negative review would be part of an indelible permanent record. That is, once you are associated with a digital key in a world of pertinent memory, anyone can choose to add any information they want about you to the public record that could never be changed.

These misconceptions could not be farther from the truth. About these issues, the DID specification states clearly that the publishing of any user’s decentralized ID is explicitly controlled and administered by the user/owner. The proposed specification for Verifiable Claims states plainly that claims are revocable, expirable, and in section 6.8 “Fitness for Purpose” that the policies of both the issuer and holder must be adhered to. It’s assumed that the normal policy for a holder is to approve every claim before acceptance. This means that a competitor, who would not be trusted to make a claim about your business, could not append a negative claim about your business without your explicit approval. This is because both the issuer and holder both have the ability to revoke any claim.

Furthermore, an interesting distinction can be found in section 8.8 “The Principle of Minimum Disclosure”, which states that the system follows a minimal disclosure approach that could help with compliance with HIPAA in the US and GDPR in the EU. This means that users can be in control of private data that they don’t even realize they have, enabling a level of control over personally identifiable data and enabling data privacy at a level heretofore never seen before.

The final, and perhaps scariest issue, is that you will likely not be able to opt out as a user from participating in the public sharing of identity data. You might choose as an individual to not identify yourself with a public key on a blockchain. But someone can still add other pointers to the ledger (your email, your phone, your photo) and then attach claims to that log that anyone can access.

One common misunderstanding concerns the perception that one cannot opt out as a user from participating in the public sharing of identity data. This notion is reminiscent of the old passive aggressive putdown, “When did you stop beating your wife?” - leaving not only a presumption that the offense occurred, but also leaving the target of the disparagement with the impossible task of proving a negative.

Why would one assume that somehow the fact that a blockchain is involved means that a user would be compelled to assert an identity in any particular case?

Beyond that is the fact that an asserted identity cannot be reconstructed from the trail it leaves on the blockchain.

Establishment of the Roadmap Tribe

One requirement for success is to establish a roadmap tribe, that would be responsible for driving the workflow for developing tools and process required for success. The roles within the tribe include: a communications workgroup that would propagate the messaging, domain leaders who would advise on key components, go-to-market resource developers, and a scrummaster to drive the workflow and insure timely results.

The volunteers who have bravely committed to join this tribe are:

* Co-chairs
  + Dan: gisolfi@us.ibm.com
  + Moses Ma: moses.ma@futurelabconsulting.com
  + ???
* Scrummaster:
  + Darrell Duane, [d@duane.com](mailto:d@duane.com)
* The communications workgroup:
  + Kate Sills: [katelynsills@gmail.com](mailto:katelynsills@gmail.com)
  + Sean Bohan: (via Drummond)
  + Kaliya Young: Kaliya@identitywomen.net
* GTM resource developers:
  + Alex Preukschat: (via Drummond)
  + Remy Lyon: remy@keemail.me
* Domain leaders:
  + David Crocker, Standards
  + Nathan George: (via Drummond)
  + Input from Manu, Drummond, ???
* Interested Resources
  + Vishal Diro: [vishal@diro.io](mailto:vishal@diro.io)

Manifesting some WOWs

Another requirement for success is to create a design process that would lead to a sustainable flow of compelling technologies that provide a “wow” factor, that can form a pipeline of compelling functionality to fortify the value proposition for decentralizing identity. Current projects and ideas for “wow prototypes” include:

1) Community Badges Toolkit

Our goal is to produce a Starter Kit for any small or large community to begin to issue verifiable credentials in the form of OpenBadges to create viral adoption (see: <https://openbadges.org>). This could be an artifact in the GTM Kit. The output of this could be fed into the Verifiable Credentials working grou.

2) Industry Exemplars

We need to develop a number of vertical industry reference dapps. For example, in fintech, the Credit Union Ledger Demo that uses Hyperledger’s Indy framework. Another example, or vision would be the World Economic Forum’s Known Traveler Report. But others can and should be developed in healthcare, education, etc.

3) Other broader concepts

There are a number of other potential reference applications that could be interesting to develop and deploy. These include a decentralized authentication system, which could be called “SuperSignOn” using the DID-AUTH platform. Another is proposing GitHub Authentication using Verifiable Credentials. Another could be to use Verifiable Claims as a basis for attestations by attorneys in ICOs. And perhaps to make a system similar to IDESG’s IDEF assessment tool: <https://www.idefregistry.org/> to receive the badge

## Deliverables

* Reality Check: Criteria for Success
* Action Tracking for the Roadmap Tribe on Trello
* Roadmap:
  + Project Team
  + Published Plan/Schedule
* MythBusters:
  + FAQ Sheet
  + A call for terminology (Glossary)
* WOW Factor: Community Badges Toolkit

### 