**Self-Sovereign Compliance: Use case for DIDs and VCs in decentralized capital formation**

Presented by Moses Ma, FutureLab

Submitted to the 6th Rebooting the Web of Trust Technical Workshop as a discussion paper

Santa Barbara, March 25-26, 2018

***Keywords:*** reputation, trust, verified claims, collaboration, innovation, framework, blockchain, decentralized, self-sovereign, capital formation, ICO

**PROPOSAL**

We propose to facilitate the collaborative drafting of a technical paper that describes the principles and key design considerations for a use case that utilizes Decentralized IDs and Verifiable Claims to implement self-auditable, self-sovereign compliance for capital market investors. We will also describe other issues, including downstream functionality, user centric needs analysis and cognitive models, ROI for digital compliance, the the potential use of incentive tokens to economically drive the eco-system.

We base much of our work on key design considerations for decentralized identity, claims and reputation, developed by C. Allen, M. Sporny, D. Reed, and many others (see references), at previous RWOT design conferences.

**BACKGROUND**

Here’s the central idea: *identity on the Internet is broken.* Not just a little broken, but *seriously* broken. Because identity is currently built in a less than optimal way, crimes like phishing can cost a typical Fortune 1000 an average of $4 million per year. Ransomware, the fastest growing form of cybercrime that has grown 1500% in only two years, has caused $5 billion in damages globally last year alone. And it’s expected to quadruple next year. And we all know that hackers using bots can seriously interfere with national elections.

What we have now is a rare and unique opportunity to fix online identity. What we need is true user-centric identity, which is possible only by making the user central to the administration and control of his or her own identity. What this means is that we need to understand the true meaning of digital identity, and in this process, enable greater user autonomy. To accomplish this, we need to create something we decentralized identity. This new way of looking at identity requires a mindshift––to evolve beyond the idea that your identity needs to be controlled by a government. This new way deconstructing and reformulating identity requires that you become your own government, to be your own sovereign. Just as Bitcoin allows you to “be your own bank”, the *decentralized identity* will empower you to fully control your own identity.

What’s happening is that we are now transitioning from a digital feudal system, similar to when vassals owned vast amounts of land in the Middle Ages. Serfs worked the land to create value but most of the value was appropriated by the vassal. Today the new asset class is data—where value is created by all of us but captured entirely by digital vassals and sovereigns (governments, social media companies, search engines, banks, etc.). To recapture your data rights, we need to stage an identity revolution. This, hopefully bloodless, revolution will actually empower society to lift the effectiveness of society, governments and businesses to the next level.

This new way to implement universally unique identifiers are called “DIDs”, or decentralized identifiers, using special features provided by blockchains. Just like Bitcoin, which uses the blockchain at its core to provide trust in a trustless environment, the DID can provide identity services in an environments that do not support trust. At a deeper level, DIDs are actually the tip of a technological spear, that unleashes an entirely new layer of decentralized digital identity and public key infrastructure (PKI) for the Internet. This decentralized public key infrastructure (DPKI) could have as much impact on global cybersecurity and cyberprivacy as the development of the SSL/TLS protocol has had on the Internet of today. This new layer of functionality is where the value of fixing identity can unlocked, starting with an emergent technology called the Verifiable Claim.

Imagine a world where identity works. Imagine the end of phishing. The end of spam. The end of fake news. And the beginning of new era for society built on a interconnecting web of trust. This is the true mission of decentralized identity. For this paper, we will envision what we can do with DIDs and verifiable claims to empower an innovation in public token offerings, in effect, to invent the next generation ICO. We believe this would provide a reference application that could not only validate the power of DIDs and verifiable claims, but to accelerate adoption as well.

**APPLICATION TO CAPITAL FORMATION**

The first thing we need to agree on is that the Security and Exchange Commission is not the enemy. In fact, it was created to be the investor’s best friend, with the investor’s best interests at heart. (There *are* ways that the SEC favors corporations over people, but we must remember that it’s walking a fine line to keep everyone happy and the markets purring.) The threefold mission of the SEC is to protect investors; to maintain fair, orderly, and efficient markets; and to facilitate capital formation.

To achieve its goals, the SEC requires the registration of all securities offerings, as well as the identity and reputation of every U.S. stockbroker and brokerage firm (a form of identity to enable tracking and oversight), and demands that investors in the most risky investments be “accredited”. It also enforces the honest disclosure of regular financial reporting. Our theory is that the SEC could perform all three tasks better, faster and cheaper using blockchains, DIDs and verifiable claims.

For example, when a company launches an IPO under the auspices of the SEC, it has to truthfully disclose the backgrounds of the management team, the capitalization structure, and significant strategic partnerships. The process now entails filing reams of documents, using accountants and attorneys to double check compliance and provide comfort letters to attest compliance. Using verifiable claims and the blockchain’s “self-auditing” feature, we believe that it is possible to automate each of these functions, and delivering compliance at an order of magnitude less cost. If the Chief Scientist of your company has a Ph.D. from MIT, why not include a blockcert that proves this computationally? If your company has a strategic alliance with a global distributor, why can’t this be recorded in a verifiable claim? In this way, the validation of representations in offering documents could be automatically and digitally validated, costing much less than relying entirely on attorneys and certified public accountants. As those trust intermediaries begin to rely on verifiable claims to assume less risk, they will be able to provide attestations and comfort letters at a much lower price.

But that’s only the beginning. If your company should lose that distribution agreement, the verifiable claim could be revoked, and such information could be relayed immediately, than a mention in the quarterly earnings call. Using a real-time framework, greater transparency could be afforded to the investor. This will actually encourage companies to develop competencies that are better for them than learning how to hide bad news. For example, companies would be incented to improve their pipeline of sales prospects, distribution alternatives and product innovations to better manage risk. This would shift the focus from needing to exceed expectations in every quarterly report to increasing the value of foresight and innovation, and help build stronger and more resilient companies. Using the analogy of personal health and fitness, increased openness and transparency would enable a transformational shift from companies focusing on ways to “get through the next physical” to focusing on managing sustainable wellness.

Another function of the government regulatory bodies is to detect money laundering by enforcing compliance with KYC (Know Your Customer) laws. At the same time, governments are telling companies to value the privacy of its customers with GDPR (General Data Protection Regulation) laws, because this is a good thing for society. By decentralizing, and moving identity verification closer to the user, we can satisfy both requirements simultaneously. In the case of ICOs and KYC, the solution is to have attorneys attest that a client is not a money launderer. For example, the investor could be a software engineer who lives in a repressive regime who was lucky enough to buy Bitcoin very early, but has left the holdings in cold storage. He simply does not want to realize a gain until they he has emigrated to a safer country. Remember, there are several countries where the governmental leaders have made money by extorting oligarchs––as in “I’ll let you out of jail if you hand over half your fortune”. These investors would be severely endangered by the governments need to know everything.

Customer centric solutions are always more effective and will enjoy greater adoption than government centric solutions. Freezing the assets of offshore crypto investors, who would prefer to support innovation globally, is not a wise solution. If we are to move toward a decentralized world, the forces of centralization need to take a breath and co-create new solutions that can provide anti-money laundering and anti-terrorism requirements… but can still insure the privacy and anonymity of the investor. If attorneys and accountants can attest that their client is an accredited, why not allow them to attest that they are not money-launderers? Why not allow them to more effectively manage their holdings and allow their capital to help make a better world? Why not endeavor to protect their identity from being leaked to a repressive regime?

And so, some of the deliverables we hope to develop during the workshop include:

1. Create a user persona for a meaningful ICO investor to analyze user needs
2. Develop a detailed use case for an ICO investor
3. Develop a spec for the use of DID within the reference application
4. Develop a spec for the use of Verifiable Claims within the reference application
5. Understand social/network interaction functionality between investors, company and regulatory agencies to map out downstream functionality
6. Seek input from top tier investors and regulatory agency technologists
7. Open discussion on other issues, such as cognitive models, ROI for digital compliance, the the potential use of incentive tokens to economically drive the eco-system

**Next Steps**

And so, our goal for this working paper is to map out functionality against the proposed DID and Verified Claims standards. The proposed paper will include a design philosophy for the implementation of decentralized identity within the framework of regulatory compliance and “zero knowledge” disclosures.

We would like to collaborate with the participants of the Rebooting Web of Trust Workshop to refine the concepts expressed in the paper and to more fully develop this use case. Our goal is to improve the standard, as well as enable the development of a pilot/prototype that demonstrates a compelling use case in vivo.

**References**

https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/did-primer.md

https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/verifiable-claims-primer.md