Opportunities Created by the Web of Trust for Controlling and Leveraging Personal Data

A White Paper from Rebooting the Web of Trust

by du5t, Kaliya "Identity Woman" Young (@identitywoman), John Edge, Drummond Reed, and Noah Thorp

Overview

In November 2015 Facebook's share price broke $100 USD/share, for a total valuation of $290 billion USD. This is evidence that both Facebook and the market understand the value of controlling and leveraging personal data. However, the now-conventional absorb-everything design of Facebook is a blunt one. Employing users as passive producers with no control of their own data only scratches the surface of what is possible with networks of information and identity.

Some of these constraints arise from Facebook's centralization, something that tends to worsen as an organization grows in size. There are limits to the amount of trust this sort of centralized authority can garner. This often results in punitive postures: democracies come with the expectation that citizens be forever watchful of their government; while corporations are watched over by regulatory bureaus and further deterred by class-action suits.

Decentralized systems that are engineered to *prevent* concentrating power as they grow avoid this. They can in fact increase their credibility as more users provide their assessments as input. Protocols and structures that are distributed and self-sovereign also offer significantly improved robustness, portability, and versatility than conventional centralized or escrowed processes — especially when combined with secure cryptography.

One of the first technologies to offer the advantages of decentralization emerged 25 years ago when the advent of PGP realized a Web of Trust that contained decentralized, cryptographically verified attestations of its users. Unfortunately, failures of UX design confined the spread of PGP to highly technical communities.

Today, decentralized Webs of Trust remain as important as ever. Now is the time to extend them to be usable by everyone who has access to digital networks, in particular to marginalized populations that can benefit from the technology. It is a fortunate tragedy that there is no shortage of real-life examples of the need for decentralized Webs of Trust in the world today. A large spectrum of individuals — from marginalized persons like stateless refugees and victims of human trafficking to members of the informal or unregulated economy — urgently need to participate in otherwise privileged economic and political fora, but they face technical, economic, and political barriers to entry.

The essential problem is to connect burgeoning new technological developments with unmet consumer needs, and vice-versa. In this paper, we present five use cases: from two relatively simple cases of managing selective disclosure to the most extreme case of establishing government-verifiable credentials from nothing for a stateless refugee.

Each case identifies basic technical implementation needs, presents a brief solution sketch, and outlines potential user experience. Afterward, we discuss common themes and summarize future prospects.

Use Cases

1. Selective Disclosure: Proof of Age
2. Short-term Contracts with Memory: Distributed AirBnB
3. Bootstrapping Long-Term Identity: Creating A Record of Credit
4. Concerns in Non-G20 Nations
5. Starting From Zero: Refugee
6. Human Trafficking: Exiting Safe Houses

1. Selective Disclosure: Proof of Age

Beth wants to go to the club with her friends, but lately the clubs have been photographing all IDs at entry for "reasons of liability." Both club owners and privacy-minded individuals like Beth are understandably concerned about how this data will be stored and used. The current system requires that the individual share an ID that gives not only their exact age but also their name, address and other information that's unneeded in this context.

The involved parties have the following goals:

- Beth wants to get into the club while providing the minimum information required: proof that she is over 21 years of age.
- The club owner wants to be able to later prove that all attendees were over 21 years of age if needed.
- The club owner *doesn't* want to incur the liability of securing irrelevant personally identifying information (PII).
- The local government wants to establish a minimum degree of verifiability of the club's records without creating undue liability issue for the club owner.

Selective disclosure can meet all these goals. It's a process by which a credential holder like Beth offers *only* the information needed by a service provider, for *only* the scope (the amount of time) needed to serve its purpose. Typically, this involves the substitution of a *verifiable claim* for the actual credential itself; in the case of "proof of age", Beth could submit a one-time claim that her age is in fact over 21 in response to a request from the club. The club owner need only check that the claim is valid.

The following process could satisfy these requirements:

1. Beth receives a request from the club owner containing a unique random number generated for this purpose ("nonce").
2. Beth supplements the nonce with a description of the claim she wants to make (i.e., "birthdate earlier than 21 years prior to now") and signs it, creating a "digest".

3. Beth submits the digest through secure channels to an independent, decentralized store whose record of truth (and therefore credibility) is out of the control of any one actor, whether government or business. The only guarantee the store needs externally provided is availability (i.e., uptime).
4. A state agency connects with the store from its end (perhaps by polling for requests), sees if the request is valid (that it came from Beth and makes sense as a request), and then signs the result and the nonce, inserting them both into the data store as a new digest available to Beth.
5. Beth provides the new digest to the club owner, who can verify that the result was signed by the right authority.

Of course, the actual user experience of this is simple: Beth could scan a QR code provided by the club owner and approve the verification request through an app on her phone. The result could then be a different QR code, which the club owner can scan to verify. All of the technical back and forth happens in the background.

Note that at the end of this process, both of the third parties involved know very little about Beth:

- The state agency storing Beth's driver's license data only knows that Beth needed to claim she was older than 21 — not where that request came from (assuming that communications metadata has been dealt with).
- The club owner only knows that the state agency agrees or disagrees with Beth's claim, and perhaps which state agency it is.

Because mechanisms that provide "ground truth" or "trust" are located in different parts of the system, it is highly resistant to malicious action at any single point or even across a collection of points. Expiry dates can be added to the data during each of the steps, ensuring that data generated at any step is only meaningful in a certain time-limited context, subject to the regulatory and social needs of stakeholders. Beth may also make adjustments to the request to ensure that the club owner and government cannot collude to deanonymize her from either direction.

Commentary: Academic Literature

Variations on this theme have been published in academic literature for decades, beginning with the "blind signatures" of David Chaum et al. (1983) and the "zero knowledge proofs" of Goldwasser et al. (1985).

Aspects of this use case are in practice in the commercialization of U-Prove (Microsoft) Technology in the German Identity System. Similarly, British Columbia's eID system was designed to provide for the selective disclosure of just a name and photo and the assertion of being above the drinking age when purchasing liquor (thus preventing the disclosure of name, address, and exact birth date to the seller).

2. Short-term Contracts with Memory: Distributed AirBnB

Tisha wants to rent an apartment from Joe for 2 weeks. They each need enough validated information (e.g., a home address) about each other to establish identity, credit status, and legal accountability, as well as some sort of letter of reference that is relevant to the proposed transaction. They do not belong to AirBnB, but would like to be able to create a similar level of assurance without giving up the same degree of information to a centralized service. Tisha generates proof of name, legal residence, and good credit as well as letters of reference, which may be anonymous or otherwise opaquely identified. Joe can then judge these submissions.

If Joe accepts Tisha's proofs, they establish a contract that sets out the terms of Tisha's stay. The result of that contract (fulfilled or broken) can later be used as a reference for subsequent stays with others.

The following process could satisfy these requiremenst:

1. Tisha maintains basic demographic identifiers securely in independent, decentralized, cryptographically verifiable, append-only repository, as per Use Case 1.
2. Tisha and other users can "bootstrap" some limited reputability by having friends issue "letters of reference" on her behalf. These could be as simple as ratings or they could be actual letters, submitted to the repository attached to their accounts.
3. When Tisha arranges a short-term contract between herself and a relative stranger, she invites them to submit proof of the contract and its result, with a rating or comment, to the same repository. Contracts created in this fashion are linked in the data repository by incorporating the signatures (or signature transactions) of all parties — once at establishment, and (optionally) once on fulfillment.

Note that throughout these exchanges, Joe and Tisha's respective privacy is protected until they are both ready to meet in person, if they choose to do so. It's then protected afterward. As a rule, personal private information should never be shared directly; once data is copied to a location out of its owner's control, no guarantees can be made of its security, and mandated deletion is unfeasible.

Commentary: Technology Possibilities

Users are both ready and willing to protect their identities in this fashion during short-term arrangements. The AirBnB app collects an inordinate and unacceptable amount of personally identifying information from its users. On the other hand, craigslist has included per-listing email obfuscation for years now, and the Berkman Center for Internet & Society at Harvard maintains a massive list of services and frameworks that regard the user as the initial and final arbiter of information exchange.

Contracts as described here are a common application for decentralized verifiable data stores; implementations targeting this area include the "smart" contracts of Eris Industries and Ethereum, and the "link" contracts of XDI. Both of these types of contracts include expirable permissions and context-limited pseudonyms.

3. Bootstrapping Long-Term Identity: Creating a Record of Credit

Darla is a citizen of a G20 nation but lacks a deposit account, extensive credit history, or reputable documentation of local residence. She can afford a secure digital device however, and through it, she can sign up for an account, whose marginal cost is close to zero. She would like to be able to store money with a bank, credit union, or other institution and build a credit rating, but she can't meet current minimum requirements set by the bank through conventional channels such as the 100 point scale. In other words, Darla needs to cross a "gap" of credibility in order to enter the conventional world of credentials.

This is similar to the previous cases, except that the goal is the creation of private credentials that are a reusable link to a conventional financial record. The credentials will be held by the account holder and have validity (in this context) equal to a fixed address.

The following process could satisfy these requirements:

1. An independent organization sets up a decentralized data store for collecting verifiable claims submitted either by the state or Darla.
2. The independent organization onboards Darla, ensures she understands the guarantees of privacy offered, and verifies that her credentials do not fundamentally depend on the state.
3. The state, in concert with the independent organization, signs Darla's initial claim, deeming it to be of sufficient strength to accomplish tasks like the above.
4. Darla submits proof of the state's approval of her established identity, *selectively discloses* any attributes additionally required by the bank, and establishes a conventional account.

Systematically speaking, implementing this protocol requires reference to the Know Your Client and Anti-Money Laundering regulations (KYC/AML) of the jurisdiction or country that is being approached. Once the regulatory compliance identity criteria are established, the delta between the existing quality of identity and the required quality of identity must be established. Common processes can then be built for improving identity to a level that passes the KYC/AML tests, which are the chief barriers to accessing established financial services.

Preserving low cost of access and progressive establishment of reputation are both essential to maintaining accessibility to services.

Commentary: Technology Possibilities

In this use case, Darla is without any "right to be forgotten", as her credit history and financial activity are inevitably stored in conventional centralized structures, such as those held by a bank. Thus, the best she can do is provide verifiable stipulations governing the exchange between herself and financial institutions. One appropriate structure for this use case is a link contract. Link contracts are semantic structures intended for peer-to-peer communications. They express stipulations of information governance in a transparent fashion, appropriate for a system that intends to guard credit and credibility. This can include rules governing the disclosure, sharing, and lifetime of information made available through networked channels. XDI, a non-profit organization, maintains one standard for such link contracts.

If well-implemented by banks and credit rating agencies, link contracts could enable users of financial systems to efficiently detect possibly fraudulent activity and to dispute or address erroneous or malicious activity associated with an account, all in a way that avoids information asymmetry and the associated power inequalities that arise from it.

3.1. Concerns in Non-G20 Nations

In the *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*, Peruvian economist Hernando de Soto highlights a fundamental difference between Western liberal democracies and the rest of the world: the West has functioning systems that enable the abstract representation of value. For example, land is not simply owned territory — it is private property registered with the state and represented by land deeds. These land deeds are an abstract representation of the land and as such can be used to leverage the ownership of the land when interacting with institutions like banks to secure capital. The West also has functioning state institutions and systems of law that imbue those deeds with cultural, financial and legal power. They have what could be considered high levels of social trust — as described by Steven M.R. Covey in *The Speed of Trust* and summarized by one of the co-authors of this document.

Millions of individuals do not have such representative records (e.g., birth certificates) registered with government entities. and some governments may not be reliable enough to serve this role. Worse, many marginalized people are prohibited from creating records that might enfranchise them, either through legal exclusion or threats of violence.

Without such abstract representation of themselves their ability to interact with institutions such as businesses, governments and NGO's is limited. The Gates Foundation considers this issue one of their eight global priorities:

> *Worldwide, more than 2.5 billion adults do not have an account at a financial institution, according to the World Bank's Global Financial Inclusion Database. Only 41 percent of adults in developing economies have an account—and that number drops to just over 20 percent among adults living in extreme poverty. Women, in particular, are largely excluded from the formal*

> *financial system. In developing countries, only 37 percent of women have accounts, compared to 46 percent of men.*

They also highlight research showing that "the most effective way to significantly expand poor people's access to formal financial services is through digital means." With this in mind, consider the following use case:

Farhad is a migrant worker at a mine. He has no fixed address and receives a regular wage in cash, which he would like to store in a secure account. He has no recurring bills or credit bureau profile, but he turns up for work on time every day, six days a week, 50 weeks a year. He's known in multiple locations by the same name and travels in the same geographies. He needs to be able to turn this accumulated consistency into a portable, self-sovereign record of economic reliability that others can assess and verify, so he can store fiat currency, pay bills, and gain access to credit.

Farhad is without state or financial institutional support, which changes the dynamic from the case of Darla residing in a G20 nation. On the other hand, this may result in a lower regulatory burden. What Farhad needs is a way to take the same semi-informal exchanges mentioned in previous use cases and bundle them up into a highly-available, privacy-respecting, verifiable record of credible activity, which is the basic information required for a consumer-facing financial market.

The following process could satisfy these requirements:

1. An independent organization sets up a decentralized data store that can be reached by users like Farhad with minimal equipment (e.g., a low-grade smartphone with data).
2. Farhad bootstraps his financial record with verifiable records of work and other met commitments, in conjunction with clients, employers, and other financial actors in his sphere (cf. use case 2).
3. With this record (and possibly an associated cryptocurrency where needed), Farhad can now make both local and electronic purchases with increased leverage.
4. Financial service companies can now make anonymous queries a la Craigslist, sending offers to users who meet a raft of criteria. Farhad can choose to submit anonymous claims that he meets different criteria, allowing him to receive these offers or apply directly for loans and other financial agreements.

This system is empowered by decentralized computing, which makes it possible to support individuals like Farhad in representing themselves — allowing them at last a self-sovereign identity that they create and control. Through it, they can link together their interactions and transactions and leverage them to create an abstract representation of themselves. This type of identity can empower unenfranchised people like Farhad by creating the "secure kernel" of identity that is taken for granted by holders of state-issued identity documents. Such a secure kernel can then give people like Farhad access to basic social needs like health insurance and

credit — privileges in the Global North that are considered dire needs of citizens in the Global South.

This system also ensures that Farhad's records are not exposed to surveillance, nor to (financial) corruption. Transaction history is not revealed to merchants or financial service providers, nor is activity. What is available is a verifiable record of commitments on contracts and their fulfillment status. This can include both positive and negative claims to reputation. Note that mechanisms of differential privacy may be needed in this case, to prevent semi-aggregated queries from permanently reducing the privacy of users whose data is contained in the store.

Commentary: Self-Sovereign Identity

It is critical to understand that this type of self-sovereign identity is different then just anchoring transactions to a phone number. Individuals *do not* have control over a phone number in the same manner. Phone numbers are rented from the phone companies and are even re-assigned to someone else when one stops paying one's bill!

4. Starting From Zero: Refugee

One way to "prove" an identity is to present identity documents from a state, but what happens when there isn't a functioning state to issue such documents, or an individual is kept from obtaining them? Can an individual establish and maintain a self-sovereign identity that can survive these circumstances and serve as a conduit of interaction with public and private institutions?

Yevgeni is a member of a persecuted or targeted class in his nation of citizenship and residence. When he flees his nation, he does not feel safe carrying identity documents with him. Information asserting his grounds for asylum must also bypass local centralized data stores, as it could be used to harm him (e.g., records identifying or locating individuals could be seized by a new hostile regime).

In order to meet this goal, a secure, decentralized,privacy-respecting data store must be made available to the legal jurisdiction of the host government that Yevgeni flees to. However, refugees often move through multiple state territories and would prefer to avoid creating permanent personal records under complete surveillance. This requires the data store be maintained independently from the states themselves.

Such a technology can empower Yevgeni to create a self-sovereign "anchor" of identity: whatever documentation or information he has can be stored as statements or photographs to be used for claims later. Yevgeni is now able to leave his country without excessive risk, and to use his self-sovereign identity at immigration, on the host government's terms. The prospective host government can poll the store to satisfy their documentation requirements, obtaining proof of identity attributes that only Yevgeni can access directly.

In this case, a technical solution does not proceed in a simple step-by-step fashion, but we can identify the chief requirements:

- Safe onboarding of a potential refugee at their current location, likely with the help of humanitarian organizations.
- Authentication methods that "survive the trip" along with the refugee, preferably passphrases, not just biometrics.
- Partnerships with refugee-hosting governments.
- Partnerships with independent organizations maintaining the data store, backed by a policy-compliant API.
- Functionality allowing refugees to progress toward an independent status, along the lines of the previous use cases.

Commentary: Webs of Trust

People share social contexts; they exist in community with each other and create webs of human connection through social relations. This can be made rigorous and verifiable with self-sovereign identities held by each person; these identities can be documented digitally by mutual verification asserted cryptographically using a secure digital medium. Creating this type of contextual social network to validate an identity is why this aspect of the technology is called a *Web of Trust*.

The network of connections securely documented between individuals' sovereign source identities could also serve as the seed to bootstrap an identity within a new jurisdiction and under new document circumstances. In other words, it is only through a Web of Trust linking self-sovereign identities that someone in dire traits as a refugee can be credentialed to a degree acceptable by Global North governments while maintaining strong guarantees of security and privacy to all the stakeholders involved.

Commentary: Vetting Refugees

In the wake of the November 2015 Paris attacks, multiple nations have cut back on refugee intake, ostensibly in response to increased fears over the vetting of refugees. While governmental immigration checks are typically quite extensive and deliberate, we believe a robust system like the one proposed here might allow for more trustworthy claims, as well as faster vetting and verifying in general, improving conditions for refugees and host countries alike. Most notably, such a system avoids the false tradeoff between 'security and privacy', allowing claims about risk to be judged in a verifiable fashion while protecting the privacy of the majority of innocent refugees.

5. Trafficking / Safe Houses

Marsha is a victim of human trafficking who has been rescued by a local group and conveyed to a safe house. She may have an identity card issued to her by the state, but she does not trust the *local* state office enough to present her identifier to access

benefits because she may be re-victimized by them if she does. An aid organization and/or the main government office is willing to provide resources such as money, food, and education to Marsha so that she can re-normalize her life, but she needs a way to access them.

Marsha has the same technical needs for bootstrapping an identity as those explained in the previous use cases. The unique challenge here is in handling existing "toxic" components of Marsha's existing identity: her traffickers may have access to many physical and digital credentials, which may also link to friends or family. Marsha might want to reconnect with people or obtain access to stores of value in existing accounts without risking further harm.

The main government or aid agency also has requirements of its own. It needs Marsha to establish core attributes of identity and to submit repeated proofs of that identity and (changing) status for compliance purposes, so that it can account for the aid provided. However, when Marsha finally leaves the safe house and resumes independent life, she must be sure that her private information leaves with her.

These requirements can be summarized as follows:

- A protocol for establishing a set of "core" initial attributes.
- Data storage at a completely independent location that has robust protection against threats.
- Strong guarantees of selective disclosure.
- If possible, reconstruction of still-valued components of a now-toxic previous identity.
- Clear threat models at every step of the process.

The key to meeting these needs is to provide an individual services across time and space in a way that avoids duplication and provides for continuity of care. In other words, it requires persistent correlatable claims — cryptographically verified statements in support of personal information. An example might be:

1. An aid organization, in conjunction with an independent provider (ideally an NGO specializing in identity management), equips Marsha with a clean, fresh device for securely handling her data and contacting aid workers.
2. Marsha enters her personal demographic data into the device without publishing the information anywhere.
3. The aid organization signs Marsha's claims to eligibility for government or other assistance programs.
4. The aid organization can now also serve as a proxy for communications with relatives or friends that Marsha needs to reach; since the aid organization and Marsha have personally established a secure, verifiable relationship, the aid organization can expand the sphere of private communication.

An independent organization can transmit these claims with the consent of the client, achieving this result for the client without compromising her privacy. Thus, she avoids direct contact with local government systems that she mistrusts.

By taking on this role, the independent organization is dis-intermediating the state issuance of identity documents. This is useful because of Marsha's mistrust of the local state office. She is now able to have the independent organization mediate the provision of support services to her via government aid from a different department or a different level of government. She is not dependent on any particular part of government infrastructure to maintain her records throughout negotiation — be it a database targeted by criminals, or a mandated program with a limited lifespan.

Commentary: Digital Quarantines

We note that this is not a speculative scenario; the 'digital quarantines' and surveillance pressures undergone by women in shelters or sex work are documented in the reporting.

Discussion

Opportunities/Unsolved Problems

The use cases presented here share a host of common themes and characteristics, including portability, security, privacy, autonomy, and universality. Any identity system that exemplifies these characteristics will almost inevitably become the basis for an unprecedented expansion in economic and social activity. However, such a system must surmount challenges in technical, political, and human spheres. Each of these challenges, of course, provides an opportunity to create value.

Technical Challenges

- Manageable and portable equipment for storing identity information and making strong claims with precise scope and context-limited disclosure.
- Decentralized data stores and secure APIs that share a minimal set of operations and content types.
- API implementations in an open, auditable form in well-maintained, cross-platform languages that target mobile and desktop OSes.
- Repudiable biometrics.

Political Challenges

- A negotiated concordance between amount of information provided by uncredentialed persons and the amount initially required by conventional institutions.
- Partnerships with local authorities for education, implementation, and outreach.
- Support structures for independent data providers, independent audits, and user onboarding (hardware) across the world.

Human Challenges

- Behavioral protcols that swap in 'proof of X' for 'X' in (all) transactions where someone's identifiers are requested.
- Bootstrapping/onboarding/enrollment from self-affirmed identity attributes, expressed in a fashion intelligible to all potential users.

Near-term prospects

Although the demands illustrated by the use cases we present are quite serious, we note that there have never been so many legally unencumbered technical and expert resources for these applications as there are at present. We believe that the main challenges ahead are those of system integration and widespread adoption, for which the prospects are good. Given adequate funding, we are certain that the challenges illustrated above can be met, with good outcomes throughout the process.

Moreover, we recognize that we are presented with an unprecedented historical opportunity — the evolution not only of the internet as infrastructure but a turning point of human culture. Development of self-sovereign identities rooted in a decentralized, distributed, verifiable data store can usher in a world where, for the first time in history, identities can be represented and communicated in a fashion that transcends any centralized authority, enfranchising every actor in the system as a unique person, community, company, or government. Through these identities, any actor, regardless of origin, can obtain the assurances they need to operate and engage in interactions that require persistance across time and space — a record of continuous commitments that will underlie incredible economic and social improvements for humankind.

Privacy-respecting, secure (in the senses defined above), decentralized systems are uniquely able to both accurately chart this experience and to empower us to foster or develop identities that have never been possible before. While this is great news from a technological standpoint, the same systems could also be employed in a coercive manner. At worst, large-scale information systems — whether centralized databases with essentially unlimited storage or decentralized append-only structures — could near-permanently foreclose the disjoint, varied, and possibly contradictory nascent identities of masses of people if mobilized at the will of a single interest group. (Imagine if a government ID system was coupled with an undeniable append-only log, fed by a ubiquitous surveillance system ... then place it at different points in history.) We have a grave responsibility to implemement these systems in an ethical and forward-thinking manner.

Doing so will preserve the largest possible potential to future generations.

Appendix: Why 'Decentralized'?

Network service infrastructure, viewed broadly, has exhibited the following four trends in rough succession:

1. Centralized - referring to the simple 'conventional model' where all users connect (or even 'dial into' in the 80s and early 90s) to a single server which handles all communication for clients. Clients are completely dependent on single servers to be both available and trustworthy.
2. Distributed - encompassing both high-availability clusters, load-balanced servers, content delivery networks, and cloud services. This design is primarily concerned with performance and robustness, leaving independence out of the picture.
3. Federated - systems like Diaspora, where small-scale 'centralized' services coordinate traffic between each other, allowing for a measure of independence (usually anyone technically literate can establish a service), while avoiding islanding or balkanization of networks.
4. Decentralized - (ideally completely) flat systems wherein essentially every user is also a 'provider' of the service. Provider activity usually consists of relaying traffic and participating in cryptographic computation to maintain the health or security of the network.

Decentralized systems, if well-implemented, have the best future outlook; they are highly robust, incredibly scalable, and offer a great deal of flexibility as the basis for an application stack. Moreover, their basic design assumptions mitigate issues with transnational privacy regulations--the data storage location is typically not allowed to view the stored data *in situ* (i.e., the data is encrypted in storage and in transit). Instead, they are tasked only to transport the data to a trusted location or temporary environment where it can serve its purpose (such as issuing or verifying claims). Systems that exemplify this feature include Tahoe-LAFS and Freenet.

Throughout the scenarios presented in this paper, we make repeated reference to an 'independent data store' or 'provider', whose main obligation is to make data available under a variety of regulatory and situational regimes. This data, combined with whatever authentication secret each use case's subject holds, is the source of 'truth' used to issue claims. As emphasized above, both of these components must be maintained independently from governments or organizations, both for reasons of practicality (financial and managerial outlay to maintain large-scale systems) as well as trustworthiness (governments, NGOs, businesses, and marginalized individuals have vastly differing incentives). A decentralized system is the most scalable way to ensure the independence of such a system.

Additional Credits

Lead Paper Editors: *du5t, Kaliya "Identity Woman" Young (@identitywoman)*

About Rebooting the Web of Trust

This paper was produced as part of the ***Rebooting the Web of Trust*** *design workshop. On November 3rd and 4th 2015, over 40 tech visionaries came together in San Francisco, California to talk about the future of decentralized trust on the internet with the goal of writing 3-5 white papers and specs. This is one of them.*

Workshop Sponsors: *Respect Network, PricewaterhouseCoopers, Open Identity Exchange, and Alacrity Software*

Workshop Producer: *Christopher Allen*

Workshop Facilitators: *Christopher Allen and Brian Weller with graphic facilitation by Sonia Sawhney and additional paper editorial & layout by Shannon Appelcline*

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: http://bit.ly/weboftrust-issues. We are also planning for more gatherings on this topic in the near future, with the object being to have something notable ready for release on the 25th anniversary of PGP, in July 2016. If you'd like to be involved or would like to help sponsor these events, email:

ChristopherA@LifeWithAlacrity.com