NEW AMERICA

May 2019

The Credential Highway

How Self-Sovereign Identity Unlocks Property Rights for the Bottom Billion

Yuliya Panfil & Christopher Mellon

Last edited on May 15, 2019 at 11:32 a.m. EDT

Acknowledgments

The authors would like to thank Amanda Richardson, Amy Regas, Gregory Myers, Frank Pichel and Tim Fella for reviewing this paper, and our colleague Tim Robustelli for his help in reviewing and editing it.

About the Author(s)

Yuliya Panfil is a senior fellow and director of New America's Future of Property Rights program.

Christopher Mellon is a policy analyst with the Future of Property Rights program at New America.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Future of Property Rights

FPR aims to help solve today's property rights challenges by shrinking the gulf between technologists and policymakers. We also strive to preempt emerging land challenges by thinking critically about the paradigms that govern new spaces.

Contents

Executive Summary

Every person in the world has a right to own, rent, or otherwise occupy property. But, billions of people lack documentary proof of their property rights.

Why? Because administrative agencies typically record rights only during major junctures in the life of a property: for example, a first registration, a sale, an inheritance, or an eviction. Understandably, given the high degree of risk involved, administrative agencies require substantial evidence in order to record and provide documentary proof of these major events. The pieces of evidence that administrative agencies require to prove a property claim—let's call them "monument credentials"— may include things like a survey plan, a notarized will, and a state-issued identity card.

This system has two major flaws:

1. **Access**: It may be prohibitively expensive or difficult for some people to produce the monument credentials that administrative agencies seek.

2. **Accuracy**: The evidence that administrative agencies accept may not fully capture the reality on the ground. In other words, there's a gap between reality and documentation.

As a result, land administration systems end up excluding billions of people.

However, the types of events that trigger documentation—which may only happen a handful of times in a property holder's lifetime—are far from the only evidence of property claims. In fact, the reality of our property rights is evidenced by a multitude of small, everyday events: where we sleep at night, where our mail is delivered, the knowledge and memories of our neighbors, or the fact that we paid to put a new roof on our house or a fence around the yard.

The reality of our property rights is evidenced by a multitude of small, everyday events.

Until recently, these everyday events have occurred unrecorded, in the analog world, and beyond the sight of administrative agencies that provide us with property documents. But what if we found a way to harness the evidence of these

everyday events and use it to supplement the small number of monument credentials currently accepted by administrative agencies?

Our lives are becoming increasingly digitized. With the proliferation of smartphones, satellites, and social media platforms, more and more of these small events leave a data trail. Taken together, this data can be used to create a tapestry of new evidence—let's call it a "tapestry credential"—that property holders could use to obtain documentation of their property rights.

But, without a system for turning it into a credential that administrative agencies can trust and use, this data cannot be leveraged by the people to whom it pertains.

This report argues that a digital identity system—specifically, self-sovereign identity (SSI)—is the vehicle for harnessing this wealth of new data in a way that is trustworthy, secure, and privacy-preserving. That is because SSI is the only model of digital identity that is designed to turn people's data trails into credentials under their personal control that can be easily verified by any third party.

Why do the rapid innovations occurring in the identity space have the potential to revolutionize the delivery of property rights? Because, at its most basic, property rights documentation is documentation of identity: the identity of the property holder, the identity of the property itself, and the relational identity between the property and its holder.

When Evidence of Property Rights is Narrowly Defined, Many People are Excluded

Natural Reality and the Administrative State

Administrative agencies often determine the ability of citizens to exercise their rights and privileges. For example, administrative agencies provide us with formal rights to vote, own property, drive cars, and travel internationally. Access to these rights and privileges comes in the form of documentation: my passport allows me to travel, my state-issued ID is proof of my identity, and my deed is proof of my property right.

But how does an administrative agency know who to issue a document to, and under what circumstances?

If an administrative agency were privy to the life story of every citizen, it would be able to determine, based on the totality of a person's life history, which rights and privileges that person qualified for. But because administrative agencies have to interface with millions of citizens and don't know the life story of every person they deal with, they must rely instead on standardized records that capture a few major life events—like births, marriages, etc.—to determine who is eligible for which rights and privileges. This creates a strange gap between natural reality (i.e., the facts of life) and the administrative record of that reality:

- **Natural Reality**: The facts of life.
- **Administrative Record**: Documentation that administrative agencies issue as a proxy for the natural reality.
- **Credential**: A predefined form of evidence that citizens present to the administrative agency in order to prove things about themselves and obtain an administrative record. In other words, a credential is the bridge between natural reality and an administrative record.

For example: The natural reality is that I am over 16 years old and know how to drive. The administrative record is my driver's license. The credentials I presented in order to obtain my driver's license were: my birth certificate, my social security card, and a document certifying successful completion of a driving test.

A property rights example: The natural reality is that John owns and lives in his home. The administrative record of that reality is a title. John obtains a title from a land office by presenting some or all of the following credentials: an ID

card, a survey plan, notarized biographical information forms, signed neighbor attestations, and a proof of property tax payments.

The Problem with Property Credentials

Our natural reality is made up of an infinite number of small facts that together define who we are. But because administrative agencies are not privy to our life stories, they have to rely on proxies that 'prove' facts about us. That means the proxies—lets call them "monument credentials"—must be trustworthy enough that even a small number of them will provide enough proof for an administrative agency to issue documents that provide us important rights—like driver's licenses and property titles—without having ever met us. In the context of property rights, monument credentials include things like a survey plan, a notarized will, or a bank-certified proof of payment.

This system has two major challenges:

1. **Access:** It may be unduly burdensome for some citizens to produce the credentials they need to receive an administrative record of natural realities.

2. **Accuracy:** Administrative records are not necessarily an accurate reflection of the natural reality they are supposed to represent. There are relatively few forms of administrative proofs, leaving a gap between reality and documentation.

An example of the access flaw: When the supporting credentials required by land agencies (e.g. a survey plan and a state-issued ID) are prohibitively expensive or unavailable for citizens to produce.

An example of the accuracy flaw: When administrative records provided by land agencies (e.g. titles) don't accurately reflect the natural reality on the ground (e.g. overlapping use rights, rights of women in the household, transhumant activity, etc.) or don't recognize informal sales.

With either an accuracy or access flaw, the result is that certain citizens are not able to exercise the rights and privileges they are entitled to, either because they are unable to produce the needed credentials or because there is no form of administrative record that can accurately reflect the tenure arrangement taking place on the ground.

To the extent that the access flaw exists, it is disproportionately borne by the most vulnerable communities—those least able to respond to administrative burdens. To the extent that those communities are affected, the result is the loss of rights that are owed to the community.

Opportunities to Bring People into the System Using New Pieces of Evidence

The types of events that trigger documentation—which may only happen a handful of times in a property holder's lifetime—are far from the only evidence of property rights. In fact, the reality of our property rights is evidenced by a multitude of small, everyday events: where we sleep at night, where our mail is delivered, the knowledge and memories of our neighbors, or the fact that we paid to put a new roof on our house or fence around the yard. These small events, in aggregate, form a more accurate picture of reality than is captured by the monument credentials currently used by administrative agencies.

The problem, of course, is that these everyday events have historically occurred in the analog world, outside the purview of administrative agencies that provide us with property documents. But what if we found a way to harness the evidence of these small events and use them to supplement the small number of monument credentials currently accepted by administrative agencies?

Our lives are becoming increasingly digitized. With the proliferation of smartphones, satellites, and social media platforms, more and more of these small events leave a data trail. Taken together, this data can be used to create a tapestry of new evidence—let's call it a "tapestry credential"—that property holders could use to obtain documentation of their property rights.

How Tapestry Credentials can Solve the Access Flaw

To obtain property documents, claimants must provide credentials such as survey plans, identification documents, and notarized forms. The problem is that these credentials are unavailable to many people.

For example, arguably the most important credential a person can have—one that is critical to property documentation—is an identity document. According to the World Bank, however, nearly 1 billion people around the world lack legal IDs.[1] Documents, including land documents, cannot be issued to you if you can't prove who you are.

But, of course, every person has an identity, regardless of whether that identity is documented. Furthermore, everyone has a social identity that they build through their relationships with other people. Where these interactions intersect with the digital world, they leave a record. This record may not be in an administratively recognized format, but it can be used to build evidence over time that can substitute for a traditional identity credential.

Similarly, a survey plan is not the only proof of the location of a property. Parcel boundaries can be seen from satellite imagery, and they can increasingly be corroborated through digital evidence like geotagged photographs, cell phone location data, delivery records, and the like. None of these data points are sufficient to prove property location on their own, but together they create a tapestry credential that could.

The tapestry of information generated through ordinary interactions can serve as a first step onto the credential ladder. As more and more such digital evidence is created, the ladder may become more like a ramp; gradual, continuous progress can be made as evidence accrues.

This idea is already being operationalized in the financial inclusion space, where applicants' social history is being used to help them open bank accounts and derive alternative credit scores.[2]

How Tapestry Credentials can Solve the Accuracy Flaw

In a sense, administrative reality as we know it has a very low resolution. This should be intuitive to anyone living in a high-tech society. The government agencies with which we interact have a few important and very well-validated pieces of information about us. But Facebook and Google possess far more data points gleaned through our daily activities in a wider variety of domains, many of which the government has no right or reason to look into. These platforms know where we go and when; they may know why and with whom. They know what we read and what we buy.

Some of this information bears directly on property rights and the credentials needed to access them. Location data is clearly in that category, as are many financial transactions, including deliveries and payment of property-related expenses like utilities and maintenance costs.

In places where property transactions occur informally, property records in the registry will quickly fall out of date while digital trails continue to capture evidence of the reality—revealing that a new person is living at the property, making upgrades to it, etc.

To give another example, in places with overlapping property rights, administrative systems often only record one or two of those rights—for example freehold ownership or long-term occupancy. This gives an incomplete picture of the occupancy and use of the land, and it also means that people with other rights to that property are locked out from administrative proof of those rights. But digital evidence can reveal other sorts of relationships, like sharecropping or seasonal occupancy.

And in places where women are still locked out of property systems, administrative records reveal only the ownership of the male head of household. Yet women make home improvement purchases, even where they have no formal property right. Operationalizing the digital trail related with these purchases promises to put women on the property map. This not only helps to solve the accuracy flaw, but also the access flaw because it provides a base of evidence for providing documents to people whose rights are not currently recognized.

The Challenges of Using Tapestry Credentials for Property Rights

And yet, there are several very real barriers to using tapestry credentials to solve the accuracy and access problems in the realm of property rights. If all of this data is to be used as evidence, then people need to be able to easily collect and share the data they generate, and administrators must be able to trust it.

From the administrative perspective, several things must be known in order to trust the data. An administrator must be able to establish who created the data, who is presenting it, and if the person presenting it is the person the data is about.

Under the current monument credential model, data is trusted because it is created by trusted parties. The location and boundaries of a property, for example, are established by a surveyor whose job is to supply reliable information. The identity of a person signing off on a property transfer is verified by a notary, who endorses the signed document with a stamp.

The tapestry credential paradigm aims to move away from this model by admitting evidence produced by the widest possible number of interactions, the vast majority of which will not involve a person trusted by the registry, like a surveyor or notary. This requires a new way of thinking about trust.

If location data is generated by a mobile phone, how do you know who owns that phone? How do you know that the owner was the one using it at the time the data was generated? If a message is posted on a social media account, how do you know who controls it?

The events that generate this data involve multiple parties (even if, on their face, interactions like text messages and mobile money transfers appear to only involve two). As people build their social identities through digital communication tools, their interactions are intermediated by networked computers—sensors that keep a record of events in the form of data. In order to establish the origin of that data, the parties in these interactions must be identified.

A Tapestry Credential System for Land Administration: Making it Work Through Self-Sovereign Identity

So what are the characteristics of an identity system for land administration, one that would make it as easy as possible to create tapestry credentials to establish property claims, interact with the land registry, and access land-related financial services?

- It must be easy to establish unique, trustworthy identities for people and things.
- It must allow people to remotely assert facts about themselves and their property.
- It must be designed to maximise user privacy and control.
- It must allow maximum flexibility to create, share, and verify credentials.

We propose that an emerging type of digital identity system, called self-sovereign identity, can operationalize these four requirements.

In the following subsections, we explain:

- Why a solution emerging from the identity space is appropriate for land administration;
- What self-sovereign identity is, and how it differs from the form of digital identity most of us are familiar with; and
- How a self-sovereign identity-based system could allow people to use tapestry credentials in order to document their property rights.

Why a Digital Identity Solution is Appropriate for Land Administration

How do we create a system that satisfies the four criteria above? The answer may come from the digital identity community, which has long been grappling with the problem of allowing large numbers of people to assert information about themselves in a trustworthy and inclusive way.

Perhaps it is unsurprising that a concept developed for identity can offer a solution for property rights. That's because, at its most basic, property rights documentation is the documentation of identity: the identity of the property holder (the "who"); the identity of the property itself (the "where"); and the relational identity between the property and its holder (the "what").

Answering the first question—**who?**—depends almost exclusively on having an appropriate identity system. While every person, by virtue of their existence, has a unique personal identity, whether that person has identity documentation—and whether that documentation is trusted—is a different story.

The second question—"**where** is the property?"—can also be understood in terms of identity. Land and buildings are quite similar to people in that they have a unique identity that is represented in a system by means of attributes. The main difference is in the type of attributes. Real or immovable, property is identifiable by its location in addition to other distinguishing characteristics.

The final question is the **what**. What sort of right does a specific person have in a specific property? This question can be thought of in terms of the relational identity between the person and the property.

What is Self-Sovereign Identity?

More than a single technology, self-sovereign identity is a new paradigm for designing digital identity systems. SSI abides by a set of core principles introduced by Christopher Allen, who coined the term in his seminal essay, "The Path to Self-Sovereign Identity."[3]

→ THE TEN PRINCIPLES OF SELF-SOVEREIGN IDENTITY

1) Existence. Users must have an independent existence.

2) Control. Users must control their identities.

3) Access. Users must have access to their own data.

4) Transparency. Systems and algorithms must be transparent.

5) Persistence. Identities must be long-lived.

6) Portability. Information and services about identity must be transportable.

7) Interoperability. Identities should be as widely usable as possible.

8) Consent. Users must agree to the use of their identity.

9) Minimalization. Disclosure of claims must be minimized.

10) Protection. The rights of users must be protected

SSI is designed to make identity in the digital world function more like identity in the physical world, in which every person has a unique and persistent identity which is represented to others by means of both their physical attributes and a collection of credentials attested to by various external sources of authority. These credentials are stored and controlled by the identity holder—typically in a digital wallet—and presented to different people for different reasons at the identity holder's discretion. The person to whom the credential is presented verifies it without checking with the issuer of the credential. Crucially, the identity holder controls what information to present based on the environment, trust level, and type of interaction. Moreover, their fundamental identity persists even though the credentials by which it is represented may change over time. While credentials can expire or be revoked by their issuers, there is no central authority with the power to revoke a user's identity. The leading SSI solutions leverage blockchain to provide users with a persistent and secure digital identity that cannot be revoked, altered, or accessed without their explicit permission.

A key component of SSI is the **verifiable credential** standard.[4] A verifiable credential is a tamper-resistant, privacy-preserving, and digitally signed

credential with clear authorship and provided by a known and trusted entity. The identity holder can use their verifiable credentials to access many different systems and services without a third party tracking the services the identity holder uses.

For example: Bob wants to open a bank account, and the bank asks for Bob's proof of address as part of its due diligence process. Bob does not have a formal address, however he does have a mobile phone. Bob asks his telecom company to issue him a location history as a verifiable credential that he can present to the bank (and to whoever else may need it in the future). Bob stores this location history credential in his digital wallet, along with various other credentials, and the bank can request access to this credential to verify Bob's address.

In this example, the verifiable credential is provided by a known and trusted entity (the telecom), digitally signed by the telecom, and stored by Bob in a tamper-resistant location—his digital wallet.

Furthermore, because the location credential is cryptographically signed by the issuer, the bank doesn't need to contact the telecom to verify the information; checking the credential against the telecom's public key is proof enough. The public key is a string of bits that is mathematically linked to a corresponding string of bits called a private key. Data that is encrypted with one key can only be decrypted with the other. As the names suggest, private keys are kept secret while public keys are accessible to everyone. The verifier can use the telecom's public key to mathematically prove that the credential was signed by the private key known only to the telecom. Similarly, the verifier can check that the credential was issued to Bob and is being presented by Bob.

Cryptographic techniques called "zero-knowledge proofs" (ZKPs) can be used to prove possession of a credential without actually revealing the credential itself, which helps to preserve the privacy of sensitive information. For example, Bob can present a proof of address derived from his location data without sharing the location data itself.

Although the concepts behind SSI have existed for decades, actual implementation was technically infeasible until recently. The arrival of blockchain and the advancement of biometrics have brought SSI from concept to reality. Blockchain enables decentralization of the public key infrastructure. This allows anyone with access to a smartphone to create a digital identity that cannot be revoked by a centralized authority, and to issue and verify credentials. Biometry can be used to establish a unique core identity and to guarantee that, when data is accessed or shared, the real identity holder is the one doing so.

→ HOW IS SELF-SOVEREIGN IDENTITY AN IMPROVEMENT ON EXISTING FORMS OF DIGITAL ID?

SSI has several advantages over existing forms of digital ID. Most digital identities today take the form of accounts that can only be used to access specific services from a specific provider. Other forms of identity, like Facebook and Google accounts, can be used for a wider, but still very limited range of purposes. Moreover, these accounts are entirely controlled by the service provider and can be revoked.

National identity schemes often create the opposite problem, and are adopted for an incredibly wide range of purposes for which they were not originally designed, which creates serious surveillance and privacy risks for their users. India's Aadhaar is the greatest example of this, though social security numbers in the United States also fit this pattern.[5]

SSI, by contrast, provides a single digital identity that is controlled by the user and can be used to access multiple different services. However, SSI is also built to maximize user privacy and control over personal information, giving users a digital identity that is anonymous where appropriate and allowing them to assert their legal identities when necessary.

How Can SSI Help Solve the Property Documentation Problem?

At the beginning of section three, we introduced four requirements for an identity system to support the use of tapestry credentials. Now, having introduced SSI, we can explore in greater detail how its features align with those requirements.

Establishing Unique, Trustworthy Identities for People and Things

In a world where smartphone penetration is increasing rapidly,[6] SSI is becoming an accessible way for people to obtain unique digital identities. The administrative form of a government-issued personal ID is often a number that serves as a unique identifier and a combination of characteristics, such as name, address, age, etc. Each of these characteristics requires some form of evidence in order to be recorded for identification purposes, and there are necessarily a limited number of trusted supporting credentials that the identity issuer can accept. In the total absence of supporting credentials, identity can be established

through a social process in which members of a community identify one another in a relational way before an identity is issued.

SSI reverses this process, allowing people to establish a digital identity and build a relational ID around it. People are able to create their own unique identities on enrollment and build credentials from multiple sources around that identity over time. If a person has a valid state-issued identity document, the appropriate government agency can reissue that document digitally as a verifiable credential. That verifiable credential is a very useful thing to have, as it provides a robust digital identity for future interactions. In the absence of a state-issued identity document, SSI provides a way to build a progressively more trustworthy identity. The identities are trustworthy because their attributes and interactions are cryptographically verifiable.

SSIs can also be generated for objects, including properties and sensors that need to share the data they collect in a secure format. For a land administration system to make use of an ever-increasing amount of sensor-derived data, we have to know and trust the identities of the sensors themselves. The vast majority of entities sharing information on computer networks will be "Internet of Things" devices—sensors connected to the internet that collect and share data. All of these devices will need digital identities to keep track of these data flows. For our purposes, an internet-connected sensor needs a public/private key pair that it can use to authenticate to other devices with which it interacts and to sign data that it generates.[7] In the short term, SSI can enable verifiable location proofs from peer-to-peer communication between devices.

In the more distant future, more data will also be generated by devices attached to properties in the form of things like thermostats, smart locks, and utility meters. In that case, the property itself would have an identity to gather and manage this data.

Allowing People to Remotely Assert Facts About Themselves and Their Property in a Way that is Trusted by Administrative Agencies

A government agency trying to verify information must answer two questions: What is the identity of the person making the claim, and what is the origin of the evidence supporting the claim? In other words, the verifier must be able to tie all of the credential data to a single, legal person, and believe that the data is legitimate.

SSI helps the government answer the first question with the help of biometrics, which allow intrinsic characteristics of the individual to be extended into the digital world. When we go in person to renew a driver's license or to have a document notarized, we are undergoing a series of implicit identity checks that may not be obvious. The first and most important of these is biometric. Human beings are exceptionally sophisticated "sensors" when it comes to recognizing other living humans and their physical features. This check is accompanied by

the submission of documents and, taken together, these checks furnish proof of identity. An SSI-based system must be able to replicate this in-person biometric check. Luckily, as smartphones incorporate increasingly sophisticated biometric sensors, like fingerprint readers and facial recognition software, this is becoming an increasingly easy problem to solve.

Biometrics can be used in a variety of ways, and this is reflected in the diverse approaches taken by current SSI platforms. Biometric profiles can be used to generate a person's identifier in the system, which allows them to recover their account if they lose access to it. In some platforms, such profiles can also be used to prevent a single user from creating multiple accounts. Most commonly, biometrics are used to access and control the digital wallet on a person's phone.

In answer to the second question, once there is a biometric tie between the SSI wallet and the wallet holder, there is a need to tie the credentials in the wallet to the wallet holder's core identity. SSI platforms allow credentials to be linked cryptographically to the wallet holder's core identity so that they cannot be used by anyone else.

Maximizing User Privacy and Control

A drawback of the tapestry credential model is that it relies on a large trove of personal data, which in aggregate is much more revealing than a small number of monument credentials. As citizens begin to collect and deploy tapestry credentials, they would therefore want assurances that they alone control who sees which pieces of data and when.

One important way in which SSI can help to ensure user privacy is by allowing different identifiers to be used for different relationships to prevent observers from being able to piece together information about the user. For example, an identity holder would use one identifier with the bank, a different one with their phone provider, and a third with the land agency. However, all credentials gathered through these interactions are linked to the user's core identity in such a way that they can be verified when used in new relationships.

This is in stark contrast to other popular forms of digital identity, which are often designed to collect as much information about the user as can be extracted from that person's activities. In fact, it can be difficult for the identity holder to prevent it from happening. A Facebook profile, for example, can fairly be defined as a digital identity consisting of all of the data Facebook has attached to that user profile, much of it without the user's knowledge or consent. SSI is a way to collect many data points from multiple sources around a single identity while still under the data subject's control.

Verifiers can request whatever credentials they need from a user, but they cannot see them unless that person consents to share them. In addition, a user can share only the relevant part of a credential to minimize the exposure of personal

information. When a physical ID card is presented, it allows the verifier to see the subjects name, address, date of birth, etc. With SSI, it is possible to mask sensitive information that is not necessary for the transaction taking place, such as the gender of the claimant.

A user's identity data is stored securely on their smartphone and/or in the cloud. In addition, self-sovereign identities can't be revoked by any external authority and are designed to persist as long as the holders want to retain them.

Maximizing Flexibility to Create, Share, and Verify Credentials

A tapestry credential system hinges on the ability to gather pieces of evidence from the greatest possible number of sources, while at the same time trusting this evidence to be legitimate. Because every participant in an SSI network can issue and verify credentials, there is tremendous flexibility to build an identity based on social validation. In other words, trust can be derived from a wide network of interactions rather than the authority of a single entity like a government.

In order for this data to function as a credential, it must be trustworthy in two respects. First, the data must have integrity, meaning that it can be proven that it has not been altered in any way. Second, the data must have a verifiable origin, or provenance. This is accomplished through the use of digital signatures, which can be checked to verify that the data was issued by the right authority to the person presenting it as a credential. Digital signatures create a chain of custody for information. In order to turn phone location data into a credential, for example, a mobile service provider must have an ID with which it can sign a location claim, and the phone user to whom it is issued must countersign it. Verifiable credentials will usually come from trusted sources, but everyone with an SSI has a key pair that they can use to sign credentials, and their public key can be looked up to verify the signature. In many cases, this will not be useful because the individuals won't be trusted to vouch for certain kinds of valuable information in the way that a bank or telecom company can. However, with respect to land claims, the ability for ordinary people to make assertions in such a secure and auditable format can certainly be useful. Neighbors with verified addresses could sign off on a property claim.

From the perspective of a government agency that needs to verify property claims, such a system provides access to many new forms of trustworthy evidence. The agency's role is to decide what combination of credentials is sufficient to establish a claim, request them, and verify them. Once a property right has been recognized, it can itself be issued to the property holder as a verifiable credential, which in turn can be used to apply for a loan, hook up to utilities, or provide a proof of address—just like in a traditional property documentation system.

Conclusion

We have argued that SSI is the best type of digital identity system for property rights, primarily because it is a powerful system for issuing and sharing new kinds of credentials. An interesting consequence of this argument is that the ideal identity system for land administration would not be designed specifically for land administration purposes. The overwhelming majority of the credentials which we envision to be useful—for example, location data, purchase histories, or neighbor attestations—are not being created specifically for the purpose of obtaining property documentation. That's a great thing, because it means that citizens can accede to the rights and privileges the are owed to them simply because they live their lives, and not by jumping through hoops to prove facts about themselves. It also means that citizens can use these same credentials for a variety of other purposes: for example to secure a loan, to obtain a passport, or to qualify for farm subsidies.

So how does a tapestry credential system become operational? The success of tapestry credentials is predicated upon the existence of an ecosystem of players who are willing to collect, issue, and accept these credentials.

Third parties that collect data about us—like Google, Facebook and MPesa—must be willing to issue verifiable credentials that citizens can use for their own purposes. In order for everyone to participate, there must be common, open identity standards. We also must invest in developing public infrastructure for registering and looking up identifiers, like a Domain Name System for identities.[8] The Decentralized Identity Foundation and the Sovrin Foundation have been leaders in these efforts. In addition to that public infrastructure, individual users need apps that allow them to store and share their identity information.

The system also depends upon the willingness of administrative agencies to amend their documentation standards to accept new forms of evidence. That means administrative agencies must believe that tapestry credentials are a suitable substitute for monument credentials.

On this last point, there is hope. Governments often rely on alternative forms of evidence when standard forms of evidence are unavailable. For example, the Pinheiro Principles, which govern property restitution for refugees, allow refugees to use a vast array of data to prove their property claims.[9] As another example, after Hurricane Maria devastated Puerto Rico in 2017, the U.S. Federal Emergency Management Agency began accepting sworn affidavits of property ownership, in lieu of title documents, to process aid for Puerto Ricans.[10]

From the perspective of the land administrator, the greatest challenge is figuring out what the new rules and standards of evidence should be. It might be wise to start by accepting attestations and credentials from trusted parties like NGOs

and banks. This would be a similar approach to that taken by alternative credit score systems developed in the financial inclusion field.

Another significant challenge will be distinguishing occupation from ownership. It is possible to imagine a scenario in which a long-term renter, or a squatter, can amass enough occupation-based credentials to fraudulently assert an ownership claim. This is a question administrative agencies will have to grapple with.

And finally, users must believe that collecting, organizing, and storing tapestry credentials is a useful exercise for unlocking services, and they must also be comfortable knowing that they have full control over their credentials.

The widespread adoption of SSI promises a wide range of benefits for governments, citizens, and businesses.

For the average person, the most noticeable benefit would be the convenience of no longer having to manage a bunch of different usernames and passwords. More importantly, the privacy and security features of SSI largely mitigate the risk of identity theft. Even if a person's credentials were somehow stolen, the thief could not use them. And if the identifier used to connect to a service were to be compromised, a new one could easily be generated.

Businesses and NGOs would have to handle and store far less personally identifiable information, reducing the burden of data management and compliance. Decentralizing storage of personally identifiable information to data subjects would make massive data leaks like the 2017 Equifax hack[11]—which exposed the social security numbers, names, addresses, and birthdates of more than 140 million people—impossible. Banks could save big on Know Your Customer and Anti-Money Laundering compliance.

SSI would also provide a new way to govern online spaces. Social media platforms could eliminate bots by requiring all users to verify that they are real people. This could be done on an automated basis by using ZKPs so that users could remain anonymous.

Governments would have access to an identity solution they could use across services without having to maintain the infrastructure or provide people with any kind of hardware. Identity documents could be issued as verifiable credentials, making them much more secure and fraud resistant. Strong biometry could allow more services, such as voting, to be accessed remotely.

Governments can encourage the growth of the tapestry credential ecosystem in several ways. One is to begin exploring the use of SSI across a variety of citizen services, from health services to voting. Anchoring SSI to important citizen services will boost user adoption and encourage more governments, businesses, and NGOs to participate. The adoption of SSI for government services should be accompanied by privacy legislation guaranteeing the rights of citizens to limit

disclosure of their private data. Storing data in a privacy-preserving platform won't help if verifiers, including government agencies, banks, and potential employers, can require people to disclose more information about themselves than is necessary. Some governments have already started screening the social media accounts of travelers at border crossings.[12] They must not be able to make the same demand of people's SSI wallets.

Beyond expanding access to property credentials, SSI can help build far more resilient and transparent land registries. Documents issued as digitally signed credentials kept in distributed storage would be extremely resilient and difficult to refute. If proof of property rights were to be issued in this way, it would give each property user proof that the government had acknowledged their claim at the time of issue. The destruction of the registry, or attempts by the government to corrupt the record, would not be able to destroy this evidence, which could be verified by any third party against the public key of the registry. This would make registries substantially more resistant to natural disasters and make land restitution and compensation for refugees and internally displaced persons much simpler.

The system we have described is ambitious. It depends on a paradigmatic shift in the way that administrative agencies look at property rights. And yet, it feels inevitable. Global smartphone penetration already stands at 37 percent, up from 20 percent just five years ago.[13] The launch of global broadband internet schemes from OneWeb,[14] Amazon,[15] and SpaceX[16] will likely further increase smartphone penetration over the coming decade. In recent years, industries from finance to education to health care have begun exploring new ways to allow people to assert facts about themselves and reap the rights they are entitled to but have not been able to access.[17]

As the world moves online, we increasingly focus on the threat of our digital trails being used against us; the specter of privacy invasion, surveillance and identity theft is everywhere. But let's not forget that this abundance of new data can be used for good. If we learn to take control of our information trails, we can deploy them towards transparency and access, particularly for the most vulnerable.

Notes

1 "ID4D Data: Global Identification Challenge by the Numbers," World Bank, accessed May 7, 2019, http://id4d.worldbank.org/global-dataset.

2 Catherine Cheney, "How alternative credit scoring is transforming lending in the developing world," *Dev ex*, September 8, 2016, https://www.devex.com/news/how-alternative-credit-scoring-is-transforming-lending-in-the-developing-world-88487, Steven Melendez, "Now wanted by big credit bureaus like Equifax: Your alternative data," *Fast Company*, April 6, 2019, https://www.fastcompany.com/90318224/now-wanted-by-equifax-and-other-credit-bureaus-your-alternative-data

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

4 Verifiable Credentials Data Model 1.0. Manu Sporny; Grant Noble; Daniel C. Burnett; Dave Longley. Verifiable Claims Working Group. W3C Candidate Recommendation 28 March 2019. URL: https://www.w3.org/TR/verifiable-claims-data-model/

5 Siddharthya Roy, "Aadhaar: India's Flawed Biometric Database," *Diplomat*, March 06, 2018, https://thediplomat.com/2018/03/aadhaar-indias-flawed-biometric-database/

6 Pew Research Center, February 2019, "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally," https://www.pewglobal.org/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

7 "What is IoT PKI?," Thales Security, accessed May 8, 2019, https://www.thalesesecurity.com/faq/internet-things-iot/what-iot-pki

8 Sovrin Foundation, "Sovrin Network Expands Global Reach," Jan. 22, 2019, https://sovrin.org/sovrin-network-expands-global-reach/

9 UN Sub-Commission on the Promotion and Protection of Human Rights, Principles on Housing and Property Restitution for Refugees and Displaced Persons, 28 June 2005, E/CN.4/Sub.2/2005/17, https://www.unhcr.org/en-us/protection/idps/50f94d849/principles-housing-property-restitution-refugees-displaced-persons-pinheiro.html

10 FEMA, "FEMA Provides Alternatives for Verifying Proof of Ownership in Puerto Rico," Guaynabo, Puerto Rico, no. 128, March 10, 2018, https://www.fema.gov/news-release/2018/03/10/fema-provides-alternatives-verifying-proof-ownership-puerto-rico

11 Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *New York Times*, Sept. 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

12 Sewell Chan, "14 Million Visitors to U.S. Face Social Media Screening," *New York Times*, March 30, 2018, https://www.nytimes.com/2018/03/30/world/americas/travelers-visa-social-media.html

13 EMarketer, Smartphone user penetration as percentage of total global population from 2014 to 2021, December 2017, Statista, retrieved at: https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/

14 Caleb Henry, "OneWeb raises $1.25 billion from returning investors," *Space News*, March 18, 2019, https://spacenews.com/oneweb-raises-1-25-billion-from-returning-investors/

15 Orion Rummler, "Amazon to launch 3,236 satellites into orbit for global broadband project," *Axi os*, Apr 4, 2019, https://www.axios.com/amazons-space-project-global-broadband-project-kuiper-7c81b6f8-1425-4f63-97ad-5a3a4358ce25.html

16 Loren Grush, "FCC approves SpaceX's plan to launch more than 7,000 internet-beaming satellites,' *The Verge*, Nov 15, 2018, https://www.theverge.com/2018/11/15/18096943/spacex-fcc-starlink-satellites-approval-constellation-internet-from-space

17 Peter Greene, "Education Micro-Credentials 101: Why Do We Need Badges?, *Forbes*, Feb 16, 2019, https://www.forbes.com/sites/petergreene/2019/02/16/education-micro-credentials-101-why-do-we-need-badges/#349c8f8e2419

NEW AMERICA

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America's work, or include our content in derivative works, under the following conditions:

• **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.