How to Convince Dad* of the Importance of Self-Sovereign Identity

** and your sister and your daughter and your best friend and your nephew*

a white paper from Rebooting the Web of Trust VII

by Shannon Appelcline, Kenneth Bok, Lucas Parker, Peter Scott, and Matthew Wong

ABSTRACT

One of the major problems with bootstrapping self-sovereign identity is that it requires adoption by a large number of people. Pushing self-sovereign identity from the top-down is most likely to result in a technology that's not actually used, but instead encouraging the average person to demand self-sovereign identity from the bottom-up will result in the organic development of a vibrant, well-utilized decentralized web-of-trust ecosystem.

This paper addresses that need by offering arguments to a variety of people who might be reluctant to use self-sovereign identity, uninterested in its possibilities, or oblivious to the dangers of centralization. By focusing on the needs of real people, we hope to also encourage developers, engineers, and software business owners to create the apps that will address their reluctance and fulfill their needs, making self-sovereign identity a reality.

INTRODUCTION

"Cogito ergo sum — I think, therefore I am."
—René Descartes

"Identity is a uniquely human concept; however modern society view this concept of identity as state-issued credentials such as driver's license and social security cards, which suggests a person can lose his very identity if a state revokes his credentials or even if he just crosses state borders. I think, but I am not."
—Christopher Allen

The possibility of losing your identity is a serious problem in the digital world. Vloggers could lose their identities if YouTube closes their accounts, while common internet citizens like you and me could lose a big part of our life if Facebook revokes our credentials. As digital accounts become a major part of our identities, we need a paradigm that allows us to bring identity back under our control.

Self-sovereign identity seeks to be that new model, creating a paradigm shift in an increasingly data-governed world. It puts the individual in control of her identity and prioritizes her privacy. It does so by acting as the root anchor for an individual's data stream, permitting an individual to manage, store, and control her own data and life. It could become a ubiquitous technology that affects the lives of billions on a daily basis.

This runs counter to the traditional model for online identity, designed from the perspective of the corporation and government, with the needs of the individual being secondary. In the age of "Surveillance Capitalism", personal data is typically abused by large corporations in the never-ending quest for profit, disregarding user privacy and inadequately safeguarding user data. The Equifax hack in late 2017 and the Cambridge Analytica scandal highlight the risks of large, centralized databases of personal information (i.e. honeypots of data), which present high-value targets for hackers.

But how do we convince the average person to move from the old, centralized model to the new, self-sovereign model? We think that this requires proactively fulfilling their needs. To highlight these needs, we've created case studies for five people who could be served by self-sovereign identity, if they were only aware of its possibilities. They are:

- Your dad, who is preparing for retirement;
- Your sister, who is a world traveller;
- Your daughter, who is a reckless social media user;
- Your best friend, who is a content creator; and
- Your nephew, who runs a convenience store.

These five people represent a spectrum of use-cases and applications, meant to portray some of the monumental possibilities of self-sovereign identity in the not-so-distant future. They are concentrated in the developed world, because we believe that is where adoption of self-sovereign identity will begin. Some of these use cases are possible now, while others will require a more fully fleshed-out web-of-trust ecosystem.

YOUR DAD IS PREPARING FOR RETIREMENT

Dad is getting ready to retire, which has him thinking more about his financial security. So much is online now! He has to use his laptop computer to pay some of his bills from his bank account, and he looks at his retirement accounts through his browser too. He has a few different logins and passwords, because the different institutions have different requirements. He keeps them written down on a yellow post-it that he hides in his desk drawer.

Recently, Dad has become paranoid about having his money stolen because his best friend got phished by someone claiming that their Microsoft Windows installation needed updating, which let the hackers install a keylogger on their computer and steal some money.

Though Dad finally traded in his flip phone for a smartphone last year, he doesn't use it for anything but reading news stories and text messages.

"I hate having to log into so many financial accounts."

The Problem. Dad gets annoyed at all these confusing accounts and logins and passwords. He'd like to have a single account that accesses all of his financial services and he'd prefer not to need a login and password for it at all.

The Solution. Using his self-sovereign identity, Dad can federate logins to various financial services. He accesses it using biometrics: he just looks at his smartphone's camera, it scans his face, and then the smartphone verifies his identity to his laptop. This gives him access to all of his federated financial accounts without needing to type logins or passwords. An app on his laptop consolidates all of the information from the accounts and allows him to view his finances, write checks, and free up retirement money.

"I'm afraid someone will steal my money through some sort of fake login."

The Problem. Dad is especially vulnerable to phishing attacks, in which someone obtains access to his financial account by pretending to represent the financial institution. He lives in constant fear of losing his nest egg: he is concerned that it is impossible to tell the difference between a legitimate representative and a scammer.

The Solution. Because Dad logs in using his smartphone and face recognition, there is no way for him to accidentally log in to a fake portal. The application will take him to the correct site.

"If I get my identity stolen, I'm screwed."

The Problem. Dad has heard a lot about the ravages of identity theft: attackers stole names, phone numbers, and addresses from Home Depot and stole reams of identity information from Equifax. Dad is afraid that the thieves could use this information to steal his money at his financial institutions or to take out credit or loans in his name.

The Solution. This sort of breach would be less likely in a world of self-sovereign identity because users can safeguard their information under their self-sovereign identity, preventing it from entering large honeypots of personally identifiable information (PII). But, even if a breach were to expose Dad's information, it wouldn't affect his access to financial institutions: the PII wouldn't give access to his accounts without validation from his smartphone; if someone tried to take out a new loan using his PII, the bank or credit bureau would reach out to Dad for verification. Thus, in the world of self-sovereign identity, PII is less valuable and its use is more tightly under Dad's control.

YOUR SISTER IS A WORLD TRAVELLER

Sis works with *Médecins Sans Frontières* offering humanitarian assistance. This brings her to dozens of countries, some of which have non-western values. Sometimes she's been targeted by the authorities, which has put her in jeopardy. She also has occasionally needed to seek treatment in these countries due to the problems that a varying diet causes for her diabetes.

"I'm afraid of losing my passport."

The Problem. Sis was once forced to leave her passport behind when she had to flee a city: she was afraid to return to her lodgings due to the local authority's disagreement with *MSF*. This terrified her, because a passport is expected to be in a traveler's possession when they are traveling in a foreign country. This left her unable to easily leave the country, which she now felt was hostile to her presence. Replacing her passport was both time consuming and logistically challenging. She is horrified by the idea of repeating this experience.

The Solution. Sis has a digital passport stored on a hardware device that acts as a data store. She keeps it attached to her keychain. She can unlock and transmit her passport data using her thumbprint. If she loses her physical passport, she has this backup. Authorities in some countries may accept it themselves, but otherwise, she can use it anywhere to establish her identity to the local embassy by logging into her government's online platform.

"I don't want the police looking at my passport if they stop me."

The Problem. Due to her country of origin, Sis experienced harassment from the police when they were reviewing her passport. She also endured extensive interviews because of the countries she has visited.

The Solution. When Sis enters a country, the border agents issue digital documents (a verifiable credential) approving her legal status in the country for a certain span of time. She adds this to her self-sovereign identity's data store. When she is stopped by the police, she uses her hardware device to selectively disclose only her name and the credential issued by the border agents. The police now know who she is and what her status is; they don't need to know about her country of origin or past travels. The border agents have already verified that information, so she doesn't need to give it to the municipal authorities.

"I worry that I don't have all of my health records with me."

The Problem. Sis has type 1 diabetes and has to ensure her sugar levels remain stable. If she were to have a medical emergency while traveling, she needs the doctors to know the details of her condition, including her current medications and allergies, without having to carry a sheaf of documents.

The Solution. Sis keeps her medical records on her hardware device. Using her self-sovereign identity, she can protect the information or share it when necessary. In addition, the encoded, digital nature of her medical records makes it easy to translate into different languages.

YOUR DAUGHTER IS A RECKLESS SOCIAL MEDIA USER

Daughter has spent her life publishing pictures, tweeting, and posting on social media services such as Facebook and Snapchat. Now that she is going for job interviews, she realizes that all of her photos of holidays and parties and all of her tweets are a bit more public than she would like.

"I don't want to show my employer everything."

The Problem. Daughter is going for a job interview soon and has heard rumors of employers making hiring decisions based on social media profiles. She is concerned over which of her images and tweets will turn up if they access her social media profiles.

The Solution. With self-sovereign identity, Daughter has granular control over who sees what in her social media feeds. When she gives access to potential employers, she gives access to feeds that selectively disclose specific tags.

"I've put something online that I can't take back."

The Problem. Daughter's photo blog features a picture of her in front of a popular storefront very near her home. This photo went viral over the weekend, which brought a huge amount of attention to her online presence. Shortly afterward, she got a creepy email from someone mentioning the store she was at and the city it's in; she's afraid she accidentally revealed too much about herself.

The Solution. Daughter's self-sovereign identity is on her mobile phone, and it signs every picture she takes and stores that signature as part of the image file. This allows her to prove ownership of the photo. After she realizes the picture is problematic, Daughter's robo-attorney sends out a signed takedown request to the social media networks and search engines; most sites will remove the photo since she can prove her ownership of the photo.

"I'm afraid of being doxxed."

The Problem. In recent years, Daughter has been vocal on the issue of presentation of female characters in video games. She just heard about a few friends getting doxxed because of similar comments online. She is afraid that she might be a target of harassment.

The Solution. Daughter's social media platform incorporates many novel features that evolved out of the self-sovereign ecosystem. This enables her to selectively disclose her PII only to people who have received attestations from a select group of friends that she defines. She immediately activates this feature to better control access to her personal information.

YOUR BEST FRIEND IS A CONTENT CREATOR

Best Friend is working in a non-Western country. He's an entrepreneur who regularly vlogs about the local startup scene. Sometimes, his comments are opinionated, which has caused tension with these companies and the local government that supports them. His vlogs are posted to the local social media networks, which are also controlled by that government, but his followers are worldwide, including both local and Western business leaders.

"I don't want my followers to lose access to my published work."

The Problem. The local social media network has a reputation for following the whims of the local government. Sometimes they arbitrarily delete posts that they don't agree with. Best Friend is concerned that when this happens, his followers will see references and citations to his work, but not be able to access the original posts.

The Solution. Best Friend uses his self-sovereign identity to publish all of his videos. They're posted to his data store, a decentralized file storage and delivery system that is accessible through his self-sovereign identity and provably attributable to him. Hyperlinked citations and references connect to this original data source. Even if the content on the local social network is removed, anyone looking at a citation or reference can still find the original content and know that he wrote it — even though it's no longer connected to his social media presence.

"I'm afraid of losing my followers"

The Problem. If Best Friend is sufficiently troublesome, the local government might delete his social media account entirely. This could cost him all the connections and relationships that he's built on the social media network.

The Solution. Best Friend created his social media account using his self-sovereign identity, fundamentally linking them. His western followers tended to do the same, while his local followers only have localized accounts. If his local social media account is deleted, he automatically maintains links to everyone with a self-sovereign identity. Unfortunately, he loses access to all of the followers with local accounts, but his self-sovereign identity's decentralized identifier (DID) was available through his social media account and remains available through any citations and references. Any local follower could choose to link to his self-sovereign identity with this information.

"I don't want to get arrested for what I write."

The Problem. The local government has decided Best Friend is troublesome and actively targets him for a smear and disinformation campaign, designed to get him arrested. They do so by publishing portions of his material that are taken out of context with a negative spin.

The Solution. All of Best Friend's videos are time-stamped and then signed with his self-sovereign identity. He can refute the out-of-context statement by showing the full video, proving that it is his, and demonstrating its origin. The more reputable news agencies only use signed videos of this sort; though the propaganda network continues using the out-of-context video, no one else replicates it.

YOUR NEPHEW RUNS A CONVENIENCE STORE

Nephew has decided to open his first business! However, he wants to do more than just run a simple convenience store: he wants to run a convenience store that's sustainable. He's done a good job of getting it off the ground, but he's a one-man operation, and sometimes details slip through the cracks. He is also thinking about serial entrepreneurship, so he doesn't plan for this to be his last venture.

"I don't want to accidentally sell products that aren't sustainable if I say they are."

The Problem. Nephew is concerned with the claims that various products make about their sustainability and provenance. There have been many recent articles about false claims, and his customers are asking questions that he can't answer. For his brand to stand out, he wants a degree of confidence about the products he's selling.

The Solution. Independent inspectors create verifiable credentials for the authenticity of the sustainable products that Nephew sells in his store. Nephew authenticates these credentials and attests their veracity with his self-sovereign identity. So long as his customers trust him, they no longer need to verify the authenticity of their goods themselves, though they may if they wish.

"I want to be able to get the best value for my business when I sell."

The Problem. Nephew knows that he could open the books of his business to show its profitability and lay out its money flow to potential purchasers. But this information isn't verifiable!

The Solution. Nephew, with the aid of self-sovereign identity, can provide a full-spectrum, well-defined, verifiable suite of business analytics. Every purchase order, credit card sale, inventory item, and bill payment is signed with the business' decentralized identifier (DID), a component of his self-sovereign identity. This provability increases the value of his business.

"I forget to order things sometimes."

The Problem. Because of his lack of staff, Nephew worries about losing track of inventory, which can result in delays of supply that have a negative impact on revenue.

The Solution. Nephew has granted permissions to his smart refrigerator to use the business' DID to initiate and sign purchase orders on his behalf. Because the refrigerator has sensors that track inventory, supplies are reordered automatically. The fridge issues a purchase order signed with the business' DID and the refrigerator's DID, verifying both the authenticity and the origin of the order. This in turn gives his supplier a sense of security that the orders are valid. Milk arrives a day later and is loaded into the drinks cooler.

CONCLUSION

These use cases may be just what you need to convince your dad (or sister or daughter or best friend or nephew) of the importance of self-sovereign identity. You can use them as a library of arguments to bring around people who are interested, respectively, in finance, government, privacy, content, or business.

And, these possibilities are just the tip of the iceberg. Because the adoption of self-sovereign identity is likely to begin in the developed world, the use cases in this paper focused on our own privileged family members. However, self-sovereign identity might be even more useful for marginalized people, who could gain protections that the developed world takes for granted. Refugees could be guaranteed identity when they flee their home state; peoples living in autocratic societies could enjoy new protections; and disadvantaged people could see their playing fields leveled. Self-sovereign identity could radically change the structure of the social contract.

The catch is that we're not there yet. Though some of the arguments in this paper refer to technologies that are already being specified and implemented, others remain mere possibilities. In order to convince dad (and sis and the rest) fully, we need to be able to point not just to our dreams of self-sovereign identity, but also to a concrete reality.

That's where *you* come in. If you're a developer, an engineer, or a software business owner, you can help realize these ideas. This article systematically approaches the problems that might be faced by people using the internet for five broad classes of works, imagines the very real problems they currently experience, and suggests how self-sovereign identity could offer solutions. The following table summarizes many of these possibilities:

Actor	Category	Needs
Dad	Finance	1. Self-sovereign federated logins 2. Biometric logins 3. Validated identity
Sister	Government	1. Digital passport 2. Selective identity disclosure 3. Digital health records
Daughter	Privacy	1. Selective data disclosure 2. Data revocation 3. Automated identity disclosure
Best Friend	Content	1. Self-sovereign content 2. Self-sovereign relationships 3. Validated content
Nephew	Business	1. Verifiable credentials 2. Validated finances 3. Delegated identity

Offering concrete solutions for these use cases could drive adoption of self-sovereign identity. We thus encourage software developers to consider these needs and see if they can make the solutions that fulfill them a reality.

Of course, any new identity system must be built with care, as it could be misused if it's poorly developed. We don't want to increase the attack surfaces on identity, and we definitely don't want to create new honeypots. Keeping the focus on *self-sovereign* identity should put the Internet's next identity system on the right path.

We own our identities.

REFERENCES

Allen, Christopher. "The Path to Self-Sovereign Identity." *Life with Alacrity.* April 25, 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Andrieu, Joe, Frederic Engel, Adam Lake, Moses Ma, Olivier Maas, and Mark Van Der Waal. "Re-Imagining What Users Really Want." *Rebooting the Web of Trust.* September 27, 2017. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2017/blob/master/final-documents/what-users-really-want.pdf.

Berners-Lee, Tim. "A Public Identity." A Public Identity - Design Issues. January 19, 2018.. https://www.w3.org/DesignIssues/PublicIdentity.html.

Casey, Michael. "Blockchain Technology: Redefining Trust for a Global, Digital Economy." *Medium.* June 14, 2016. https://medium.com/mit-media-lab-digital-currency-initiative/blockchain-technology-redefining-trust-for-a-global-digital-economy-1dc869593308.

Broudy, Alex. "How Blockchains and Decentralized ID Solutions Flip the Switch on Privacy." *CryptoDigest.* June 12, 2018. https://cryptodigestnews.com/how-blockchains-and-decentralized-id-solutions-flip-the-switch-on-privacy-63e21e060670.

Pettey, Christy. "The Beginner's Guide to Decentralized Identity." *Smarter With Gartner.* June 28, 2018. . https://www.gartner.com/smarterwithgartner/the-beginners-guide-to-decentralized-identity/.

Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times.* March 17, 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Smolenski, Natalie. "The Evolution of Trust in a Digital Economy." *Scientific American.* Accessed January 2018.https://www.scientificamerican.com/article/the-evolution-of-trust-in-a-digital-economy/.

Stempel, Jonathan. "Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach." *Reuters.* March 08, 2016. https://www.reuters.com/article/us-home-depot-breach-settlement/home-depot-settles-consumer-lawsuit-over-big-2014-data-breach-idUSKCN0WA24Z.

Swamynathan, Yashaswini. "Equifax Reveals Hack That Likely Exposed Data of 143 Million Customers." *Reuters*. September 08, 2017. https://www.reuters.com/article/us-equifax-cyber/equifax-reveals-hack-that-likely-exposed-data-of-143-million-customers-idUSKCN1BI2VK.

Wolff, Josephine. "How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure." *Slate Magazine.* December 21, 2016. https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html.

ADDITIONAL CREDITS

Lead Author: Lucas Parker

Authors: Shannon Appelcline, Kenneth Bok, Peter Scott, and Matthew Wong

Contributors: Pamela Dingle

About Rebooting the Web of Trust

This paper was produced as part of the Rebooting the Web of Trust VII design workshop. On September 26th through 28th, 2018, over 40 tech visionaries came together in Mississauga, Ontario 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.

Leadership Team: Christopher Allen, Joe Andrieu, Kim Hamilton Duffy, Manu Sporny, and Heather Vescent

Gold Sponsors: Civic, Protocol Labs, Sovrin, an anonymous donor

Silver Sponsors: HTC, Microsoft, PTB Ventures, Spherity, Tierion

Community Sponsors: Blockchain Commons, Learning Machine, Legendary Requirements, Purple Tornado, Veres One

Workshop Credits: Christopher Allen (Founder), Joe Andrieu (Producer and Facilitator), Shannon Appelcline (Editor-in-chief), and Claire Rumore (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/rwot7/issues

The next Rebooting the Web of Trust design workshop is scheduled for the week of February 27th to March 1st, 2019. If you'd like to be involved or would like to help sponsor the event, email:

rwot-leadership@googlegroups.com
