NEW AMERICA

October 2018

The Nail Finds a Hammer

Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World

Michael Graglia, Christopher Mellon, & Tim Robustelli

Last edited on October 17, 2018 at 4:01 p.m. EDT

Acknowledgments

The authors would like to thank the following individuals for their time and valuable insights: Dr. Sari Stenfors, who sent us on this identity journey; Bob Reid, Brad Witteman, and Mike Kail of Everest; Drummond Reed, Elizabeth Renieris, James Monaghan, Tyler Ruff, and the rest of the Evernym team; Robby Greenfield and Paul Kohlhaas of ConsenSys; Rouven Heck and Alice Nawfal of uPort; Titus Capilnean of Civic; Arjun Raman of Mooti; Paige Nicol of Omidyar Network; Peter Simpson of iRespond; John Jordan of the Government of British Columbia; Chris Worman of TechSoup; Shailee Adinolfi; and Kaliya Young, "the Identity Woman."

The majority of the insights here are to their credit, any errors or omissions are entirely the fault of the authors.

About the Author(s)

Michael Graglia is the director of the Future of Property Rights program at New America.

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

Tim Robustelli is a graduate of the MA Program in International Relations at NYU. He is part of 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

The Future of Property Rights initiative engages with policy makers, technologists, academics, civil society, and jurisdictions, as well as the property rights formalization community of practice. Property rights formalization is a powerful tool for creating wealth, opportunity, and security. A number of recent technology developments and advancements greatly reduce the time, cost, and complexity of property rights formalization. As a result, there are many ripe opportunities to apply this policy solution. Our role is to highlight these opportunities, expand the conversation and facilitate instances of property rights formalization improving lives.

Contents

Introduction

Why We Wrote This Report

Section 1: SSI, Registries, and Land Use Cases

The Case for Self-Sovereign Identity

- The Problems With Identity Today
- The Evolution of Digital Identity
- Creation and Use of a Self-Sovereign Identity
- Why the Time for Self-Sovereign Identity Has Come

Registries and Self-Sovereign Identity

- Registries and Society
- The Challenge of Identity Within Registries
- Self-Sovereign Identity and Asset Registries

Digital Identity and Land Use Cases

- Increased Efficiency in Real Estate Markets
- Property Rights in Post-Conflict Environments
- Natural Disaster Resilience
- Women's Land Rights

Contents Cont'd

Section 2: Three Solutions Through Ten Principles

The Principles of Self-Sovereign Identity

Three Self-Sovereign Identity Platforms to Watch

- Everest
- Evernym
- uPort
- These Three Firms Within the Digital Identity Space

Exploring Three Platforms Through the Principles

1. Inclusion - Identity should be available to all
2. Control - Users must control their own identities
3. Access - Users must have access to their own data
4. Transparency - Systems and governance must be transparent
5. Persistence - Identities must be long-lived
6. Portability - Identity information and services must be transportable
7. Interoperability - Identities should be as widely usable as possible
8. Consent - Users must agree to the use of their identity or data
9. Minimization - Disclosure of identity information must be minimized
10. Protection - Users' right to privacy must be protected

Introduction

Our interest in identity systems was an inevitable outgrowth of our earlier work on blockchain-based[1] land registries.[2] Property registries, which at the simplest level are ledgers of who has which rights to which asset, require a very secure and reliable means of identifying both people and properties. In the course of investigating solutions to that problem, we began to appreciate the broader challenges of digital identity and its role in international development. And the more we learned about digital identity, the more convinced we became of the need for self-sovereign identity, or SSI. This model, and the underlying principles of identity which it incorporates, will be described in detail in this paper.

We believe that the great potential of SSI is that it can 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 wallet—and presented to different people for different reasons at the identity holder's discretion. 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.

The digital incarnation of this model has many benefits, including both greatly improved privacy and security, and the ability to create more trustworthy online spaces. Social media and news sites, for example, might limit participation to users with verified identities, excluding bots and impersonators.

The need for identification in the physical world varies based on location and social context. We expect to walk in relative anonymity down a busy city street, but will show a driver's license to enter a bar, and both a driver's license and a birth certificate to apply for a passport. There are different levels of ID and supporting documents required for each activity. But in each case, access to personal information is controlled by the user who may choose whether or not to share it.

Self-sovereign identity gives users complete control of their own identities and related personal data, which sits encrypted in distributed storage instead of being stored by a third party in a central database. In older, "federated identity" models, a single account—a Google account, for example—might be used to log in to a number of third-party sites, like news sites or social media platforms. But in this model a third party brokers all of these ID transactions, meaning that in exchange for the convenience of having to remember fewer passwords, the user must sacrifice a degree of privacy.

A real world equivalent would be having to ask the state to share a copy of your driver's license with the bar every time you wanted to prove that you were over the age of 21. SSI, in contrast, gives the user a portable, digital credential (like a driver's license or some other document that proves your age), the authenticity of which can be securely validated via cryptography without the recipient having to check with the authority that issued it. This means that while the credential can be used to access many different sites and services, there is no third-party broker to track the services to which the user is authenticating. Furthermore, cryptographic techniques called "zero-knowledge proofs" (ZKPs) can be used to prove possession of a credential without revealing the credential itself. This makes it possible, for example, for users to prove that they are over the age of 21 without having to share their actual birth dates, which are both sensitive information and irrelevant to a binary, yes-or-no ID transaction.

Although the concepts behind SSI have existed for over a decade, actually implementing them was, until recently, technically infeasible. The arrival of blockchain and the continuous advancement of biometrics have brought SSI from concept to reality. Blockchain allows for distributed data storage and peer-to-peer transactions, both of which are helpful for a system that requires the users to control data instead of having it under the control of a centralized authority. Similarly, biometrics is critical for enabling SSI, as it allows intrinsic characteristics of the individual to be extended into the digital world.[3] Biometric capabilities are becoming increasingly common in smartphones, including fingerprint readers, facial recognition, and iris scanners.

The ability to securely tie a digital identity to a unique, living person through biometry is powerful. When paired with "a transparent, immutable, reliable and auditable way to address the seamless and secure exchange of cryptographic keys,"[4] it becomes extremely compelling. With the recent emergence of blockchain the SSI community finally found a secure infrastructure for managing keys and attestations in a way that is both public and decentralized. Skeptics have sometimes described blockchain as a hammer looking for nails. Blockchain for SSI is just the opposite; not a case of a hammer looking for nails, but of a nail finding its hammer.

Why We Wrote This Report

Though we live in a world that is increasingly digital, the benefits of the tech revolution have not been evenly shared. In the words of science fiction author William Gibson, "the future is already here — it's just not very evenly distributed."[5] Policymakers and international development professionals must take this as a challenge. Ensuring that the positive impact of emerging technology is extended to the less fortunate is a daunting task, and it is not always obvious where to begin. But sometimes it is. Digital identity is one such case.

Identity is widely recognized as both a crucial tool and a pressing need in international development. When the Sustainable Development Goals were announced in September 2015, Goal 16.9 explicitly targeted "providing legal identity for all" by 2030.[6] The development community has recognized that connecting people efficiently and securely to essential services requires a robust identity solution. As systems and services increasingly become digitized, so must identity. Already, the Identification For Development (ID4D) initiative at the World Bank is funding a set of initiatives in more than 20 developing countries to improve digital identity systems.[7]

But what is the optimal approach to digital identity? Digital identity platforms offer efficiency, transparency, convenience, and inclusion. Of course, if designed poorly, they can also create or exacerbate privacy and data security challenges. The dangers of centralized and insecure storage of personal data have been well illustrated by recent events—notably the Facebook-Cambridge Analytica scandal,[8] the Equifax data breach,[9] the ongoing challenges facing the Aadhaar system in India,[10] and the most recent Facebook hack.[11]

Alan Gelb and Anna Diofasi Metz of the Center for Global Development published *Identification Revolution: Can Digital ID Be Harnessed for Development?*[12] in January 2018. They review the case for digital identity, highlight the increasing importance in developing economies and examine current case studies such as Aadhar. They "conclude that digital ID has the power to do both tremendous good and to inflict serious harm depending on how it is used."[13] We agree completely and do not intend to repeat nor review their exceptional work here. Instead, we look to the next evolutionary stage of digital identity, which we believe is self-sovereign identity. We expect that SSI will be widely adopted in the coming years as it addresses the shortcomings of centralized identity systems.

The report has two sections. The first section is relatively non-technical and accessible: we describe SSI and its advantages; we discuss registries, broadly highlighting their role in society; and, we look at four areas in which we believe SSI can have a positive impact on land administration.

The second section assumes that the first section has succeeded in arousing the uninitiated reader's curiosity about SSI. The curious reader must also be patient; our attempts at brevity resulted in an unacceptable density of jargon and so were abandoned. The second section has three parts: We review ten broad principles of SSI that have been in use for some time; we describe three emerging solutions from **Everest**, **Evernym**, and **uPort**, companies that have invested in SSI and should be taken seriously; and, we look at each firm through the lens of the set of ten principles previously described. This analysis does not imply our endorsement of these three. There are many companies competing in this rapidly growing space. Instead, by exploring three solutions which are both influential and markedly different along various axes, we hope to make clear to the reader the breadth of what is possible and the options they can explore.

Disclaimer: The week of final edits on this paper was punctuated, almost daily, by the release of a major publication about digital identity and/or SSI. This paper is neither definitive nor exhaustive. Instead, we intend it to be a useful tool for policy makers to learn about an emerging technology we see as inevitable. The only thing of which we can be certain is that by the time we send it to print, parts of it will have become outdated. This is a frustration familiar to anyone who analyzes emerging technology. Our hope is that even though our citations and examples may age quickly, some of the work here will be useful and stand the test of time.

Section 1: SSI, Registries, and Land Use Cases

This section is relatively non-technical and intended to be accessible. First, we describe and make the case for SSI. Second, we discuss registries broadly, highlighting their role in society. Third, we look at four use cases regarding land registries where we believe SSI can have a positive impact.

The Case for Self-Sovereign Identity

The Problems With Identity Today

The way that identity and personal data are handled is fundamentally broken. We see at least four issues with how identity and personal data are managed today. Societally, we lack a coherent approach to regulating the handling of personal data. Users share and generate far too much data—both personally identifiable information (PII)[14] and metadata, or "data exhaust"—without a way to manage it. Private companies, by storing an increasing amount of PII, are taking on an increasing level of risk. Solution architects are recreating the wheel, instead of flying over the treacherous terrain we have just described.

Society: Data does not have to be property to be protected. Elizabeth Renieris and Dazza Greenwood recently argued that treating data as property may be an insufficient legal framework for protecting our digital identities. Instead of trying to secure our privacy by applying property law to personal data, they suggest that some sensitive information may qualify for protection under human rights law. As such, they point out:

> constitutional and international human rights laws protect our personhood, they also protect things that are property-like or exhibit property-like characteristics. The Fourth Amendment of the U.S. Constitution provides "the right of the people to be secure in their persons" but also their "houses, papers, and effects."[15]

The implications of this are significant and we encourage the reader to consider their work. Simply put, if their position is correct, regulators will have a powerful legal tool that does not require overhauling our property laws.

Users: We are creating too much data, both from oversharing and from "data exhaust," but have no way to manage it. A common example of oversharing is entering a bar, which requires patrons to prove that they are above the legal drinking age.[16] This is usually accomplished by presenting a state-issued driver's license to the bouncer, which displays the customer's date of birth. Yet an individual needlessly shares an exact birthdate for binary information: Is the person over or under the age of 21? Worse, sharing a driver's license exposes other PII that is irrelevant to the identity transaction taking place, such as the bearer's full name, home address, and status as an organ donor. Similar examples are sharing full credit histories, household income, and assets with a department store for a modest line of credit. One has to ask if sharing this information is necessary, and if so, what rules govern their future use of that data? Can they

keep it? Can they resell it? Are they profiling their customers with it? More importantly, once this data is shared, how is it possible to know where it has gone or how it has been used?

As troubling as these questions are, issues around "data exhaust" are potentially more concerning. "Data exhaust" has been described as the "evil twin brother" of big data. It is the trail of cookies, session logs, and other metadata created during online activity.[17] While this data is useful to firms for improving the user experience, it can also be used to develop profiles and individual-specific insights that compromise any reasonable definition of privacy. Unlike oversharing, users are often unaware of the amount of data they are leaving behind and the ways in which it can be used.[18]

Companies: Directly managing identity databases is risky. As companies and NGOs collect large amounts of information on their employees or the populations they serve, these organizations assume the responsibility of protecting that data. That burden is significant legally, financially, ethically, and socially:

- **Legally:** The EU General Data Protection Regulation (GDPR) went into force on May 25, 2018. This far-reaching regulation imposes significant penalties on entities if they manage personal data in ways that are legally deemed as irresponsible.

- **Financially:** Software maintenance, routine updates, server hosting, and the archiving of data are a nontrivial cost for companies and NGOs.

- **Ethically:** The Harvard Humanitarian Initiative released a report entitled *Signal Code* in January 2017 that describes the increasing volume of digital information humanitarian organizations are now handling and the responsibilities that data management entails.

- **Socially:** Everyone—employees, refugees, or social media users—is increasingly aware that their data is valuable and should/will be reluctant to share valuable data if there is no assurance that it will be well guarded.

Solution architects: We have too much functional identity and too little foundational identity. Many identity solutions are functional in design. A functional identity is used solely for a narrowly defined purpose. For example, a medical insurance card is used to access health care and a voter ID card serves the purpose of conducting a vote.[22]

A foundational identity, on the other hand, is multi-purpose, allowing access to multiple services or applications. Various national ID card systems or university ID cards, for example, could be classified as foundational.[23] SSI provides a way

through the complexity of a centralized foundational ID, gives the individual a way to manage multiple credentials from multiple sources, and provides a user-centric platform that can in effect become the ultimate foundational identity—one solution that can be applied in most, if not all, use cases.

For all of these reasons, we see identity as broken, which is why we are excited about digital identity in the form of SSI.

The Evolution of Digital Identity

Christopher Allen described four stages of digital identity in 2016.[24] In **Phase One**, a single and centralized authority controls the system. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) is the lone administrator—and source of truth—for domain name servers online.[25] Within **Phase Two,** a federated solution, such as Microsoft Passport, allows users to utilize the same identity on multiple sites. A powerful institution, however, is usually at the center of the federation. Through **Phase Three,** there is a modicum of respect for consent concerning disclosure of PII across interoperable and user-friendly platforms, but final ownership and control of user-centric identities remain with the registering entity, such as Facebook, the Google G Suite, or OpenID. **Phase Four** is self-sovereign identity, requiring that users be in full control of their digital identities and are the sole managers of their PII—there is no central authority.[26]

Table 1: Christopher Allen's "Evolution of Identity" and Updated Examples

Phase of Evolution	Summary	Example
Phase One: Centralized Identity	Administrative control by a single authority or hierarchy	**ICANN**
Phase Two: Federated Identity	Administrative control by multiple, federated authorities	**Microsoft Passport**
Phase Three: User-Centric Identity	Individual or administrative control across multiple authorities without requiring a federating authority	**Facebook, Google G Suite, OpenID**
Phase Four: Self-Sovereign Identity	Individual control across any number of authorities	**Platforms Within Report**

SSI provides users with full control over the administration and use of their identities.[27] One criterion that serves as a "litmus test" for SSI is whether a user's identity can be revoked or deleted by the platform provider or any other third party. If this outcome is possible, the identity scheme is at best user-centric.[28]

Creation and Use of a Self-Sovereign Identity

A user can create a self-sovereign identity on a given platform through a process known as enrollment. To be precise, the user is creating a public identifier that they control via a public/private key pair. The identity can be enriched over time as valid claims are added to it by credible third parties. Data input may include basic demographic and contact information, likely a full name, phone number, and email. Biometric information, such as a set of fingerprints or a face scan, may also be added depending on the platform in question. After the creation of this baseline identity, a user can compile a number of credentials, distributed by various issuing authorities. These initial credentials, such as a driver's license, a passport, or a diploma, will be incorporated into the individuals SSI wallet.[29]

A credential is a set of one or more claims provided by an issuer—a known and trusted real-world entity.[30]Anticipated issuers include banks, universities, hospitals, and governments, among numerous others. Within an SSI ecosystem, these established entities can provide credentials that are easily verifiable and tamper-resistant through digital signatures.[31]

As an individual user accumulates more verifiable credentials, their self-sovereign identity becomes more robust. In the future, a substantial SSI might include a digital driver's license provided by the State of Maryland, a digital passport issued by the U.S. Federal government, and a digital diploma signed by Georgetown University. Furthermore, activities like paying taxes or credit card bills on time can also be recorded in an SSI wallet. Users will be able to disclose these verifiable credentials, or parts of them, as well as transaction histories, at their discretion. Furthermore, since the data sits in users' wallets, their approval will be required if their information needs to be accessed.

Equipped with a self-sovereign identity, a user can return to their local bar and present the verifiable credential that "I am over the age of 21" (derived from the digital driver's license) in a secure manner. Through algorithms known as zero-knowledge proofs (ZKPs), the user can validate that they are of the legal drinking age without sharing underlying or secondary data. The bouncer simply learns that the individual is older than 21, without viewing their date of birth or any other PII contained within the digital license. At that point the bar would have a record that the person associated with this wallet (which can be verified biometrically) is over 21, but would not have any other information.

Table 2: Selected Definitions of Self-Sovereign Identity Terminology

Term	Definition
Claim	An assertion made about an identity
Credential	Set of one or more claims provided by an issuer --a known and trusted entity
Verifiable Credential	A tamper-resistant and digitally-signed credential with clear authorship. Provided by an issuer --a known and trusted entity
Issuer	A known and trusted entity that issues credentials about one or more identities
Presentation	Process of sharing data derived from one or more credentials, issued by one or more issuers, with another entity

Source: "Verified Credentials Data Model 1.0," World Wide Web Consortium (W3C).

Why the Time for Self-Sovereign Identity Has Come

We have traditionally kept identity data in centralized databases, which were the only technical option. Now that distributed ledger technology is becoming available and affordable, however, SSI projects are developing rapidly. As noted by Phil Windley, chair of the Sovrin Foundation, self-sovereign identity is now possible thanks to the development of distributed ledger technology (DLT). There is no central authority within the SSI model and no central database storing PII. DLT is ideal for SSI platforms because it enables secure enrollment, data storage, validation of credentials, and the recording of transactions without the need for a principal administrator.[33] Now that implementation of self-sovereign identity is feasible, there is a choice to be made. Bob Reid, of Everest, describes that choice as "either [data control] goes to individuals or it goes to major institutions that will mine our data."[34]

A self-sovereign identity solution can be adapted for a wide range of use cases, including subsidies, banking, microfinance, healthcare, and land administration. The interoperability and flexibility of SSI can also help to prevent the creation of

identity "silos" designed for a specific purpose, such as for subsidies in a refugee camp. A single-purpose digital identity solution often places an unnecessary burden on marginalized populations; it is another password to remember, another card to safeguard, a new bureaucratic system to worry about.[35]

Widespread adoption of an advanced technical solution in the Global South may be challenging, but it is not impossible. Both mobile phone penetration and internet access are increasing in many developing countries (See Box 6 below).[36] Thoughtfully-designed digital solutions—those which do not impose administrative and financial burdens or require a high level of technological know-how in the end user— can now attain widespread adoption in emerging economies. Examples include M-Pesa, which allows for the transfer of funds via text message, in Kenya and Tanzania, and WhatsApp, a messaging service with over 200 million users in India.[37]

We believe that self-sovereign identity will be widely adopted due to: 1. social realities, as everyday life is increasingly digital and existing systems leave their users vulnerable; 2. the development of enabling technologies, such as DLT and smartphones; and 3. growing capacity for adoption of new technologies in the developing world. Various firms are already working with governments and other stakeholders to develop and implement SSI solutions. To borrow a quote from the Evernym homepage: "Self-sovereign identity: now that it's possible, it's inevitable."[38]

→ BOX 1

The ID2020 Alliance Manifesto

Shortly before we finalized this report, and well after the previous section was completed, the ID2020 Alliance[39] published the following manifesto.[40] Points one through eight align with the case that we have just laid out. Point 10 mentions pilot projects; the first two were announced at the ID2020 Summit in New York, on September 14, 2018. One is the Everest project mentioned in the paper below.

1. The ability to prove one's identity is a fundamental and universal human right.

2. We live in a digital era. Individuals need a trusted, verifiable way to prove who they are, both in the physical world and online.

3. Over 1 billion people worldwide are unable to prove their identity through any recognized means. As such, they are without the protection of law, and are unable to access basic services, participate as a citizen or voter, or transact in the modern economy. Most of those affected are children and adolescents, and many are refugees, forcibly displaced, or stateless persons.

4. For some, including refugees, the stateless, and other marginalized groups, reliance on national identification systems isn't possible. This may be due to exclusion, inaccessibility, or risk, or because the credentials they do hold are not broadly recognized. While we support efforts to expand access to national identity programs, we believe it is imperative to complement such efforts by providing an alternative to individuals lacking safe and reliable access to state-based systems.

5. We believe that individuals must have control over their own digital identities, including how personal data is collected, used, and shared. Everyone should be able to assert their identity across institutional and national borders, and across time. Privacy, portability, and persistence are necessary for digital identity to meaningfully empower and protect individuals.

6. Digital identity carries significant risk if not thoughtfully designed and carefully implemented. We do not underestimate the risks of data misuse and abuse, particularly when digital identity systems are designed as large, centralized databases.

7. Technical design can mitigate some of the risks of digital identity. Emerging technology—for example, cryptographically secure, decentralized systems —could provide greater privacy protection for users, while also allowing for portability and verifiability. But widespread agreement on principles, technical design patterns, and interoperability standards is needed for decentralized digital identities to be trusted and recognized.

8. This "better" model of digital identity will not emerge spontaneously. In order for digital identities to be broadly trusted and recognized, we need sustained and transparent collaboration aligned around these shared principles, along with supporting regulatory and policy frameworks.

9. ID2020 Alliance partners jointly define functional requirements, influencing the course of technical innovation and providing a route to technical interoperability, and therefore trust and recognition.

10. The ID2020 Alliance recognizes that taking these ideas to scale requires a robust evidence base, which will inform advocacy and policy. As such, ID2020 Alliance-supported pilots are designed around a common monitoring and evaluation framework.

We humbly recognize that this is no easy task, but we see urgency as a moral imperative. This is why we have set ambitious targets and why we hold ourselves to account.

Registries and Self-Sovereign Identity

Self-sovereign identity could have a significant catalytic effect on registries. Before explaining further, it is useful to review the nature of registries and their importance in society.

Registries and Society

Registries are key components of any functional society. Without shared, verifiable information about people and assets, collaboration, trade, and finance would all be all but impossible. A registry is a list of people, organizations, or things accompanied by information about them which is relevant to the purpose for which the registry was established. This information is endorsed and made credible by its inclusion in a trusted public ledger. Registries of people serve many purposes, from securing citizens' access to services to helping researchers understand rare diseases. Asset registries allow for documentation of who has which rights to what assets. These records create value and serve as "market-enabling institutions," for the various actors in different sectors of social and economic life who use registries on a daily basis.[41]

Examples and typology of registries follow, although this list is far from comprehensive:

Entity registries capture essential information about people or organizations.[42]

- **Natural persons** are individual human beings, as opposed to a legal person, which may be a private (business entity or non-governmental organization) or public (i.e., government) organization.
    - **Vital records** describe the group of birth, death, marriage, and divorce registries. In some jurisdictions, civil unions or domestic partnerships will also be included. A birth registry --complete with names, parents, time, date, and location-- may be used for the purposes of citizenship or identity. The UNDP notes that in almost all societies a birth certificate automatically grants a number of rights, such as the right to health care, schooling, a passport, property ownership, voting, formal employment, and access to banking services.[43]
    - **Patient registries** allow patients and researchers to collaborate, further disease understanding, and enable rapid decision making. [44] Similarly, a clinical quality registry is established with the purpose of monitoring quality of care for patients, providing

feedback, benchmarking performance, describing patterns of treatment, and as a research tool. According to a 2017 study published by the University of South Australia, these registries play an increasingly important role in improving health outcomes and reducing health care costs. [45]

- **Legal persons** are organizations or companies.
    - **Company registries** are usually managed either by a government or a chamber of commerce. Any company that wishes to be constituted legally must register with the managing entity, and may be placed within an industry-specific registry. Company registries improve the functioning of the private sector and facilitate tax collection, to name only a few key functions. [46]
    - **Organizational registries** list any other kind of organization from NGOs to churches. TechSoup's NGOSource is one of the largest such registries that we are aware of. The registry and its impact are described in the following box.

→ BOX 2

TechSoup and NGOSource.org

TechSoup has developed an organizational registry, NGOSource.org. At first, this tool allowed tech firms to efficiently distribute software to NGOs. Then members were eligible for cloud-based storage and compute. It did not take long for non-U.S. NGOs to request access to the digital treasure trove. But granting to foreign NGOs is not a simple matter. In order to protect their tax-exempt status, philanthropic funds and charitable organizations in the U.S. must only donate to other tax-exempt organizations. If a donor organization wishes to donate outside of the U.S., regulations require a process called an equivalency determination, or ED.

In the absence of a registry, each donor would need to incur this cost every time they gave to a new organization. By including foreign organizations in NGOSource, TechSoup has made it possible for U.S. donor organizations to reduce the time and cost of this process. Once a donor includes a new grantee, all subsequent donors can benefit from the ED. A description of the organization and its registry follows, as provided by TechSoup.[47] *The purpose of including this here is to illustrate the ways a credible registry creates value.*

TechSoup, launched in 1987, has grown around its core technology donation program as a social enterprise into the world's largest NGO data repository. Currently, TechSoup counts 1.1 million registered nonprofit, nongovernmental, social benefit organizations. Of these, roughly 400,000 are in the United States and the remainders are across all non-U.S. embargoed states. To date, TechSoup has served at least one organization in each country where American organizations are allowed to work, and an additional 600 to 800 organizations register each day.

TechSoup's work establishing the frameworks for validating organizations through its global network of partners has further led to a variety of additional, non-technology specific, civil society identity partnerships. The most developed of these is NGOSource.org, which, in partnership with the Council on Foundations, established a US 501(c)(3) equivalency determination process that has become the "go-to" solution for U.S. foundations using equivalency determinations to support their international grant making. More than 250 foundations use NGOSource.org, representing some 90 percent of international grant making.

Asset registries at their core, identify unique assets and then describe who has which rights to those specific assets.

- **Real assets** are physical things with intrinsic value.
    - **Immovable registries** describe parcels of land, from urban plots to sections of forests, as well as discrete buildings, apartments, etc. Broadly, the rights that an organization or person may have to these assets include, but are not limited to, ownership, occupancy, logging, mining, flyover, etc. A property registry helps to ensure strong land tenure security and enables mobility, security, financial inclusion, gender equality, and many other elements of socioeconomic development.[48] Land registries also help facilitate efficient tax collection and help identify property owner(s) during a transaction such as the purchasing or renting of land.
    - **Movable registries** describe objects which are not fixed in place, such as vehicles, boats, livestock, and mechanical equipment. Rights vary from ownership, to possession, to liens. A car may be owned by a dealership, possessed by the lessor, but have a lien held by a financing agency or bank. The FAO highlights how a registry can be used to levy taxes or to confirm ownership before a sale in

the case of shipping,[49] but this is also true of automobiles and other vehicles.

- **Movable asset collateral registries** record various assets that borrowers offer lenders to secure a loan.[50] While it may seem duplicative to list it here, the category is important enough to be distinctly labeled. These registries allow lenders to "perfect" a security interest,[51] provide recourse in case of loan default, and ensure an asset cannot be fraudulently used as a security for multiple loans. Collateral registries facilitate lending to businesses, with land and buildings widely accepted as collateral for loans.[52] Many banks in the developing world are beginning to accept movable assets as collateral, increasing financial inclusion for small- and medium-sized enterprises that lack immovable resources.[53] For example, a 2013 International Finance Corporation study found that access to bank finance increased by almost 8 percent on average across seven countries after collateral registries and related lending practices were established.[54]

- **Non-physical assets,** are valuable but intangible things.
  - **Financial assets** are stocks, bonds, fiat or cryptographic currency, or debts owed by someone. Sometimes, financial assets can be included in the collateral registries described above.[55]
  - **Digital assets** range from rights to everything from music files, to satellite imagery, to parts of virtual worlds. They would also include utility tokens that are ostensibly non-financial in nature.

In all these cases, registries connect assets and/or related information with people or a group of people. Registry managers essentially perform four key tasks:

1. **Verifying individual identity:** Confirming the identity of the person or the group in question.
2. **Identifying objects:** Identifying the unique object in question, such as a boat or land parcel, where applicable.
3. **Gathering data:** Validating associated information, where applicable.
4. **Managing the registry:** Managing the process of adding, amending, and/or referencing information in the registry.

The occupation of these managers generally depends on the specific registry. A collateral registry will be staffed with financial experts, such as bankers and underwriters; a property registry will be staffed with property experts, such as surveyors and assessors; and a clinical quality registry will be staffed by medical experts, such doctors and researchers. Although establishing the identities of the people who interact with these registries is fundamental to their successful operation, this process usually relies on legacy systems and regulations. This often entails cumbersome and costly in-person identification, for example a lawyer or notary witnessing the seller's signature on a property transfer document.

→ BOX 3

Corporate Registries: An Example from British Columbia[56]

While our report primarily focuses on self-sovereign identity for individuals, other use cases do exist. An ongoing and experimental effort by the Government of British Columbia, known as the Verifiable Organizations Network, provides self-sovereign digital identity for businesses throughout the province.[57] Project leadership aims "to create a trusted digital network of verifiable data about organizations which is globally connected, interoperable, secure, and easy to join."[58]

Foundational information about an organization is derived from British Columbia's Corporate Registry. This data, supplemented by various other "verifiable credentials," is issued to TheOrgBook. This public-facing repository aims to enable web- and API-based searches of registrations, licenses, and permits which are cryptographically signed by provincial and municipal authorities. The platform, based on Hyperledger Indy,[59] increases efficiency through consolidation and exhibition of trusted information without demanding that a company possess its own digital wallet.[60]

Canadian officials currently aim to verifiably connect individual digital identities with organizational identities based on ownership. Scaling of the project to at least one other province (Ontario) is underway.[61] Public Services and Procurement Canada, a federal department, is co-developing the technology for use within the context of supplier registration.[62]

This success and expansion of the Verifiable Organizations Network and TheOrgBook demonstrates that the creation and roll out of complex organizational identities is possible. We believe that the concept can be

effectively translated to encompass real assets, including land parcel data, which is arguably less complicated than organizational data. While we are arguing in this report that SSI for individuals can help registries to evolve in many domains, we are also making the point that the technology can also be used for non-human entities like companies or properties. The creation of digital property identity provides a compelling opportunity to improve land tenure and create opportunities around real estate.

The Challenge of Identity Within Registries

Our current identity systems are increasingly challenging, complex, and congested. People are more mobile and more connected than ever before. In the developed world, technology allows individuals to complete myriad tasks remotely—from renewing a license to buying a house; from selling shares to moving money between bank accounts. With such activities now possible online, there are also increased opportunities for fraud, as many basic checks on identity, namely completing a transaction in person, are eliminated. According to Javelin, a California-based advisory firm, "it is no coincidence then that adoption of digital channels and devices have grown in tandem with fraud."[63] The number of identity fraud victims in the U.S. reached 16.7 million in 2017, a record high since Javelin began tracking identity fraud in 2003. These crimes continued to shift online and away from physical stores.[64]

Within emerging markets, large groups of people are beginning to take part in digital financing. Societies that have used physical money for generations are now utilizing mobile phone applications, such as M-Pesa, to transact in refugee camps, town markets, capital cities, and remote villages.[65] A 2016 report by McKinsey Global Institute asserts that the continued spread of digital financing in the developing world could be "transformative." Provision of basic financial services via mobile devices can reduce costs for providers, while increasing convenience and opening access to capital for individuals; businesses can ease inefficiencies and generate significant productivity gains.[66] As a result:

- The GDP of all emerging economies could increase by 6 percent, or $3.7 trillion, by 2025.
- This additional GDP could create up to 95 million jobs across all economic sectors.
- 1.6 billion "unbanked" people could gain access to formal financial services; more than half of this total would be women.

- An additional $2.1 trillion of loans could be made to individuals and small businesses.

The report also warns that this trend is not without risks, including the creation of new transaction costs, as well as potential for fraud and abuse of technological newcomers. Secure digital identity is critical for combating fraud, which is the predominant risk that comes with increasing digitization of financial services. This risk extends to registries, which, as we discussed above, must be secure and reliable in order to support a wide range of critical economic activities. SSI could become a common solution to these growing problems. There will be both push and pull in the market:

- **Push** from registries: We expect registries to recognize both the increasing importance of digital identity and the complexity involved in managing identity for any given registry. We expect them to move from using existing government issued foundational identities (where, and if, available) to self-sovereign identity platforms for their registries.

- **Pull** from users: As the general population increasingly understands the value of personal information, people will demand the best available tools to protect their data. Also, as the foundational nature of SSI becomes clear, it will be preferable to use one SSI instead of creating a new functional identity (a service specific profile often managed with a username and password).

Self-Sovereign Identity and Asset Registries

As self-sovereign identity platforms go into production and gain wider adoption, registries will have the opportunity to evolve. As the British Columbia example illustrates, transitioning to decentralized identity is possible for an established registry.[68]

Kaliya Young, the "Identity Woman," emphasizes the myriad interactions between individuals and institutional contexts where personally identifiable information ends up in databases; many, but not all of these, involve various types of registries. In *The Domains of Identity,* she describes 16 such identity interactions in detail (See Figure 1 below).[69] Aside from registration at birth, a person completes a number of secondary registrations and transactions over the course of a lifetime. Events include professional licensing, tax payments, and the purchase of land.[70] Many of these identity-based transactions suffer from inefficiency or "bottlenecks" variously caused by the requirement for a notary's signature, the mailing of documents, or the need for an escrow agent.

Current registry infrastructure is usually centralized, with a government or private authority hosting and controlling the data. Numerous stakeholders are involved in administering these systems and jurisdictions adhere to different rules and regulations—especially as it relates to identity issues. As a result, individuals can experience difficulty in accessing relevant data, or can become entangled in protracted bureaucratic processes.

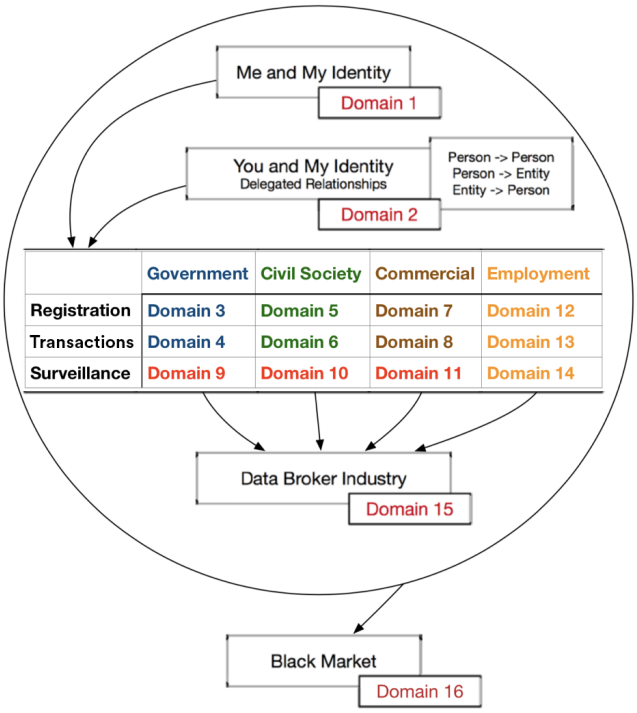
Self-sovereign identity solutions—through cryptographically-signed attestations, pairwise connections, and digital identities—put the information about the user under the control of the user. Individuals or groups can be explicitly linked to their assets via SSI. Registry functionality and scope will evolve as a result, and the challenges of verifying identity and sharing information will evolve to issuing verified credentials and managing the other components of a registry that are not benefiting from SSI.

To be clear, the role of government in registry management will not disappear. SSI should relieve government registrars of the tasks of validating identities and providing ad hoc reports, which would instead be offered by the owner of the relevant SSI. But governments still need to control a registry and manage the other critical data in the registry, as well as issue verifiable credentials.

Through this forward-looking model, it is possible to imagine the utility of asset registries depending on SSI for their identity function, especially in developing countries. Resource-constrained governments with limited technological and infrastructural resources can avoid the repetitive work of building identity into system after system. A state may also continue to arbitrate disputes, but if the integrity of information within identities—and by extension asset registries—improves over time, the need for arbitration or policing should diminish.

Eventually, SSI-based asset registries could also help to generate more accurate, trusted information regarding potential loan borrowers in the developing world. Juan Antonio Ketterer and Gabriela Andrade, both financial market specialists at the Inter-American Development Bank, assert that "more transparent and more efficient registries of assets as collateral could diminish constraints rooted in information asymmetries and thus facilitate access to finance."[71] As shown by recent initiatives in Latin America and the Caribbean, the expanded use of movable assets as collateral can have a significant impact on economic growth for small- and medium-sized companies, female business owners, and young entrepreneurs.[72]

Figure 1: Domains of Identity by Kaliya Young



Source: Courtesy of Kaliya Young

Digital Identity and Land Use Cases

Self-sovereign identity will be disruptive for property rights. The technology could explicitly connect people to land parcels within property registries and also provide a platform for documenting land claims and associated data in the absence of a secure formal registry. Discussion below will examine the impact of SSI on four other land-related topics:

- **Efficiency in real estate markets:** Mitigating fraud risk within real estate markets requires a high degree of due diligence around the identities of the transacting parties, contributing to workflow inefficiencies and high transaction costs. A self-sovereign identity solution could securely connect landowners to their properties and enable trusted and transparent online workflow, including legally-binding digital signatures.

- **Property rights in post-conflict situations:** The legal return of property to refugees and internally displaced persons (IDPs) contributes to peaceful rebuilding in post-conflict situations. But the process of restitution is complex, as many of the displaced lack important land-related documents or fear persecution for asserting their claims. A self-sovereign identity solution could enable these vulnerable individuals to securely store property ownership documents or to receive verifiable credentials from an NGO in order to better record a claim in the absence of a functioning registry. Of course, if a country had an SSI-integrated registry in the first place, refugees would never be separated from their claim to property.

- **Natural disaster resilience:** Accurate property rights are crucial for disaster preparedness and can expedite reconstruction. Current disaster resilience programs do utilize emerging technology, but a self-sovereign identity solution could provide individuals with a more secure and accessible tool to demonstrate their property rights and apply for aid and reconstruction grants. Distributed document storage would ensure the survival of essential records and biometrics would allow people to prove their identities and authenticate to services even if their physical identity documents were lost or destroyed.

- **Women's land rights:** Women make up almost half of the world's agricultural workforce, but are often excluded from land ownership by entrenched, discriminatory customs and practices. Recently, many countries have passed legislation to improve gender equality in property ownership. A robust self-sovereign identity platform could bolster this

progress by connecting women more securely to their properties. Paper land records can be withheld or fraudulently transferred by male relatives. Similarly, physical identity documents needed to interact with the registry can be stolen or destroyed. The personal control and persistent identity afforded by SSI would help to address both of these issues. SSI could also improve transparency in judicial decisions related to land disputes, and allow gender-blind interactions with the land registry and related financial and administrative services via zero-knowledge proofs. In turn, a greater degree of women's land ownership could support socioeconomic development throughout the Global South.

Increased Efficiency in Real Estate Markets

Even advanced land administration systems often lack sufficiently robust identity solutions. For example, in Ontario, real estate lawyers are required to verify the identity of their clients in property transfers. This means that clients must either be physically present with their lawyer for the signing of the documents or, if they are traveling, must hire a second lawyer in their location to attest to their identity. There is no settled law in Canada on the standards for remote, digital identification and authorization. Even a live video call with the client is considered insufficient. In addition, only verified real estate professionals (primarily lawyers) are allowed to file documents for registration in Ontario's electronic land records system. In order to create an account they must submit an application and appear in person with two forms of ID.[74] The rationale for restricting access to verified professionals is largely the need to shift liability for verifying the identities of buyers and sellers away from the registry.[75]

In technologically sophisticated and well-governed jurisdictions like Ontario this system functions very well. But the increased cost of registration and restricted access to the land registry is a greater burden in the developing world. SSI and biometrics can help to reduce fraud by bringing existing, verified, foundational identities to the registry.

The consequences of lower liability in real estate can be especially critical for countries in the developing world. Secure connections between people and property through SSI will better allow individuals to use property as collateral, and subsequently access banking services such as loans and mortgages.[76] Financial inclusion encourages improvements in land and housing, raising property values and enhancing livelihoods. For those who do not own property, transparent and secure registries provide better access to markets.[77] Formalization of land and stronger property rights should also increase investor confidence, leading to an inflow of capital.[78]

Property Rights in Post-Conflict Environments

The legal return of property to refugees and internally displaced persons (IDPs) is critical for rebuilding in post-conflict situations. But the process of restitution is complex, as many of the displaced lack important land-related documents and/or fear persecution for asserting their claims. A self-sovereign identity solution could enable these vulnerable individuals to securely store property ownership documents or to receive verifiable credentials from an NGO in order to better record a claim in the absence of a functioning registry.

The 2005 United Nations' Pinheiro Principles state that "all refugees and displaced persons have the right to have restored to them any housing, land or property of which they were arbitrarily or unlawfully deprived..."[79] Such recovery and/or restitution of property can be complicated. Whole families can change as a conflict carry on for years or decades. People often flee hundreds of miles and cannot return home easily. Many lose their identification cards, passports, deeds, and other important documents as they take refuge in other countries.

This phenomenon is far from new. Jewish groups are still attempting to obtain the return of Holocaust-era assets throughout Europe[80]; Palestinians continue to claim houses and land lost during the chaotic formation of Israel.[81] And ruinous intra-state conflicts have proliferated since 1945; these civil wars last an average of seven to 12 years.[82] According to the 2017 *Global Trends* report by UNHCR, an unprecedented "68.5 million people were displaced as of the end of 2017. Among them were 16.2 million people who became displaced during 2017 itself, either for the first time or repeatedly."[83] The relative ease of modern travel has resulted in millions fleeing far from home to Europe and beyond.

Case studies demonstrate the dire need to secure land rights in war-ravaged states. John Dempsey, formerly a senior advisor for Afghanistan to the U.S. Agency for International Development, notes that the South Asian country has produced roughly 8 million refugees and IDPs since the 1979 Soviet invasion. Families often return home to find their property long occupied by others. Poorly-organized, conflicting, and informal property claims unsurprisingly lead to land disputes, which easily devolve into violence, perpetuating instability.[84]

The Syrian Civil War has currently displaced 12 million people, or approximately half of the pre-conflict population.[85] Although fighting has largely subsided, many refugees are afraid of returning to a state still controlled by the brutally repressive Assad regime. The Assad regime does appear to be interested in the homecoming of millions officially viewed as the opposition. Instead, Assad aims to reshape the demographics of his war-torn country.[86]

Even for those Syrian refugees who do desire to return home, it will be increasingly difficult to lay claim to property. Recent surveys indicate that only 17 percent of Syrian refugees possess documentation of their property rights, while only 9 percent of IDPs have managed to maintain their records.[87]

Worse, the vindictive Assad regime in April 2018 passed *Law No. 10*, which enables the government to expropriate informal settlements for the ostensibly benign purpose of reconstruction or development. Most inhabitants of informal communities supported the opposition and fled the country. Both Syrians and international observers perceive *Law No. 10* as little more than formalized land grabbing as punishment for rebellion.[88]

The Assad regime is clearly aware of the immense power of land ownership, but instead of utilizing property as a tool for reconstruction and peace, the state is exploiting land as another weapon against its opponents. And Assad may very well realize a demographic revision of Syria.[89] Human Rights Watch notes that a significant segment of the Syrian refugee population is "unlikely to return without a house or property to return to."[90]

Precautionary actions could have been taken to mitigate this crisis. Various organizations are presently examining new technologies to support marginalized populations, including refugees and IDPs.[91] Implementation of self-sovereign identity is a compelling option to empower vulnerable groups during their displacement and repatriation. Digitized land records encrypted in distributed storage would not be destroyed or become inaccessible during displacement. These would ideally be copies of the legal land records held in the state-sanctioned registry. But other information to support land restitution claims can be recorded by an NGO through personal interviews and earth observation data. Such information can then be connected to a self-sovereign identity through a credential, giving refugees and IDPs time stamped documentation of their claim to that property. These credentials could later be used in the post-conflict dispute resolution and land restoration process.

Natural Disaster Resilience

Hurricanes, typhoons, and floods have all intensified in recent decades.[92] As vulnerable communities confront these natural disasters, land administration is increasingly recognized as a critical part of the emergency planning and recovery process. A lack of clear property rights particularly leads to conflict, delay, and higher costs during reconstruction.[93]

Sameh Wahba et al. argue compellingly that land records and related geospatial data are vital in "all phases of disaster risk management, such as disaster reduction, risk reduction, preparedness and mitigation, and emergency

response."[94] In the aftermath of a natural disaster, thorough and secure registries ensure protection of property rights and livelihoods for returning evacuees. Post-disaster access to PII and land data facilitates loss valuation, reconstruction planning, and access to financial services including reconstruction grants.[95]

Many disaster resilience programs do not take full advantage of emerging technologies, but there are notable exceptions. In the eastern Indian state of Odisha, for example, an initiative run by the state government in partnership with the Tata Trusts and Omidyar Network combines drone mapping, land title formalization surveys, and financial assistance to encourage the construction of permanent "monsoon-resistant" housing.[96] (Disclosure: Omidyar Network is a funder of the Future of Property Rights Program at New America, and provided financial support for this report.)

Investment in a more storm-resistant housing stock is essential for human security and economic development in places like Puerto Rico, where FEMA recovery grants --based on the replacement value of the existing structure, have been too small to allow for sturdier reconstruction that will survive the next major storm. According to reporting by *The New York Times*, the median repair grant was $1,800, and while "a new roof of cheap corrugated zinc typically starts at about $5,000 and might blow off again in the next hurricane; a concrete roof that could survive future storms costs about $15,000."[97]

Paper land and identity documents are vulnerable to loss or destruction, and even simple ways of increasing the durability of documents, like lamination, may prohibit service at banks or government institutions.[98] Paper records still serve an important role, especially in communities where connectivity is limited. But the issuance of paper documents should be accompanied by the concurrent creation of digital credential, linked to a SSI, in order to create a more resilient system.[99] The process of digitizing land records is relatively simple and has many practical benefits. We have written about the success of large-scale digitization projects in Punjab, Pakistan.[100] SSI could provide individuals with more agency and opportunities during post-disaster situations, especially given a synthesis of digital identity platforms and land registries. Due to decentralization, a self-sovereign identity solution will be more resistant to destruction, more accessible to vulnerable populations, and will allow for improved data management.[101]

Women's Land Rights

Almost half of the world's farmers are women, but they are often excluded from land ownership due to entrenched discriminatory customs and practices. Although many countries have passed legislation to improve gender equality in property ownership, a robust self-sovereign identity platform could bolster this progress by connecting women more securely to their property. SSI could also improve transparency in judicial decisions related to land disputes. In turn, a

greater degree of women's land ownership could support socioeconomic development throughout the developing world.

On average, women comprise 43percent of the agricultural workforce in developing countries.[102] Small farms are labor intensive, and women are often expected to perform additional duties, including supplying food to men in the fields, fetching water, collecting firewood, caring for children, and preparing meals.[103] Women are also heavily involved in the livestock sector, and many others labor under contract farming arrangements.[104]

Female farmers often lack proper access to resources and services such as land, animals, human capital, financial services, and new technology.[105] There is an enormous gender disparity in global land ownership. A recent analysis of eight African countries revealed that women comprise less than one quarter of landowners. The proportion of female landholders in Latin America is about 20 percent; in the Middle East and North Africa it is as low as 5 percent.[106] Poor women usually work in harsh conditions, earn meager wages, and are subject to sexual harrasment.[107]

In many contexts, a woman's right to use land depends on her relationship to a man: a husband, father, brother, or other male relative. If said man dies or becomes estranged, the woman may be coerced off of land or out of a home with little or no recourse. Paper land records may be withheld from a woman or fraudulently transferred to a man during a subsequent dispute. These physical documents, needed to interact with a registry, might also be stolen or destroyed.

Even in places where women have equal land rights before the law, practices and customs often favor male rights over female. Officials often fail to protect women's rights, and male relatives can withhold court notices to sabotage proceedings related to land-grabbing and other disputes.[108]

Various developing countries, such as Nepal, have enacted progressive legislation to fight discrimination against women's land ownership.[109] The African Union formally pledged in 2016 to ensure that women constitute 30 percent of landowners by 2025.[110] Punjab, Pakistan recently connected "next of kin" data within the national identity system to its provincial digital registry in order to guarantee women properly receive legally-mandated land inheritance. Related legislation concerning female property rights was previously ignored; now technology has improved lives by helping to ensure that good laws are executed.[111]

Technology is not a panacea, and laws, behaviors, and attitudes will need to change. Yet a self-sovereign solution could mitigate many of the aforementioned abuses and help to sustain progress in gender equality. Personal control of a persistent identity afforded via a self-sovereign identity platform would allow for more secure management of land-related documents. It would be difficult for a

male relative to fraudulently transfer, steal, or destroy a title connected to a women's SSI, and stored on a biometrically-secure smartphone or in the cloud. Through use of zero-knowledge proofs, women might not even need to disclose their gender when interacting with a land registry or related financial and administrative services.[112]

It is unrealistic to assume that digital identity can prevent real world threats and physical intimidation in land disputes. But an SSI ecosystem connecting women to the judicial system and/or relevant NGOs could help to streamline reports of injustice, as well as document sharing for legal proceedings. Increased transparency and the potential for human rights organizations to monitor data via observer nodes[113] might prompt previously apathetic officials to protect female title security. Repeated abuse could be connected to specific identities and clearly displayed on a blockchain for easy access by law enforcement.[114]

The importance of women's land rights cannot be overstated. Title security is strongly correlated with higher economic gains for women in countries like Tanzania, Rwanda, and India.[115] Female land ownership further promotes entrepreneurial investment, agricultural productivity, and food security. Multiple studies have even demonstrated that the resulting economic stability reduces women's vulnerability to domestic violence, poverty, and the impact of HIV/AIDs.[116]

Section 2: Three Solutions Through Ten Principles

This section has three parts. First, we review 10 broad and well-established principles of SSI. Second, we describe three noteworthy SSI solutions from **Everest, Evernym**, and **uPort**. Third, we look at each of these three firms through the lens of the well-established set of principles previously described. We do not do this to make the case for any one of the three; by exploring solutions which are markedly different along various axes, we hope to clarify for the reader the breadth of possible options to be explored.

The Principles of Self-Sovereign Identity

There is no universally recognized definition of SSI, although we agree with Christopher Allen that in the absence of a common description, the best course of action is to evaluate each solution by its overall adherence to the principles of self-sovereign identity, which "actually provide a better, more comprehensive, definition of what self-sovereign identity is."[117] A sizable and growing body of literature surrounding the "principles of identity" seems to be harmonizing on to a consistent set.

Key members of the international development community have developed separate, yet overlapping principles for identification. Prominent sets are introduced in:

- The *National Digital Identity Programmes: What's Next?* report by Access Now
- *The Known Traveller* report by the World Economic Forum
- The *Principles on Identification for Sustainable Development* report by the World Bank
- The ID2020 Alliance *Concept Note*

Several thought leaders[122] within the digital identity space have developed their own principles or laws:

- Kim Cameron of Microsoft introduced seven laws of identity in 2005.
- Christopher Allen presented ten principles of self-sovereign identity in 2016.

These various sets are relatively consistent. The table below shows that principles prevalent throughout this recent literature broadly include universal coverage and accessibility, protection, data minimization, and users' rights to control and transport their identities.

Table 3: Various "Principles of Identity"

Kim Cameron[125] (2005)	Chris Allen[126] (2016)	World Bank[127] (2017)	ID 2020[128] (2017)	WEF[129](2018)	Access Now [130](2018)
	Existence	Universal Coverage	Universal Coverage	Existence	
User Control and Consent	Control	User Privacy and Control	Control	Control	Control
Human Integration	Access	Remove Barriers to Access and Usage	Access	Access	Access
	Transparency	Open Standards	Open Standards	Transparency	Transparency
	Persistence	Sustainability	Persistence	Persistence	Persistence
Consistent Experience Across Contexts	Portability	Independent Oversight	Portable	Transportable	
Pluralism of Operators and Technology	Interoperability	Interoperable and User-Responsive	Interoperability	Interoperability	
Justifiable Parties	Consent	Legal and Regulatory Framework	Permissioned	Consent	Consent / Accountability
Minimal Disclosure for a Constrained Use	Minimalization	Mandates and Accountability	Private	Minimization	Minimization
Directed Identity	Protection	Unique, Secure, Accurate Identity	Secure[131]	Protection	Protection[132]

We have synthesized and recast these principles. The major differences being the addition of the principle of "Inclusion" and the removal of "Existence." The former is critical for adoption in developing countries and the latter is implicit in other principles, including "Consent." We believe that these principles incorporate all key principles in the space.

1) Inclusion: Identity should be available to all

Every individual should be provided with an identity from birth to death. Enrollment processes cannot discriminate against an individual due to ethnicity, gender, socioeconomic status, illiteracy, language, a lack of resources, or lack of technological literacy. An identity platform should ensure minimum cost to the end user in order to maximize inclusion.

2) Control: Users must control their own identities

Individuals must have ultimate authority over their identities and all related personal data. Storage should be decentralized to the greatest extent possible. It is the user's prerogative to update, share, and hide any information. Solution administrators and/or stewards must be incapable of revoking a user's identity.

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

Users should be able to easily and directly access their identities and all related data. Access must not depend entirely on the technological or infrastructural capacity of the user, especially on the possession of a smartphone. Gatekeepers cannot restrict access.

4) Transparency: Systems and governance must be transparent

The manner in which an identity system functions, is managed, and is updated must be publicly available and reasonably comprehensible. Solution design should be based on open protocol standards and open source software, in part to prevent vendor lock-in. The governance model of the solution should limit the power of administrators to access, revoke, or otherwise interfere with the user's identity and personal data.

5) Persistence: Identities must be long-lived

Identity systems must be long-lasting; user identities should last from birth to death. Solution developers should implement sufficient foundational infrastructure, and design sustainable commercial and operational models. As a caveat, the persistence of digital identities should not contradict the "right to be forgotten."[133]

6) Portability: Identity information and services must be transportable

A digital identity cannot be restricted to a single platform. Users must be able to transport their identities – as well as credentials and attestations—from one platform to another. The transfer of data should be uncomplicated from the user perspective. All firms, governments, and third parties should strive for simple and consistent user experiences.

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

There are numerous contexts in which an identity is required. Through open standards and scalability, digital identity firms should allow myriad stakeholders to leverage the benefits of a solution. Different organizations, databases, or registries must be able to quickly and efficiently communicate with each other globally through an identity system.

8) Consent: Users must agree to the use of their identity or data

Users must give explicit permission for another entity to access and/or utilize their data. The process of expressing consent should be interactive, deliberate, and well-understood by the user. Shared information must only be used for a specific function. Users must restate consent for personal data to be used in a different manner and/or to be used another time.

9) Minimization: Disclosure of identity information must be minimized

Any identity solution should mitigate against extensive disclosure of personally identifiable information. A platform must minimize the type and quantity of information collected by entities that verify individuals. A user should share only the least possible amount of data necessary to accomplish the task at hand. Minimization can help to ensure user privacy.

10) Protection: Users' right to privacy must be protected

Any solution must be embedded with "privacy-by-design."[134] Safeguards should exist against tampering, data traffic should be encrypted end-to-end, and restrictions should be placed on the monitoring of information. Affected parties

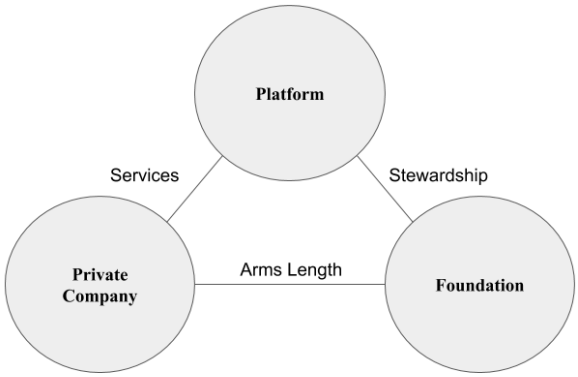
must also be notified of a data breach. Users' right to privacy must always come first.

Three Self-Sovereign Identity Platforms to Watch

The first instinct of many governments, NGOs, and international organizations may be to create single-purpose identity solutions through the use of biometrics and commonly available identity products.[135] This is increasingly impractical and a disservice to the end user. Our analysis concentrates on firms dedicated to developing self-sovereign identity solutions.

The firms included within our report offer slightly different ecosystems. Each will include a self-sovereign identity platform and a private company (or group of companies) that will sell value-added services for their respective platform. Two of the ecosystems—from Everest and Evernym—will include an independent foundation as steward of the SSI platform with a fiduciary responsibility to uphold established principles. We believe that this structure is a strong model for governance.

Figure 2: A Suitable Model for a Self-Sovereign Identity Ecosystem



Source: Courtesy of author

Multi-purpose, independent self-sovereign identity solutions are generally preferable to a collection of single-purpose tools for at least four reasons:

- **Leverage:** Any network-based ecosystem requires a critical mass of users to function and becomes more useful at scale. SSI is no exception. As an SSI solution interacts with an increasing number of services and credential providers, identities becomes stronger, more robust, and increasingly valuable. Each entity that provides a service or offers a

credential increases the quality of an identity. Consider how you feel about a social media profile that has hundreds of contacts, some of whom you know, as well as years of posts and interactions: it is probably a real person. Now consider one with dozens of contacts, none in common with you, and a series of single issue posts: It might be a bot. The same is true with identity.

- **Complexity of Related Technology:** The technology needed to create and administer secure digital identities is complex and constantly evolving. Specialists and/or third party firms are better suited to create, deploy, and maintain digital identity solutions. These private entities are also more adept at keeping pace with rapidly evolving technologies. For instance, a firm interviewed for this report is actively tracking the rate at which the speed and cost of DNA sequencing are decreasing. Its leadership is waiting for the day when the technology can be used for biometrics.

- **Risk Mitigation**: Because identity is the core business of SSI platforms, their developers have a greater incentive to prioritize privacy and security than a government with competing priorities.

- **Market Forces:** Competition and the needs of various user groups will motivate and support both development and technological innovation.

Using the principles of SSI as a basis for analysis, we have developed a number of questions concerning the design specifications of various self-sovereign identity platforms and/or products. The three companies we have included in our analysis are **Everest**, **Evernym**, and **uPort**. Each firm is briefly described below.

Table 4: Attributes of the Self-Sovereign Identity Firms

Attribute	Everest	Evernym	uPort
Headquarters	California	Utah	New York
Year Founded	2016	2013	2016

Attribute	Everest	Evernym	uPort
Leadership	Bob Reid (Co-founder & CEO); Brad Witteman (Co-founder & CPO)[136]	Jason Law (Co-founder & CEO); Timothy Ruff (Co-founder, CTO & Chairman)[137]	Rouven Heck (Co-founder & Project Lead); Michael Sena (Co-founder & Product Lead); Christian Lundkvist (Co-founder); Pelle Braendgaard (Co-founder & Engineering Lead)[138]
Purpose	"Dedicated to liberating humanity from subservience to centralized, non-user friendly identity management and capital allocation organizations."[139]	"Evernym is developing a sophisticated identity platform built on Sovrin...to significantly ease the deployment and integration of self-sovereign identity infrastructure in many different industries."[140]	"Our Mission: We believe that everyone has the right to control their own digital identity --how it's shaped, shared, and sustained."[141]
Website	everest.org	evernym.com	uport.me
Network	Identity Network	Sovrin Network	Ethereum[142]
Foundation	Identity Network Foundation (Anticipated establishment in 2018)[143]	Sovrin Foundation (Established 2016)[144]	N/A

Attribute	Everest	Evernym	uPort
Decentralized Application (dApp)[145]	Everest dApp[146]	Connect.Me[147]	uPort ID[148]
Token(s)	ID token[149]	Anticipated use of Sovrin Token	Utilizes Ether as Gas[150] within the Ethereum ecosystem[151]
Initial Coin Offering (ICO)[152]	Fall 2018[153]	2018[154]	Initial Coin Offering for Ether launched in 2014[155]
Use Cases	- **Cambodian health services**; - **Indonesian gas subsidies**	- **MyCUID**; - **Illinois Birth Registration**; - **Financial services in Canada**; - Digital passport and reputation system for UK doctors[156]	- **Government eServices in Zug, Switzerland**; - **Gnosis prediction market**[157]; - **FOAM geospatial data protocol**; - **Asset management**; - **Online poker**

Everest

The Basics: Originally known as EverID, Everest is a California-based digital identity firm founded by Bob Reid and Brad Witteman in 2016.[158] Everest describes itself as "dedicated to liberating humanity from subservience to centralized, non-user friendly identity management and capital allocation

organizations."[159] Through distributed, encrypted data storage, Reid and Witteman aim to socioeconomically empower billions of people.[160]

Network: The firm is creating the Identity Network (IN): "a non-profit, stewarded identity and value transfer network for the common good of the planet."[161] Everest asserts that IN will provide the technological infrastructure and protocols for every human to own and control their identity data, including biometrics. The blockchain-based network is designed to be self-funded, transparent, and to exist in perpetuity.[162] It is anticipated to go live in late 2018.[163]

Governance: The governance model will include the Identity Network Foundation (INF) charged with safeguarding the independence, transparency, and longevity of the network. Board members must be from an established NGO or international organization dedicated to socioeconomic development.[164] The targeted launch date for the INF is December 2018.[165]

Decentralized Application: The Everest decentralized application is designed to operate within the IN ecosystem. The dApp will contain EverID, described in the *Everest Whitepaper* as a "digital biometric identity system to store and confirm user identity data."[166] Everest technology creates a user identity and records user information into a proprietary, encrypted storage file: the EverID Datagram.[167] This dataset is stored on an individual's smartphone, if available and also on a network of InterPlanetary File System (IPFS)[168] nodes.

Everest plans to create and support a new economy to verify identity and record, update, store, and transfer value.[169] In order to do so, Everest will include two additional components within its platform. The first is EverWallet, a multi-currency digital wallet with built-in document storage, which is included in the Everest decentralized application.[170] The second is EverChain, a transaction system built on a private, permissioned instance of the Ethereum blockchain.[171]

Per the *Everest Whitepaper*, a robust digital identity will allow individuals to validate themselves to large organizations, such as banks or hospitals, and obtain services. In turn, these entities can use the Everest platform to cost-effectively verify user identity, track service delivery and consumption, and ensure that funds are delivered securely. The Identity Network ecosystem is intended to mitigate issues such as leakage, fraud, and inefficiency.[172]

Token & ICO: Everest will use a utility token, the ID, and a USD-pegged token,[173] the CRDT.[174] IDs will allow entities to interact with the system,[175] while CRDTS are the digital currency used to move value.[176] Institutions that want access to the Everest economy or want to operate observer/transaction nodes will gain access by purchasing and holding a predetermined number of ID tokens corresponding to their role in the network. Everest plans to conduct an initial coin offering in Fall 2018, and will issue a maximum of 800 million IDs for three rounds of financing.[177]

Every enrollment, verification, update, or transaction will require spending CRDTs. Everest intends to initially peg the CRDT to the US dollar, and each token will be equal to USD $0.01. "The goal of pegging to a known and accepted fiat currency is to achieve stability, liquidity, and transparency."[178] There is no planned ICO for the CRDT, as it will only be used to verify identities and exchange value within the Everest ecosystem.[179]

Use Cases: The Everest "testnet"[180] launched in July 2018, and Everest 1.0 is scheduled to go live in October 2018.[181] The firm is currently engaged in a health service project in Cambodia and a gas subsidy pilot project in Indonesia.[182] Other possible use cases listed on the Everest website include land administration; micro-insurance; micro-financing; cash transfers; remittances; medical records; and humanitarian aid.[183]

→ BOX 4

Live Use Cases in the Developing World: Everest[184]

Everest recently emerged from "stealth mode" and is pursuing a number of projects globally. The following use cases are examples of the many ways in which self-sovereign identity solutions can be applied in the developing world.

Cambodia

Everest has partnered with the Cambodian Ministry of Health and WAH Foundation, a local NGO, to improve infant development- and maternal health-related services in Kampong Chhnang, a central Cambodian province. Women will be enrolled into the Everest platform at local clinics, and will receive supplements relevant to pregnancy when appropriate. While the provision of medicine and related services will be transparently and immutably recorded on the Everest transaction blockchain, patient privacy will be protected via encryption. The partners believe that the pilot can improve health care administration, medical records keeping, and maternal delivery programs.

WAH Foundation founder Christopher Wilson notes that Everest technology can also help to monitor mothers from pregnancy until the thirtieth day of their child's life, enhance overall communication between medical institutions and patients, and create a value transfer platform to receive medicine. Project implementation is planned for November 2018. The pilot has the potential to scale to all 42 health centers and three hospitals in the province, which has a population of 500,000.[185]

Indonesia

Everest partnered with the Indonesian Office of the Vice Presidency[186] and the Ministry of Energy and Mineral Resources to provide propane gas subsidies via the Everest platform; funding for the project came from ID2020. An individual will be enrolled at a distribution center and receive a monthly subsidy voucher for a propane canister within their digital wallet. To redeem the voucher, users will go to a distribution center, provide their PIN, conduct a face or fingerprint scan,[187] and acknowledge receipt of gas. The voucher will be deducted from their digital wallet and the transaction will be recorded on the EverChain. This promises to reduce graft, streamline secure distribution, improve supply chain management, enable inter-agency coordination, and allow for the real-time monitoring of activities by the Indonesian government.[188] Trials for the program will begin in late 2018.

Evernym

The Basics: Evernym was founded in 2013 by Jason Law and Timothy Ruff, and is headquartered in Salt Lake City, Utah.[189] Evernym is a well known player in the digital identity space, and endeavors to "significantly ease the deployment of self-sovereign identity infrastructure in many different industries."[190] The company is perhaps best known for creating Sovrin in 2016.[191]

Network: Sovrin is designed solely for identity, and the platform is described as "the first global public utility exclusively for self-sovereign identity and verifiable [credentials]."[192] The software is based entirely on open standards, with the core network code being open sourced under the Hyperledger Indy project.[193] The Sovrin white paper asserts that platform architecture accounts for the four major

requirements of self-sovereign identity: governance, scalability, accessibility, and privacy.[194] The Sovrin Network is planned for launch in late 2018.[195]

Governance: Company leadership recognized the need to engage with digital identity, security, and privacy experts to assist with design and governance. To that end, they established the Sovrin Foundation in late 2016 as an international non-profit comprised of a Board of Trustees and a Technical Governance Board. In early 2017, the Sovrin Foundation transferred its open source code to the Linux Foundation[196] to create the Hyperledger Indy project. The foundation is now finalizing version two of the *Sovrin Trust Framework*, a document defining the business, legal, and technical terms for participation in the Sovrin Network.[197]

Decentralized Application: Evernym was difficult to distinguish from Sovrin only a year ago, but has separated itself from the governance of the platform.[198] The company is now a vendor of Sovrin-enabled software and services. Its Connect.Me wallet, a smartphone application, will enable individuals to create secure, peer-to-peer communication channels with other people and organizations.[199] The application also allows a user to manage digital keys and verifiable credentials, giving a person "true control over their digital identity for the first time."[200]

Token & ICO: Evernym does not plan to conduct an ICO, but will participate in the Sovrin ecosystem as a vendor of Sovrin based solutions.[201] Through implementation of advanced "privacy-by-design" features, including pairwise pseudonymous identifiers, peer-to-peer exchanges, and selective data disclosure through zero-knowledge proofs, Evernym believes that it can help to transform major economic sectors. The four highlighted within the Sovrin white paper are: 1. identity and access management; 2. cybersecurity; 3. regulatory technology; and 4. data integration.[202]

The Sovrin Foundation plans to create a digital token—the Sovrin token—for privacy-preserving value exchange. By providing an economic incentive for network participants, the Sovrin Foundation intends to enable a global marketplace for digital credentials of various types and values. Ancillary markets for digital credential insurance and permissioned personal data may also emerge.[203] An initial coin offering is scheduled for 2018.[204]

Use Cases: Launch of the Evernym Connect.Me application is planned for 2019.[205] The firm has already conducted a number of pilots across varying geographies and sectors. Prominent examples include a digital identity solution for credit unions, financial services in Canada, a partially completed birth registration project in Illinois, and a nationwide initiative to provide U.K. doctors with a digital passport and reputation system.[206]

→ **BOX 5**

Live Use Cases in the Developing World: iRespond[207]

iRespond is a Seattle-based nonprofit utilizing biometrics and blockchain technology to provide SSI for a variety of services in low-resource environments.[208] Peter Simpson, the executive director at iRespond, describes the organization as a "biometric service provider" and its technology as an identity "plug-in" for open platforms.

The iRespond platform records an individual's iris signature[209] and converts it into an encrypted and unique 12-digit number.[210] iRespond leverages blockchain to prevent fraud and ensure privacy. The iRespond solution also includes a cloud-based database, but can operate offline (and sync at a later time) allowing it to serve areas in the developing world with low smartphone penetration or limited coverage.[211]

By allowing users to identify themselves with an iris scan, iRespond helps marginalized individuals access services such as healthcare, education, banking, and humanitarian aid. Three examples:

East Africa

iRespond has operated in multiple East African countries since 2013. While internet connectivity is usually sufficient, there are often simple logistical challenges such as an inability to recharge phones and other electronic devices. iRespond has nonetheless been able to implement its digital identity solution to facilitate health care services related to HIV and other infectious diseases. Prominent partners across the region include Johns Hopkins Medicine and the Centers for Disease Control and Prevention.

Myanmar

iRespond has been active in Myanmar for approximately five years. The country, which suffers from unreliable electricity, poor internet connectivity, and a technologically illiterate population, has proven to be a challenging environment. Despite these obstacles, iRespond has deployed its digital identity solution to improve healthcare service delivery for infectious diseases, notably tuberculosis and malaria. The nonprofit further assists with privacy-supported HIV testing throughout the country. Multiple hospitals and clinics, and a significant number of patients, use iRespond every day.

Thailand

iRespond partnered with the government of Thailand in 2017 to fight human trafficking and labor abuse. The Thai economy has a large fishing sector, and seafood companies employ many Burmese and Cambodian migrant workers. These migrants often lack formal documentation of citizenship or work history. iRespond provides biometrically-based, unique IDs to foreign workers, preventing corporations from exploiting undocumented migrants through forced labor or "seafood slavery."[212]

Biometrics are complicated, and the related hardware costs are nontrivial. But iRespond demonstrates that biometrically-based digital identity solutions for a variety of services are possible—and even scalable—in the Global South.

uPort

The Basics: uPort grew out of ConsenSys, a Brooklyn-based blockchain firm. Rouven Heck, Michael Sena, Christian Lundkvist, and Pelle Braendgaard are considered the founders.[213] The stated purpose of uPort is to "return ownership of identity to the individual by creating a trustworthy, flexible, and inclusive identity solution that empowers people."[214]

Network: Unlike the Everest and Evernym solutions, uPort is built on the public Ethereum blockchain. Founded in 2015, Ethereum was conceived as an improvement on Bitcoin, the first public blockchain, adding support for smart contracts and decentralized applications.[215] While there is constant discussion[216] about the future of blockchain technologies, the Ethereum ecosystem—which is supported and nurtured by ConsenSys—is relatively broad and robust.[217]

Governance: uPort leadership has not expressed any intention to create a foundation for stewardship of its digital identity solution. But if uPort intends to become a major player within the space, we expect that such an entity will be created. Both Everest and Evernym will have independent foundations to safeguard the interests of users and hold all participants within their respective ecosystems to the highest possible standards. In order for uPort to remain a

viable and competitive option, an independent foundation with stewardship over uPort may be necessary.

Decentralized Application: The company website describes uPort as an "interoperable identity network for a secure, private, and decentralized web."[218] By creating base infrastructure for digital identity on Ethereum, uPort claims to "lay the foundation for a radically free, equitable, [peer-to-peer], user-centric internet society."[219] According to uPort, its dApp is simple to use and meets demanding usability, flexibility, and interoperability requirements.[220]

The firm released an updated version of the uPort ID dApp in late September 2018, and it is available to download for iOS and Android. This new version is built on the Ethereum mainnet.[221] The smartphone application allows users to register their own identity on Ethereum, send and request credentials, sign transactions, and securely manage keys and personal data.[222] Per uPort, "users are always in control of their data and they are free to share it with whoever they choose."[223]

Token & ICO: The uPort solution does not have its own token and there are no plans for an ICO. Instead, uPort is based on Ethereum and uses Ether and other ERC20-compliant tokens.[224] As such, the application will charge Gas to complete smart contract transactions within the Ethereum ecosystem.[225] Rouven Heck, co-founder of uPort, emphasized that uPort shifts costs away from the end user, as Gas fees are paid by the identity issuer.[226]

Use Cases: uPort has been applied to a number of initial use cases. These include the Gnosis prediction market, the FOAM geospatial data protocol, asset management, and online poker. In addition, uPort has completed a pilot with the city of Zug, Switzerland.[227] Through its base-layer identity application, uPort can issue "citizenship" to city residents. After input of basic information online, the scanning of a QR code associates the PII with a uPort address. Citizens must then visit Zug city hall, where the government validates the uPort ID and signs the data with a private key. The resulting credential is stored on the user's smartphone and can be used to log in to city services. A citizen of Zug can use their uPort identity to vote, access a bike-sharing service, and log in to the citizen's tax portal. As of late May 2018, approximately 300 Zug residents were registered with uPort.[228]

ConsenSys highlighted a number of benefits of the Zug pilot in a 2017 blog post: 1. reliance on the public Ethereum blockchain lowered infrastructure requirements; 2. decentralized data storage decreased the risk of cyber attack or data theft; and 3. the early version of the application, situated on a testnet, was cost effective and scalable.[229]

These Three Firms Within the Digital Identity Space

Everest, founded in 2016 and only recently emerged from "stealth mode," is a relatively new actor.[230] The California-based company is developing proprietary software, which raises eyebrows in the open source community. Nonetheless, Everest has created a potent multifunctional platform which does not require smartphones, and has conducted a number of impressive pilots with a diverse group of partners (See Box 4 above). Evernym has a longer public record in the digital identity space, having developed Sovrin and the Hyperledger Indy project.[231]

We believe that the differences between Everest and Evernym are similar to the broad differences between Apple and Google. Akin to Apple with iOS, Everest plans to operate in an integrated system where they offer services. In contrast, the indicated commitment of Evernym to open source technology is more analogous to Google and its Android Open Source Project.[232]

As a part of the ConsenSys mesh, uPort is part of an increasingly important Ethereum ecosystem. ConsenSys was founded by Joseph Lubin, co-creator of Ethereum, and it very engaged with the community.[233] Schemes include ConsenSys Labs, which "supports entrepreneurs and developers around the world as they build on the Ethereum platform," and ConsenSys Academy, an educational institution "developing the global blockchain ecosystem by bridging the Ethereum knowledge gap."[234] ConsenSys also has a number of high-profile partnerships. For example, the company is an advisor to the Government of Dubai on blockchain, and has even engaged in a proof-of-concept with the Emirate to build a blockchain-based land registry.

Exploring Three Platforms Through the Principles

The features of a digital identity solution are obviously technical, and are often explained in jargon. To many stakeholders, therefore, the specific aspects of a platform can be overlooked if it is functional overall. For example, Aadhaar appears sufficient at a distance, but it has frequently suffered data leakages[236] from its centralized servers.[237] Yet correct solution design, including data storage, accessibility, and privacy, is critical if individuals are to safely and securely utilize a digital identity every day in the real world.

Our goal is to familiarize policymakers and other stakeholders within the international development space with effective solutions to their identity problems. Utilizing our adopted set of "Principles of Identity" as a framework, we now examine the design specifications of the aforementioned firms' self-sovereign identity solutions. We aim to provide high-level overviews of the three platforms, comparing and contrasting their functionality.

Our methodology included desk research and interviews with company leadership and employees. To help ensure uniformity and impartiality, an identical and standardized set of questions was asked during interviews. General design question themes include platform architecture, governance, data storage, tokenization, key management, and biometrics. [238]

1. Inclusion - Identity should be available to all

The three firms aim to maximize inclusion within their solutions through free access to basic services.

All claim to not discriminate against potential users due to ethnicity, gender, socioeconomic status, or language. However, their respective degrees of outreach to different audiences vary.

Everest strives to include the "Bottom of the Pyramid,"[239]—the "unbanked" and the "unverified"—within its solution.[240] To accommodate for illiteracy and a lack of technological know-how, its platform will employ pictograms, biometric scans (in place of written passwords), and voice commands. Everest will also allow coaches—or "agents"—to guide users through any process.

Evernym, through Sovrin, wants to enable universal accessibility. The Sovrin white paper explicitly states that, "a global public utility for self-sovereign identity must meet the identity needs of everyone," and that "the goal must be **identity for all**."[241] The firm, through a concept of "guardians", will enable a person to manage an identity on behalf of a vulnerable individual or anyone else unable to manage their digital wallet.[242]

uPort, as part of ConsenSys, is more so configured to support people within the Ethereum community, and within the crypto-community generally. Nonetheless, the firm provided the example of red and green buttons as a cross-cultural and intuitive design feature that it is considering for use within its platform.

Everest and **Evernym** are noteworthy for two reasons. First, use of their dApps will not necessarily require smartphone ownership. Although studies do suggest that hardware penetration is increasing in the Global South, access in least developed countries is still a challenge (See Box 6 below).[243] As our study is focused on the developing world, we believe that it is essential to account for individuals lacking sufficient resources. **Everest**, in particular, intends to ease enrollment, and therefore inclusion, through the use of paid "agents" owning smartphones.

Second, the ability for an "agent" or a "guardian" to ease interaction with an identity solution can help to ensure widespread inclusion and use. Even the most intuitive and user-friendly system may still be challenging for uneducated or illiterate individuals with limited technological exposure. Important tasks, such as accessing food subsidies, voting, or scheduling a medical appointment, may seem intimidating or even impossible no matter how "simple" a process has been designed to be.[244]

→ BOX 6

Smartphones and the Developing World

The term "smartphone" refers to hardware that enables a user to connect and transfer data to an external network and/or the internet. Through decentralized applications, these gadgets essentially serve as entry/exit points to an SSI platform and its wider ecosystem.[245]

Most stakeholders within the space believe that users will usually access their self-sovereign identity via smartphones with internet connectivity. Recent statistics concerning mobile phone penetration and internet access throughout the developing world suggest that the implementation of SSI solutions is possible and will likely become easier with increased smartphone penetration.

- According to the Pew Research Center, "the share of people who use the internet or own a smartphone continues to expand in the developing world." Between 2013 and 2014, a median of **42 percent** of respondents across 19 emerging and developing economies said they accessed the internet at least occasionally or owned a smartphone. By 2017, a median

of **64 percent** of respondents across these countries responded the same.

- A 2017 report by the International Telecommunication Union indicated that the penetration rate for mobile subscriptions was at **98.7 percent** in developing states. Even in least-developed nations, the penetration rate was at **70.4 percent** and rising. The report suggested that there will soon be more than one subscription per person except in the world's poorest countries.

- The World Bank reports that "all regions of the world are gaining access to the internet and mobile phones, with mobile phones driving a great deal of the gains. In sub-Saharan Africa, more than **60 percent** of individuals now have access to a mobile phone…mobile phones are superseding or preceding other communication methods as the technology of choice for individuals looking for greater interconnectedness."

- As a caveat, the World Bank 2016 World Development Report, *Digital Dividends*, cautions that, "despite the rapid spread of digital technologies, more than 800 million people lack mobile access worldwide (**63 percent** of them in the bottom **40 percent** of the income distribution), and 4.3 billion lack internet access (**49 percent** in the bottom **40 percent**). For every person connected to the internet in developing countries, almost three are not, and in some countries, 20 are not."

Mobile phones are not identical to smartphones, but trends do suggest the trajectory of increasing smartphone penetration in the developing world in the coming years.[251]

---

2. Control - Users must control their own identities

Individuals, not technology companies or governments, must have ultimate control over their identities and related PII. Only users should be able to access, update, share, hide, or delete their personal data. No self-sovereign identity firm, or any other third party, should ever be able to revoke an identity. All three firms agree, but will enable an individual user to possess and control their self-sovereign identity through different methods.

The **Everest** solution will allow only a user to "unlock" their EverID Datagram. This will be accomplished via biometry—a faceprint and/or a fingerprint scan—

and a PIN/password. Lacking smartphone ownership, a user will be able to control their data through an "agent device."

Decentralized storage of private keys and personal data within the Everest solution will further ensure user control. Through the Identity Network Foundation (INF) supernode infrastructure,[252] data will be stored in IPFS, spread across multiple data centers and various geographies.

Everest will further provide for the ability to recover control of an identity. Through provision of biometrics and successful completion of a "challenge process," a user can regain command of their EverID Datagram on any Everest-enabled hardware device. We believe that this feature is especially pertinent to the developing world, as social upheaval, natural disasters, and large-scale population movements can easily result in the loss of a personal device.

Evernym will store all personal data on the user's smartphone. If desired, PII and a "recovery key" can also be encrypted and stored on the cloud. Control in the Evernym solution will also be enabled through biometry; but the Connect.Me dApp will use the default biometrics on a given smartphone.

The Evernym solution will provide a simple export/import option to recover a private key and therefore control of an SSI.[253] While the firm did not provide details, exportation of a private key usually involves the creation of a file containing private key data and its transfer to a new or different wallet. An individual can generally import a private key into a digital wallet via a text file or QR code scanning.[254]

Tech savvy individuals may find this process relatively simple and straightforward. But a refugee is unlikely to carry along a text file containing Evernym private key data as they flee violence; a poor migrant worker may lack the resources and knowledge to manage their key in such a way. The aforementioned ability to backup both PII and a key in the cloud, as well as the potential to designate a "guardian," may mitigate this concern in the developing world.

uPort stores private keys and PII on user smartphones, and does not necessitate the use of biometrics to enable control of a self-sovereign identity. An individual can use the standard biometric functions of a smartphone as an additional security layer, but the solution only necessitates provision of a PIN and a basic password for control. In general, uPort is concerned with the potential for biometrics to allow for identity correlation.[255]

uPort relies on a seed phrase to recover control of an identity.[256] In regard to its target audience, it should be relatively easy for a member of the crypto-community to record a seed phrase for later use. Vulnerable individuals—such as IDPs, refugees, and persecuted minorities—in developing countries might

encounter considerably greater obstacles in storing their own seed phrases for quick access.

Overall, user control of an identity will allow individuals to selectively update, share, hide and delete personal information. Decentralized and encrypted storage can also limit third-party access to data and should bolster privacy.[257] For marginalized populations in the developing world especially, control over identity is crucial. Selective disclosure of PII can help to protect ethnic and religious minorities, women and children, migrants, and individuals diagnosed with infectious disease such as HIV from discrimination, abuse, and violence.

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

Self-sovereign identity firms should endeavor to create easy enrollment in, and access to, their platforms. Indeed, all three will allow for self-enrollment within their solutions. At a minimum, an individual must input basic demographic and/or biometric data to satisfy enrollment requirements.

Enrollment and subsequent access will require interaction with hardware—typically a smartphone or tablet, or possibly a laptop—and internet connectivity (See Box 6 above). Reliance on these devices might compromise access in the developing world, but this could be mitigated via agents and/or public access centers. Additionally, hardware is constantly improving and becoming more affordable. Humanity continues to urbanize, and technological resources tend to be more readily available in cities.[258]

Everest will employ coaches—or "agents"—to help users without smartphones enroll and access its solution. Following user provision of biometrics to an "agent device," pre-designated "agents" should be able to guide individuals through any process in the Everest platform. These "agents" will be compensated based on the subsequent economic activity of previously enrolled users.

This arrangement may become less necessary with increasing rates of smartphone ownership and accompanying technological literacy. But a network of Everest "agents," employed to enroll and authenticate users without personal devices, would be especially helpful during and after chaotic population upheavals caused by conflict or natural disasters. Perhaps multiple Everest "agents" would be present in a refugee camp within such a scenario, allowing for continued access to self-sovereign identities.

Evernym, via Sovrin, will include a concept of "guardianship." The feature will enable a trusted party to manage the identity of a vulnerable person. We believe that Evernym is prescient to allow for this possibility within its solution design. There will always be defenseless individuals in the world, such as sex-trafficked children, the elderly, refugees, or people who are ill. The Evernym decentralized

application will allow pre-designated and responsible "guardians" to manage self-sovereign identities in the best interests of these groups.

uPort does not currently plan to utilize "agents" or "guardians" within its solution. But the firm does attempt to expand access by reducing reliance on a specific hardware device. uPort asserts that an individual smartphone, or any other device, is not part of a user's decentralized identifier (DID)[259] within its solution. This allows individuals to switch devices without the loss of an SSI, and protects against the loss or replacement of a device.

→ BOX 7

Multiple Enrollments & DIDs

The platforms have significantly different opinions regarding if one person can or should have multiple identifiers on their platform. The debate becomes philosophical quickly and is beyond the scope of this paper.

- During enrollment, **Everest** will cross-references a single-purpose database of encrypted and anonymized biometric data that flags attempts by existing users to create new accounts. The firm holds that one individual should only have one identity on their platform.

- **Evernym** stated that organizations utilizing the Connect.Me dApp will be responsible for identifying and authenticating users before issuing credentials, and for enforcing any duplication requirements within their own "trust frameworks." Of note, Evernym does enable the use of multiple decentralized identifiers on their platform (See "9. Minimization - Disclosure of identity information must be minimized" in this section).

- **uPort** reviews previously enrolled phone numbers whenever a new user creates an identity. An individual could theoretically create a second identity through possession of a second phone number. But uPort maintains that it becomes harder to possess multiple IDs in relation to sensitive applications of the solution—such as KYC/AML—that require verifiable credentials issued by governments or employers.

---

4. Transparency - Systems and governance must be transparent

Transparent governance and open solution design should help individuals make informed decisions about their identities and PII. As demonstrated in Figure 2, we believe that a suitable model for an SSI ecosystem includes a platform, a private firms providing value-added services for that platform, and an independent foundation stewarding the platform.

Everest plans to establish the Identity Network Foundation (INF) in December 2018. The INF will be a nonprofit organization and will govern the Everest ecosystem.[262] As previously mentioned, INF board members must originate from an established NGO or international organization committed to socioeconomic development. Everest states that the INF "is designed to ensure transparency, neutrality, security and longevity of the Identity Network."[263]

The Everest platform is based on two private and permissioned instances of the Ethereum blockchain.[264] Everest believes that there is no need for the general public to access its technology through any mechanism other than the dApp or the software development kit/application programming interface (SDK/API).[265] Everest utilizes Ethereum code specifically because "it is a proven, trusted open-source system which is built by a highly-engaged distributed organization and which has a vibrant developer community."[266]

Evernym, and the Sovrin ecosystem, will be governed by the Sovrin Foundation, an international nonprofit organization. The Sovrin Foundation Board of Trustees consists of 13 individuals from around the world and is bounded by the *Sovrin Trust Framework*, a set of business, legal, and technical policies originally published in June 2017.[267]

Through the Sovrin Network, Evernym uses an open source, hybrid architecture that provides access in a permissioned ledger. The overlying identity system does not require permissioning; only the need to be cheap and fast.[268] Any individual and/or organization will be allowed to enroll and create DIDs. But all nodes, and most importantly, validator nodes,[269] will be managed by stewards. Organizations are invited by the Sovrin Foundation to become a steward, and must agree to act in accordance with the rules set out in the *Sovrin Trust Framework*.[270]

Responsible governance provided by the INF or the Sovrin Foundation, along with secure blockchain implementation, might help to prevent the misuse of digital identity and PII in the developing world. For example, in contrast to the poorly-defined legal framework surrounding official use of Aadhaar-related data, [271] a limited, enforceable, transparent set of rules—such as the *Sovrin Trust Framework*—could mitigate against unwarranted data collection and location

monitoring. Malicious actors might be prevented from tracking and targeting marginalized groups, ethnic, religious, or otherwise.[272]

The **uPort** platform, which was conceived as base infrastructure for projects requiring digital identity-- does not have a governance model. Leadership has not declared an intention to create a foundation analogous to the INF or the Sovrin Foundation, yet we believe that such an entity is necessary if uPort aims to become a major player within the digital identity space. This independent organization could help to protect users' interests and to ensure that all actors within the ecosystem behave accordingly.

uPort is based on the open source and public Ethereum blockchain, largely because it is relatively easy to create a wide range of decentralized applications using the technology. This choice noticeably introduces additional costs, as the public Ethereum blockchain requires expensive computational activity and Gas fees in order to add new transactions to the ledger.

Table 5: Blockchain Implementations of the Self-Sovereign Identity Firms

Self-Sovereign Identity Firm	Blockchain Implementation	Reasoning
Everest	Permissioned Ethereum Blockchain	- Privacy/protection of Everest technology - Trusted system backed by highly-engaged organization and active developer community
Evernym	Hybrid Hyperledger Indy Blockchain	- Public: anyone can use identity ledger - Permissioned: achieve trust in Sovrin as a global public utility[273]
uPort	Public Ethereum Blockchain	- A tool for dApps within Ethereum ecosystem

5. Persistence - Identities must be long-lived

A self-sovereign identity solution must last for decades, at least. An individual should possess an identity from birth until death. Each firm also recognizes the need for long-term persistence, although they have developed very different strategies for achieving this goal. These schemes are rooted in both foundational infrastructure and commercial/operational models.

At the core of the **Everest** solution are two private Ethereum-based blockchains: the EverChain, a blockchain-based transaction system, and the EverID blockchain, which includes a pointer to the storage location of the EverID Datagram on IPFS and a hash[274] of the EverID Datagram for integrity checks.[275] Everest supernodes, which host the two blockchains, will be operated by members of the Identity Network Foundation.

The two Everest blockchains will exist in parallel to the public Ethereum blockchain. The private and permissioned network will utilize independent software and hardware and Everest leadership maintains that their solution would be unaffected if the Ethereum mainnet were to suddenly disappear.[276]

Everest claims that its solution will reduce fraud and leakage, possibly saving significant sums for organizations globally, and that it will "make identity verification at scale more cost-effective than ever before."[277] Although these benefits, if realized, might lead to widespread adoption, the Everest business model also involves driving other economic activity within its ecosystem. The firm will charge entities for access to its multi-functional marketplace, and will levy small fees for specific user actions.[278]

Evernym will be based on the Sovrin Network, a purpose-built blockchain for self-sovereign identity. As of late July 2018, forty-one Sovrin stewards have commited to host network nodes in at least 12 countries.[279] Evernym infrastructure for the Connect.Me dApp will be primarily hosted on the AWS.

We are cautiously optimistic regarding the persistence of Sovrin, despite the fact that the blockchain is single-purpose. By electing to make the software open source as Hyperledger Indy, Evernym has positioned the network for widespread adoption and has likely increased its odds of persisting.[280] In addition, the Sovrin steward framework, with companies such as IBM, Cisco, and ATB signed on to operate nodes, suggests that the ecosystem has staying power.[281]

The Sovrin Foundation claims that the Sovrin Network can help to mitigate the enormous costs—hundreds of billions per year globally[282]—related to cybercrime and data breaches.[283] The white paper specifically asserts that the Sovrin Network could reduce costs and increase efficiency in the major industries of: identity and

access management; cybersecurity; regulatory technology; and data integration.[284]

For its part, Evernym maintains that its Connect.Me dApp will lower the costs and risks of identity verification. The firm will therefore sell its identity verification "toolkit"—which includes the Hyperledger Indy SDK, a user interface, and its mobile application—to institutions on a subscription basis.[285] Evernym also plans to support the Sovrin Network through future products and services.

uPort, as part of ConsenSys, is dependent on the live, public Ethereum blockchain and views itself as an enabler of the ecosystem. But the uPort team does not host any servers. dApp developers must maintain the physical infrastructure of the platform instead.

The working assumption within its community is that Ethereum will persist.[286] The platform is "generalized so that anyone can program it for their specific needs."[287] This versatility may very well incentivize widespread adoption of the technology. At present, Ethereum has a market cap exceeding $20 billion, over 1,900 decentralized applications, and scores of developers building upon it.[288]

uPort asserts that its foundational identity infrastructure will always be free to the user. Only entities need to pay Gas costs in order to validate credentials. Eventually, uPort would like to be utilized in an identity validation market, and anticipates requiring organizations to pay fees. The firm hopes to gain a better understanding of a holistic and viable business model as the underlying Ethereum platform evolves.[289]

Table 6: The Persistence of Self-Sovereign Identity Solutions

Self-Sovereign Identity Firm	Ecosystem	Business Model
Everest	Private Ethereum Blockchains - INF Supernodes - Private chains - Unaffected by loss of Ethereum mainnet	- Charge entities for access to multi-functional platform[290] - Levy small fees for specific user actions

Self-Sovereign Identity Firm	Ecosystem	Business Model
Evernym	Sovrin Network - Hyperledger Indy - Steward Framework including IBM, Cisco, and ATB	- Sell identity verification "toolkit" to institutions on a subscription basis - Support Sovrin ecosystem through other products and services
uPort	Ethereum - Utility of smart contracts and dApps - Engaged and growing community - Ecosystem valuation	- Eventually aims to be utilized in an identity market and will require entities to pay a small access fee - Will gain better understanding of business model as Ethereum matures

Even given viable incentives for adoption, or sustainable business models, there is no guarantee that any solution will be utilized and/or exist in perpetuity.[291] We remain confident but guarded about each. While unlikely, it is not impossible that a network could fail. The ability for users to transport their identity to another system is clearly crucial.

6. Portability - Identity information and services must be transportable

It should be possible for the user to transport their identity and any related data from one platform to another, different platform. The wider community is aware of this necessity and is currently within the process of establishing open standards at forums such as the Decentralized Identity Foundation (DIF)[292] and the World Wide Web Consortium (W3C).[293] Due to this extensive collaboration, we expect that the transportation of a self-sovereign identity will be possible in the future.

The digital identity firms claim to account for portability within their solutions:

- **Everest** is planning for the user to be able to transport their self-sovereign identity to another platform through use of DIF standards.

- **Evernym** noted that the *Sovrin Trust Framework* states that, "the design, governance, and operation of the Sovrin Network shall provide Members with portability of their Public Data and Private Data to the greatest extent feasible consistent with the other principles herein."

- **uPort** leadership maintained that the transfer of an identity and any pertinent data to another service would be intuitive.

The use of open source code, open standards, and a standard process for private key recovery[296] may reduce dependence on any single solution. But the actual process of transporting a self-sovereign identity from "solution A" to "solution B" remains unclear from available resources. One reason that firms will need to address interoperability is to be able to manage against vendor lock-in --people are not going to invest in an SSI solution if they are not able to get out at a later date.

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

The digital identity space is becoming increasingly competitive, and it is far from clear if any particular platform will experience widespread and predominant adoption in the future. As the community expands, solutions must be able to communicate with each other at scale. Governments and large organizations will greatly value the ability to choose a distinct SSI solution and still be able to communicate quickly and efficiently with entities that decided to adopt a different platform.

Although Kaliya Young recently observed that there is still a significant amount of work to be done regarding interoperability, important stakeholders are coordinating with one another to build a broad, interoperable ecosystem.[297] This is still clearly an evolving arena, but the digital identity firms within this report have signaled use of common technical standards:

- **Everest** stated that its solution will be able to interoperate with existing systems over its API or Conduit System, and with other SSI solutions based on DIF standards.

- **Evernym**, as well as the larger Sovrin ecosystem, will adhere to emerging DIF and W3C standards, as well as a communication protocol derived from the open source Hyperledger Indy project.

- **uPort** shared that it is an active member of the W3C, and that its architecture complies with accepted Ethereum, smart contract, and verifiable credential standards.

Significant attention has been directed towards the interoperability of decentralized identifiers, or DIDs. According to Michiel Mulders, a blockchain developer at TheLedger,[301] a DID is "nothing more than a scheme with several attributes that uniquely identifies a person, object, or organization."[302] DIDs are fully owned and controlled by the "DID subject," independent from any centralized registry, identity provider, or certificate authority. Additionally, every DID is cryptographically secured by a private key managed by the owner. [303]

Markus Sabadello, CEO of the digital identity and personal data company Danube Tech, notes that "DIDs are an important innovation because they give us the ability to establish digital identifiers that are persistent, secure, and globally resolvable."[304] And because the technology is based on an open standard, any self-sovereign identity vendor can create a "DID method," defining how DIDs are written and read on their particular blockchain.[305]

Everest currently perceives the use of DIDs as unnecessary within its solution. Leadership does view the principle of interoperability as important within the SSI space, but does not believe that the DID protocol has reached an adequate level of sophistication for adoption at present. Everest does not want to risk the security of PII through interoperability at this moment.[306]

In contrast, the **Evernym** solution will utilize multiple, pseudonymous DIDs in order to prevent identity correlation (See "9. Minimization - *Disclosure of identity information must be minimized*" in this section). A unique DID will be created for every new connection between individuals, and also for every new relationship between an individual and organization, within the Sovrin Network.

uPort also incorporates the decentralized identifier into its solution. The firm critically does not use multiple DIDs, however. uPort considers the extensive writing of data on to the Ethereum ledger to be too expensive to do so.

The Decentralized Identity Foundation is currently developing a "Universal Resolver" to enable communication between DIDs situated within different solutions. This software[307] will retrieve information, such as the "DID method," public key, and service endpoint, of a particular decentralized identifier, allowing for the more widespread formation of relationships, transactions, data sharing, and messaging. Both **Evernym** and **uPort** decentralized identifiers are included in the initial phase of this project.[308]

→ **BOX 8**

Scaling of the Self-Sovereign Identity Solutions

A self-sovereign identity solution may experience millions of data writes, data reads, and transactions each day given interoperability and worldwide expansion. The Everest target population includes 1.1 billion people without a verifiable identity, 2.6 billion people without a bank account, and 5 billion people without a smartphone.[309] The Sovrin Foundation aims to create a global public utility for self-sovereign identity that meets the needs of *everyone*; its whitepaper explicitly mentions the 1.1 billion people worldwide without a legal identity.[310]

Blockchain technology has already suffered from issues related to scalability and transaction times.[311] Although a number of resolutions have been proposed and/or are in development,[312] it is critical for digital identity firms to account for scalability:

- **Everest** asserts that its EverID blockchain will ensure that user validation is quick and cost-effective, as it will cost only a few USD cents per validation. The firm states that EverChain, its private and permissioned transaction blockchain, will be able to handle a volume of billions of transactions a month—with the ability to scale to trillions—utilizing the Proof-of-Authority consensus mechanism.

- **Evernym** did not express much concern regarding scalability, as the company stated that the majority of user connections within its Connect.Me dApp are pairwise and/or peer-to-peer, and do not require interaction with the Sovrin public ledger. Still, the Sovrin Foundation is aware of potential issues related to scalability once the Sovrin Network goes live. The Sovrin whitepaper reads:

> If you image every person, organization, or thing needs a collection of DIDs—one for every relationship they have—then it is easy to imagine that there could be trillions of DIDs in a globalized decentralized identity system…to overcome this hurdle, the Sovrin Network is designed to use two rings of nodes: a ring of validator nodes to accept write transactions, and a much larger ring of observer nodes running read-only copies of the blockchain to process read requests.[315]

- The Ethereum community currently recognizes that scalability is an issue, largely because the public Ethereum blockchain only processes about 15 transactions per second. Developers are actively attempting to solve the problem, and **uPort** recently shared a resolution for its platform:

> Instead of registering one or multiple smart contracts on the blockchain, all [a user] must do now is create an Ethereum key pair...since no transaction is needed, [an identity] is strictly speaking anchored on the blockchain rather than created on the blockchain...the process is so rapid and seamless that millions of identities could be created in a single day...this means [uPort] can finally support very large-scale applications, such as national identity projects[317] (See "10. Protection - Users' right to privacy must be protected).

---

8. Consent - Users must agree to the use of their identity or data

The recent creation of massive and centralized databases by firms, such as Facebook and Equifax, and by governments, such as India with Aadhaar, has resulted in controversial and often unauthorized use of personal data.[318] Digital identity firms should prevent misuse of personally identifiable information by requiring organizations to ask for explicit and repeated permission to access, utilize, and share user data.

Everest will require user biometry to access a EverID Datagram and any related data. PII will not be able to be accessed and shared otherwise. The firm even plans to incorporate "proof-of-aliveness" tests within its biometric system in order to prevent replay attacks.[319]

The **Evernym** Connect.Me dApp will necessitate user biometrics in nearly all circumstances to access a particular identity and its associated information. Individuals will also be obligated to provide biometric data to create peer-to-peer communication channels with other people and organizations; to accept credentials from an issuer; and to share credentials.

uPort stated that PII within its solution can never be accessed without explicit permission from the user. Any and all data requests are displayed in a clear and concise format for approval or rejection.

In most cases, nearly all adult users should be able to express consent when using a self-sovereign identity solution. But we believe that self-sovereign identity should be provided from birth to death. Infants and younger children will not be able to understand requests and give consent for a third party to access their personal data.

As the **Everest** solution is designed to provide a self-sovereign identity across a human lifespan, the firm plans to enroll minors and associate them with their parents who have custody of them.

Evernym, through the *Sovrin Trust Framework*, ensures that adults will be able to operate in a "guardianship" capacity for identity owners who cannot manage their own SSI, including minors.[320]

uPort does not explicitly claim to provide self-sovereign identity for a complete lifetime. This feature is likely unnecessary, as the decentralized application is largely designed for use by the Ethereum community. Leadership nevertheless claimed their intention to include a function for the management of others' digital identities in a future version of its dApp.

The need for privacy and the ability to consent to, or deny, the sharing of PII is increasingly recognized as a right throughout the industrialized world, as demonstrated by the 2018 EU General Data Protection Regulation and the 2018 California Consumer Privacy Act.[321] This ability to safeguard sensitive personal information is also vital for vulnerable groups.

For example, a recent UNHCR initiative collected the biometric data of Rohingya refugees in order to more effectively distribute humanitarian aid; but the agency also shared this information with the Bangladesh Government. This intimate information has been used to control refugee movements in Bangladesh as a result. Worse, "the fear for the Rohingya is that this biometrically-enabled control system could be used to send them back to Myanmar."[322] Hundreds of thousands of lives are threatened, as Rohingya PII may be given to Myanmar officials during the repatriation process. A government accused by the United Nations of a "textbook example of ethnic cleansing"[323] could soon possess their targets' most sensitive data.[324] Self-sovereign identity, adequately incorporating the principle of consent, could mitigate similar dangers in the future.

9. Minimization - Disclosure of identity information must be minimized

Identity correlation and subsequent fraud have recently proliferated throughout the developing world.[325] A self-sovereign identity solution should lessen the real-world identification of users. A 2013 *Scientific Reports* article notes that "re-identification" of an individual only requires a few seemingly unrelated fragments of information;[326] minimization of data exposure is therefore crucial.

Everest asserts that there will be no method to correlate biometric data with an underlying EverID Datagram within its solution. In addition, the Everest system will not be exposed to open data traffic because it will be private and permissioned. The firm will protect user information through a "layers of the

onion" approach, requiring any individual to complete unique challenges in order to progressively access more sensitive data.[327]

By way of comparison, **Evernym** connections within the Sovrin Network will be associated with a "pairwise-pseudonymous identifier," or a unique DID for every relationship. As explained in the Sovrin white paper:

> Imagine that when you open a new account with an online merchant, instead of giving them a credit card number or phone number, you gave them a DID *created just for them*. They could still use this DID to contact you about your order, or to charge you a monthly subscription, but not for anything else. If the merchant suffered a breach and your DID were compromised in any way, you would just cancel it and give them a new one—*without affecting any other relationship*...Not only can the criminal not use it anywhere else, but the moment either you or the merchant detects a problem, you simply can change the DID. The giant data breaches we are experiencing today, like Equifax and Yahoo, would become a relic of the past.[328]

uPort is aware that public blockchains such as Ethereum are available for all to read and analyze. Malicious actors might then be able to track public data and public actions back to a common identity.[329] The firm conceals all transactions within its solution using Secure Hash Algorithms 2/3,[330] as they believe that hashing can help to prevent identity correlation.

Of note, uPort suggests that, "one simple improvement is for identity systems and wallets to promote the use of application-specific accounts." This design feature "makes it much more difficult to track a single user across the applications they use just by analyzing the blockchain."[331]

Perhaps the most substantial difference related to the principle of minimization is the use of zero-knowledge proofs (ZKPs):

- Both **Everest** and **Evernym** will attempt to further reduce the risk of identity correlation utilizing ZKPs.

- **uPort** does not, believing that the technology is immature, computationally intensive, slow, and expensive.

Like other design principles, data minimization is particularly helpful to marginalized groups. Ethnic and/or religious minorities could adopt a self-sovereign identity solution without fear that their personal data could be used to identify and persecute them. Refugees could access humanitarian aid without fear of being added to a centralized list. Citizens subject to a volatile political

systems could vote for an opposition party without fear of repercussions. SSI may allow individuals to assert their rights while also protecting their privacy.

10. Protection - Users' right to privacy must be protected

Recent data management scandals, along with many companies' self-proclaimed prerogative to collect PII, have amplified demands for better protection of users' right to privacy.[332] In order to better serve their users, digital identity firms must incorporate "privacy-by-design" into solutions:

- **Everest** plainly states "that privacy is a human right" within its whitepaper.
- **Evernym** will incorporate "privacy-by-design" into its solution, as the *Sovrin Trust Framework* declares that, "the design, governance, and operation of the Sovrin Network shall follow the principles of Privacy by Design to provide Members with privacy for their Sovrin Identities and Private Data."
- **uPort** specifically acknowledges the need for privacy in the description of its platform.

Cryptographic key management is vital for user protection in any self-sovereign identity solution. A user's public key is accessible for anyone to use; it encrypts data. A private key decrypts data into readable information.[336] Basically, whoever or whatever "owns" the key pair has access to the related data.[337] If a private key is not stored within a secure and well-managed location, it can be stolen, allowing hackers and/or criminals to decrypt data, read messages, and possibly control an identity.[338]

Everest will store a user's private key within their EverID Datagram. The system will manage this key, and a user will be required to present their biometric data and enter a PIN in order to gain access to their private key. Everest will write encrypted public keys on to EverChain, its private transaction system.

The **Evernym** Connect.Me dApp will directly issue private and public keys, which will then be stored on the user's personal device. The solution will write DIDs—and not public keys—on to the Sovrin ledger. Public keys will instead be written to the associated DID documents[339] of identity owners.

The **uPort** decentralized application issues cryptographic keys, and the private key is stored on the user's personal device. The solution writes public keys directly on to the public Ethereum blockchain to serve as a decentralized identifier.

Table 8: Key Management

Self-Sovereign Identity Firm	Writes on a Blockchain	Private Key Storage
Everest	Encrypted public keys on Everchain, its private transaction blockchain	Stored within EverID Datagram and protected by biometry and PINs/ passwords
Evernym	DIDs on Sovrin ledger	Personal device
uPort	Public keys on public Ethereum blockchain	Personal device

The protection of users' right to privacy is already necessary in the developing world. In Africa and Asia, less than 40 percent of countries have passed legislation to secure data protection and privacy.[340] Most prominently, India currently does not have any comprehensive national law protecting personal security through privacy.[341] As a result, some argue, there are relatively weak and ill-defined protections dictating the use of Aadhaar data.[342]

Notes

1 Blockchain is a type of distributed ledger technology (DLT). The World Bank defines DLT as, "a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants" (FinTech Note No. 1, Distributed Ledger Technology (DLT) and Blockchain, World Bank Group, 2017, http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf). While not all distributed ledgers employ blockchain technology, this report will refer almost exclusively to the blockchain model of DLT. Note also that there is no single, rigorous definition of blockchain.

2 See J. Michael Graglia and Christopher Mellon, "Blockchain and Property in 2018: At the End of the Beginning," Innovations 12, no. 1-2 (Summer-Fall 2018).

3 The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel, World Economic Forum and Accenture, January 2018, www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf, accessed April 25, 2018.

4 Dan Gisolfi, "Self-sovereign identity: Why blockchain?," Blockchain Unleashed: IBM Blockchain Blog (blog), IBM, June 13, 2018, http://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/, accessed October 1, 2018. Also, cryptographic keys are code employed by a user to set off algorithms for data encryption and decryption. Information can therefore be transmitted and stored in a more secure and private manner ("Private Key," Techopedia, accessed June 26, 2018, http://www.techopedia.com/definition/16135/private-key).

5 "The Future Has Arrived --It's Just Not Evenly Distributed Yet," Quote Investigator, accessed September 28, 2018, quoteinvestigator.com/2012/01/24/future-has-arrived/.

6 "#Envision2030 Goal 16: Peace, Justice, Strong Institutions," UN Division for Social Policy and Development Disability, accessed April 25, 2018, http://www.un.org/development/desa/disabilities/envision2030-goal16.html.

7 Identity For Development (ID4D), "Country Action," World Bank Group, accessed September 27, 2018, http://www.id4d.worldbank.org/country-action.

8 Andrea Valdez, "Everything You Need to Know About Facebook and Cambridge Analytica," Wired, March 23, 2018, http://www.wired.com/story/wired-facebook-cambridge-analytica-coverage/, accessed September 25, 2018.

9 Alfred Ng, "How the Equifax hack happened, and what still needs to be done," CNET, September 7, 2018, http://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/, accessed September 25, 2018.

10 Tech2 News Staff, "Aadhaar Faces Yet Another Data Leak Allowing Access to Personal Data to "All" Enrolled in the System: Report," Firstpost, March 24, 2018, http://www.firstpost.com/tech/news-analysis/aadhaar-faces-yet-another-data-leak-allowing-access-to-personal-data-to-all-enrolled-in-the-system-report-4403621.html, accessed September 18, 2018.

11 Mike Isaac and Sheera Frenkel, "Facebook Security Breach Exposes Accounts of 50 Million Users," The New York Times, September 28, 2018, http://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html, accessed September 28, 2018; Will Oremus, "The Massive Facebook Hack Might Have Affected Other Apps and Websites, Too," Slate, September 28, 2018, http://www.slate.com/technology/2018/09/facebook-hack-50-million-affected-apps-other-websites.html, accessed October 1, 2018.

12 Alan Gelb and Anna Diofasi Metz, Identification Revolution: Can Digital ID Be Harnessed for Development? (Washington, DC: Center for Global Development, 2018).

13 Alan Gelb and Anna Diofasi Metz, "Identification Revolution: Can Digital ID be Harnessed for Development? A New Book from CGD," Commentary and Analysis (blog), Center for Global Development, January 16, 2018, http://www.cgdev.org/blog/identification-revolution-can-digital-id-be-harnessed-development-new-book, accessed October 1, 2018.

14 Personally identifiable information "means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information" (Legal Information Institute, "2 CFR 200.79 - Personally Identifiable Information (PII)," Cornell Law School, accessed August 28, 2018, http://www.law.cornell.edu/cfr/text/2/200.79).

15 Elizabeth Renieris and Dazza Greenwood, "Do we really want to "sell" ourselves? The rise of a property law paradigm for personal data ownership.," Medium (blog), September 23, 2018, medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa, accessed October 1, 2018.

16 See Jem Matzan, "Leaving Your Identity at the Bar," Pacific Standard, June 9, 2008, psmag.com/economics/leaving-your-identity-at-the-bar-4502, accessed September 25, 2018.

17 Katherine Noyes, "5 things you need to know about data exhaust," PCWorld, May 13, 2016, http://www.pcworld.com/article/3069507/5-things-you-need-to-know-about-data-exhaust.html, accessed October 1, 2018.

18 For an extreme take on data exhaust, see Dr. Jeremy Bailenson's op-ed "Protecting Nonverbal Data Tracked in Virtual Reality" about what is collected during virtual reality sessions. While not the direct focus of this paper, it speaks to the issue of how technology is racing beyond our appreciation of what is being gathered about us (Jeremy Bailenson, "Protecting Nonverbal Data Tracked in Virtual Reality," JAMA Pediatrics 172, no. 10 (October 2018), http://vhil.stanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf).

19 Matt Burgess, "What is GDPR? The summary guide to GDPR compliance in the UK," Wired, June 4, 2018, http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018, accessed September 25, 2018.

20 Faine Greenwood, Caitlin Howarth, Danielle Escudero Poole, Nathaniel A. Raymond, Daniel P. Scarnecchia, "The Signal Code: A Human Rights Approach to Information During Crisis," Harvard Humanitarian Initiative, January 2017, http://hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis, accessed August 29, 2018.

21 See "What if People Were Paid for Their Data," Me dium (blog), The Economist, July 11, 2018, medium.com/@the_economist/what-if-people-were-paid-for-their-data-8df63f021e38, accesed July 17, 2018; and Elise Thomas, "Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database," Wired, March 12, 2018, http://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh, accessed July 10, 2018.

22 Social Protection and Labor Team, PMT-based social registries: Integrating social registry with ID systems, World Bank Group, accessed August 30, 2018, http://olc.worldbank.org/sites/default/files/3.pdf.

23 Ibid.

24 In a recent report, Identity in a Digital World: A new chapter in the social contract, the World Economic Forum lays out a progression of three "System Archetypes" for digital identity: centralized, federated and decentralized. This essentially collapses

Allen's phase two and three into one "federated" bucket, while giving SSI a light touch with the term decentralized. It is curious that the WEF did not name or further explore SSI, but perhaps their framework is better suited for the current moment, while Allen's is helpful to appreciate how we arrived here (Identity in a Digital World: A new chapter in the social contract, World Economic Forum, September 2018, www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf, accessed September 24, 2018).

25 As an aside, see "Home," Handshake, accessed September 21, 2018, http://handshake.org.

26 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, accessed April 25, 2018.

27 Allen, "The Path to Self-Sovereign Identity."

28 Ibid.

29 Comment from Kaliya Young (September 22, 2018).

30 "Verified Credentials Data Model 1.0: Expressing verifiable information on the web (W3C Editor's Draft 28 August 2018)," World Wide Web Consortium (W3C), August 28, 2018, w3c.github.io/vc-data-model/#introduction, accessed August 28, 2018.

31 A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. The digital equivalent of a handwritten signature or stamped seal, but offering more security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide added insurances of evidence to origin, identity, and status of an electronic document, transaction, or message, as well as acknowledging informed consent by the signer (Margaret Rouse and Michael Cobb, "Definition: digital signature," WhatIs.com, TechTarget, lasted updated November 2014, searchsecurity.techtarget.com/definition/digital-signature, accessed August 29, 2018).

32 "Verified Credentials Data Model 1.0," World Wide Web Consortium (W3C).

33 Phillip Windley, "How blockchain makes self-sovereign identities possible," Computerworld, January 10, 2018, http://www.computerworld.com/article/3244128/security/how-blockchain-makes-self-sovereign-identities-possible.html.

34 Russ Juskalian, "Inside the Jordan refugee camp that runs on blockchain," MIT Technology Review, April 12, 2018, http://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/, accessed August 29, 2019.

35 "The Problem," Evernym, accessed September 25, 2018, http://www.evernym.com/problem/.

36 Jacob Poushter, Caldwell Bishop, and Hanyu Chwe, "Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones," Pew Research Center, June 19, 2018, http://www.pewglobal.org/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/, accessed September 18, 2018.

37 Daniel Staesser, "The Emergence of Mobile Apps in Developing Countries," The Blog (blog), The Borgen Project, April 13, 2018, borgenproject.org/emergence-mobile-apps-in-developing-countries/, accessed September 4, 2018; Suparna Dutt D'Cunha, "WhatsApp, Already India's Favorite Chat App, Wants To Be Its Leader In Digital Payments, Too," Forbes, February 9, 2018, http://www.forbes.com/sites/suparnadutt/2018/02/09/whatsapp-already-indias-favorite-chat-app-wants-to-be-its-leader-in-digital-payment-too/#2a8f9deae4dd, accessed September 4, 2018.

38 "Home," Evernym, accessed September 6, 2018, http://www.evernym.com/.

39 The ID2020 Alliance describes itself as "an innovative public-private partnership committed to improving lives through digital identity. The Alliance brings together multinational institutions, nonprofits, philanthropy, business, and governments to set the technical standards for a safe, secure, and interoperable digital identity that is owned and controlled by the user. It funds high-impact pilot projects that bring digital identity to vulnerable populations, and uses the data generated to find scalable solutions and inform public policy. Partners include Accenture, FHI360, Gavi, the Vaccine Alliance, Hyperledger, IDEO.org, iRespond, Kiva, Mercy Corps, Microsoft, Simprints, and United Nations ICC" ("Our Manifesto," Medium (blog), ID2020, September 14, 2018, medium.com/@id2020/our-manifesto-78c6969ca960, accessed September 17, 2018).

40 See "Our Manifesto," ID2020.

41 Benito Arruñada, "Registries," Man and the Economy 1, no. 2 (2014), 209.

42 "Natural Person," Wikipedia, last updated February 6, 2018, en.wikipedia.org/wiki/Natural_person, accessed October 1, 2018.

43 Lene Mikkelsen, Alan Lopez, David Phillips, "Why birth and death registration really are "vital" statistics for development," HDialogue (blog), United Nations Development Programme, April 14, 2015, hdr.undp.org/en/content/why-birth-and-death-registration-really-are-%E2%80%9Cvital%E2%80%9D-statistics-development, accessed September 17, 2018.

44 Matthew I. Bellgard, Lee Render, Maciej Radochonski, and Adam Hunter, "Second generation registry framework," Source Code for Biology and Medicine 9, no. 14 (June 20, 2014).

45 Dewan Hoque et al., "Impact of clinical registries on quality of patient care and clinical outcomes: A systematic review," PLOS One 12, no. 9 (September 8, 2017).

46 Tim Robustelli, "High-Tech Solutions in Colombia," FPR Blog (blog), New America, September 6, 2018, http://www.newamerica.org/future-property-rights/blog/high-tech-solutions-colombia/, accessed October 2, 2018.

47 The information below was provided by Chris Worman, Vice President, Alliances and Program Development, TechSoup, in an email to Michael Graglia on October 1, 2018.

48 See Patrick Kelley and Michael Graglia, "Why Property Rights Matter," FPR Blog (blog), New America, March 10, 2017, http://www.newamerica.org/future-property-rights/blog/why-property-rights-matter/, accessed July 23 2018.

49 "III. Rationale for the Operation of Open Registers," Food and Agriculture Organization of the United Nations, accessed September 17, 2018, http://www.fao.org/docrep/005/y3824e/y3824e06.htm.

50 "Collateral," Investopedia, accessed September 17, 2018, http://www.investopedia.com/terms/c/collateral.asp.

51 See also, Inessa Love, Martínez Pería, María Soledad, and Sandeep Singh, Collateral Registries for Movable Assets: Does Their Introduction Spur Firm's Access to Bank Finance? (Policy Research Working Paper No. 6477), International Finance Corporation, World Bank Group, 2013, openknowledge.worldbank.org/handle/10986/15839, accessed September 17, 2018.

52 International Finance Corporation "Secured Transactions and Collateral Registries," World Bank Group, accessed September 17, 2018, http://www.ifc.org/wps/wcm/connect/793e79804ac10fff9ea69e4220e715ad/Secured+Transactions+and+Collateral+Registries+Brochure-English.pdf?MOD=AJPERES.

53 International Finance Corporation, "Collateral Registries: A Smart Way to Expand Access to Finance," Stories of Impact (blog), World Bank Group, October

2016, http://www.ifc.org/wps/wcm/connect/news_ext_content/ifc_external_corporate_site/news+and+events/news/impact-stories/collateral-registries-smart-way-to-expand-a2f, accessed September 17, 2018. See also, Love, Pería, Soledad, and Singh, Collateral Registries for Movable Assets.

54 Love, Pería, Soledad, Singh, Collateral Registries for Movable Assets, 4.

55 Alejandro Alvarez de la Campa, "Secured Transactions and Collateral Registries Program," Presentation at International Finance Corporation, Amman, Jordan, June 25, 2013, http://www.smefinanceforum.org/sites/default/files/post/files/459816_s1_-_secured_transactions_and_collateral_registries_program.pdf, accessed September 23, 2018.

56 Within this box, we examine the Verifiable Organizations Network (VON) and TheOrgBook. The two are related, but different. The VON is the overall initiative, while TheOrgBook is a tangible data repository used within the project (comment from John Jordan, Executive Director of Services Strategy, Government of British Columbia (July 17, 2018)).

57 "Home," Verifiable Organizations Network, accessed July 16, 2018, von.pathfinder.gov.bc.ca/.

58 "About VON," Verifiable Organization Network, accessed July 16, 2018, von.pathfinder.gov.bc.ca/aboutvon/.

59 Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. It provides tools, libraries, and reusable components for creating and using independent digital identities based on blockchain technology ("Hyperledger Indy," The Linux Foundation, accessed June 26, 2018, http://www.hyperledger.org/projects/hyperledger-indy/).

60 "About VON," Verifiable Organizations Network.

61 Interview with John Jordan, (July 13, 2018).

62 Comment from John Jordan, (July 16, 2018).

63 Al Pascual, "The Fraud Implications of the Digital Identity Revolution," Javelin, April 12, 2017, http://www.javelinstrategy.com/blog/fraud-implications-digital-revolution, accessed September 24, 2018.

64 "Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study," Javelin, February 6, 2018, http://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin, accessed September 24, 2018.

65 See Staesser, "The Emergence of Mobile Apps in Developing Countries."

66 James Manyika, Susan Lund, Marc Singer, Olivia White, and Chris Berry, Digital Finance For All: Powering Inclusive Growth In Emerging Economies (Executive Summary), McKinsey Global Institute, September 2016, http://www.mckinsey.com/featured-insights/employment-and-growth/how-digital-finance-could-boost-growth-in-emerging-economies, accessed September 26, 2018.

67 Ibid.

68 See Juan Antonio Ketterer and Gabriela Andrade, "Blockchain Asset Registries: Approaching Enlightenment?," CoinDesk, December 30, 2017, http://www.coindesk.com/blockchain-asset-registries-entering-slope-enlightenment/, accessed September 18, 2018.

69 Kaliya Young, The Domains of Identity, 2018, identitywoman.net/domains-of-identity/.

70 Ibid., 3-4.

71 Ketterer and Andrade, "Blockchain Asset Registries."

72 International Finance Corporation, "Collateral Registries."

73 Used with permission from Kaliya Young. See Young, The Domains of Identity, identitywoman.net/domains-of-identity/, 2.

74 "Guide for the Application for authorization To submit documents for registration in the Electronic Land Registration System," ServiceOntario, August 15, 2013, files.ontario.ca/electronic_land_reg_application_guide.pdf, accessed October 4, 2018.

75 This information is derived from field notes composed by Christopher Mellon, Policy Analyst, Future of Property Rights Program, during a learning trip to Manitoba and Ontario in May-June 2018.

76 "Blockchain and Smart Contracts Could Transform Property Transactions," CFO Journal (blog), Wall Street Journal, January 3, 2018, deloitte.wsj.com/cfo/2018/01/03/blockchain-and-smart-contracts-could-transform-property-transactions/, accessed July 23, 2018.

77 John Dempsey and Michael Graglia "Case Study: Property Rights and Stability in Afghanistan," FPR Blog (blog), New America, May 5, 2017, http://www.newamerica.org/future-property-rights/blog/case-study-property-rights-and-stability-afghanistan/, accessed July 24, 2018.

78 Kelley and Graglia, "Why Property Rights Matter."

79 The Pinheiro Principles: United Nations Principles on Housing and Property Restitution for Refugees and Displaced Persons, Centre on Housing Rights and Evictions, 2005, 2001-2009.state.gov/documents/organization/99774.pdf, accessed July 24, 2018.

80 JTA, "House passes bill to help Holocaust survivors obtain restitution, seized assets," The Times of Israel, April 25, 2018, http://www.timesofisrael.com/house-passes-bill-to-help-holocaust-survivors-obtain-restitution-seized-assets/, accessed July 24, 2018.

81 Comment from Kaliya Young (July 27, 2018).

82 Max Fisher, "Political science says Syria's civil war will probably last at least another decade," The Washington Post, May 23, 2013, http://www.washingtonpost.com/news/worldviews/wp/2013/10/23/political-science-says-syrias-civil-war-will-probably-last-at-least-another-decade/?noredirect=on&utm_term=.8767a26b881f, accessed July 24, 2018.

83 "Forced displacement above 68m in 2017, new global deal on refugees critical," UNHCR, June 19, 2018, http://www.unhcr.org/news/press/2018/6/5b27c2434/forced-displacement-above-68m-2017-new-global-deal-refugees-critical.html, accessed October 4, 2018. See also, Global Trends: Forced Displacement in 2017, UNHCR, 2018, http://www.unhcr.org/5b27be547, accessed October 4, 2018.

84 Dempsey and Graglia "Case Study: Property Rights and Stability in Afghanistan."

85 "Syria emergency," United Nations High Commissioner for Refugees, last updated April 19, 2018, http://www.unhcr.org/en-us/syria-emergency.html, accessed September 24, 2018.

86 "The future of Syria: How a victorious Bashar al-Assad is changing Syria," The Economist, June 28, 2018, http://www.economist.com/middle-east-and-africa/2018/06/28/how-a-victorious-bashar-al-assad-is-changing-syria, accessed September 10, 2018.

87 Deyaa Alrwishdi and Rebecca Hamilton, "Paying Attention to Land Rights in Syria Negotiations," Just Security, April 12, 2018, http://www.justsecurity.org/54781/paying-attention-land-rights-syria-negotiations/, accessed July 19, 2018.

88 Ibid.

89 "The future of Syria" The Economist.

90 "Q&A: Syria's New Property Law," Human Rights Watch, May 29, 2018, http://www.hrw.org/news/2018/05/29/qa-syrias-new-property-

law#_What_barriers_would, accessed September 10, 2018; see also Maha Yahya, Jean Kassir, and Khalil el-Harir, Unheard Voices: What Syrian Refugees Need to Return Home, Carnegie Endowment for International Peace, 2018, carnegieendowment.org/files/Yahya_UnheardVoices_INT_final.pdf, accessed October 4, 2018.

91 Young, The Domains of Identity, identitywoman.net/domains-of-identity, 15.

92 Stephane Hallegatte et al., Shockwaves: Managing the Impacts of Climate Change on Poverty, World Bank Group, 2016, openknowledge.worldbank.org/bitstream/handle/10986/22787/9781464806735.pdf?sequence=13&isAllowed=y, accessed September 21, 2018.

93 LandLinks "Land Tenure and Disasters: Response, Rebuilding, Resilience," USAID, February 13, 2015 http://www.land-links.org/event/land-tenure-disasters-response-rebuilding-resilience/, accessed July 24, 2018.

94 Sameh Wahba, Anna Wellenstein, Francis Ghesquiere, and Wael Zakout, "Securing land rights for all is key to building disaster-resilient communities," Sustainable Cities (blog), World Bank Group, October 13, 2017, blogs.worldbank.org/sustainablecities/securing-land-rights-all-key-building-disaster-resilient-communities, accessed July 24, 2018.

95 Ibid.

96 Rina Chandran, "With titles, 1 million slum dwellers in India's Odisha become homeowners," plac e, July 19, 2018, http://www.thisisplace.org/i/?id=5926137d-43cf-4404-a4d3-81f36bd182c0, accessed July 24, 2018.

97 Frances Robles ad Jugal K. Patel, "On Hurricane Maria Aniversary, Puerto Rico is Still in Ruins," The New York Times, September 20, 2018, http://www.nytimes.com/interactive/2018/09/20/us/puerto-rico-hurricane-maria-housing.html, accessed September 21, 2018.

98 See R. Sujatha, "Lamination of documents has risks too," The Hindu, last updated May 13, 2016, http://www.thehindu.com/news/national/tamil-nadu/lamination-of-documents-has-risks-too/article5587404.ece, accessed July 24, 2018; and Bharat A. Patel, "Don't laminate important documents" Bangalore Mirror, last updated September 9, 2015, bangaloremirror.indiatimes.com/bangalore/others/documents-laminate-de-laminators-banks-original-duplicate/articleshow/48875268.cms, accessed July 24, 2018.

99 We are not advocating for the complete disuse of paper-based records. For example, these documents can "point" to the online storage location of digital records.

100 See Michael Graglia, Tim Robustelli, and Matthew Marcus, The Punjab Example: Systemic Land Reform in Rural Pakistan, New America, July 11, 2018.

101 Kaliya Young cautions that the resiliency and utility of a self-sovereign identity solution is also contingent upon proper key recovery within a decentralized key management system (comment from Kaliya Young (July 27, 2018)).

102 "The Vital Role of Women in Agricultural and Rural Development," paper presented at the Thirty-seventh Session of the FAO Conference, Rome, June 25-July 2, 2011.

103 Durre Samee et al., Women in Agriculture in Pakistan, Food and Agriculture Organization of the United Nations, 2015, http://www.fao.org/3/a-i4330e.pdf, 103.

104 "The Vital Role of Women in Agricultural and Rural Development."

105 Ibid.

106 Meighan Stone and Guest Blogger for Rachel Vogelstein, "A Place of Her Own: Women's Right to Land," Women Around the World (blog), Council on Foreign Relations, May 21, 2018, http://www.cfr.org/blog/place-her-own-womens-right-land, accessed July 25, 2018.

107 See Shiza Malik, "The stooped labour of women rice farmers," Dawn, last updated August 10, 2017, http://www.dawn.com/news/1347349, accessed July 25, 2018.

108 Janet Walsh, "Widows, Land and Power," Human Rights Watch, March 19, 2018, http://www.hrw.org/news/2018/03/19/widows-land-and-power, accessed July 25, 2018.

109 Khushbu Mishra and Abdoul G. Sam, "Does Women's Land Ownership Promote Their Empowerment? Empirical Evidence from Nepal," Worl d Development 78 (2016), 360-371.

110 Stone and Guest Blogger for Rachel Vogelstein, "A Place of Her Own."

111 Graglia, Robustelli, and Marcus, The Punjab Example, 16, 34.

112 Comment from Elizabeth Renieris, Global Policy Counsel, Evernym (July 27, 2018).

113 A node is a copy of a blockchain that exists on a computer or other type of hardware device. Any node, including observer nodes, ensures the validity and continuity of a blockchain. In doing so, a node can also verify asset ownership and identify bad actors within the system. But observer nodes cannot add transactions or blocks to the blockchain. Only transaction, or validator, nodes can add new transactions or new blocks to the blockchain ("Nodes," World Crypto Index, accessed June 28, 2018, http://www.worldcryptoindex.com/how-nodes-work; "Introduction," BitTicket, accessed August 30, 2018).

114 Walsh, "Widows, Land and Power."

115 LandLinks, "Fact Sheet: Tenure and Women's Empowerment," USAID, December 1, 2016, http://www.land-links.org/issue-brief/fact-sheet-land-tenure-womens-empowerment/, accessed July 26, 2018.

116 Stone and Guest Blogger for Rachel Vogelstein, "A Place of Her Own."

117 Allen, "The Path to Self-Sovereign Identity."

118 Naman M. Aggarwal, Wafa Ben-Hassine, and Raman Jit Singh Chima, National Digital Identity Programmes: What's Next?, Access Now, March 2018, http://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf, accessed April 25, 2018.

119 The Known Traveller, World Economic Forum and Accenture.

120 Principles on identification for sustainable development: toward the digital age, World Bank Group, February 27, 2017, documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf, accessed April 25, 2018.

121 Concept Note, Secretariat for the ID2020 Alliance, 2017, static1.squarespace.com/static/578015396a4963f7d4413498/t/5a5f92bcc8302548e722dff3/1519157409748/ID2020+Alliance+Doc+-+Jan+2018.pdf, accessed May 4, 2018.

122 We do not claim that our list is comprehensive. Other valuable contributions within the identity space include: Carly Nyst, Steve Pannifer, Edgar Whitley, and Paul Makin, Digital Identity: Issue Analysis, Consult Hyperion, June 8, 2016, http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf, accessed August 6, 2018; Kaliya Young, "Vision & Principles for the Personal Data Ecosystem," Identity Woman (blog), September 13, 2010, identitywoman.net/vision-principles-for-the-personal-data-ecosystem/, accessed August 6, 2018; and Phillip Windley, "PDX

Principles," Phil Windley's Technometria (blog), September 10, 2010, http://www.windley.com/archives/2010/09/pdx_principles.shtml, accessed August 6, 2018.

123 Kim Cameron, "The Laws of Identity," Identity Blog (blog), May 11, 2005, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf, accessed April 25, 2018.

124 Allen, "The Path to Self-Sovereign Identity."

125 Cameron, "The Laws of Identity."

126 Allen, "The Path to Self-Sovereign Identity."

127 Principles on identification for sustainable development, World Bank Group.

128 Concept Note, ID2020 Alliance.

129 The Known Traveller, World Economic Forum and Accenture.

130 Aggarwal, Ben-Hassine, and Chima, National Digital Identity Programmes.

131 The ID2020 Alliance explicitly states that digital identity must be: 1. Personal; 2. Persistent; 3. Portable; and 4. Private. Other "principles of identity" can be discerned within their Concept Note. For reasons related to relative conformity, the list is paraphrased into ten overarching principles.

132 Access Now lists 17 "recommendations and digital rights safeguards" under three pillars: 1. Governance; 2. Data Protection and Privacy; and 3. Cybersecurity. For reasons related to brevity and relative conformity, the list is paraphrased into eight overarching principles.

133 The "right to be forgotten" is the concept that individuals have the civil right to request that third parties remove their personal information from the internet. In particular, the removal of old, inaccurate, or irrelevant data is viewed as a legitimate request. While the "right to be forgotten" aims to support personal privacy, we feel that it is necessary to mention the concern that it conflicts with the open nature of the web and the free flow of information (Margaret Rouse and Laura Aberle, "Definition: right to be forgotten," WhatIs.com, TechTarget, last updated June 2014, searchcontentmanagement.techtarget.com/definition/The-right-to-be-forgotten, accessed August 22, 2018; Dave Lee, "What is the 'right to be forgotten'?," BBC, May 13, 2014, http://www.bbc.com/news/technology-27394751, accessed August 22, 2018).

134 "Privacy-by-design" is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices (Sylvia Kingsmill and Ann Cavoukian, Privacy by Design: Setting a new standard for privacy certification, Deloitte, accessed July 18, 2018, www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF).

135 For principles concerning the use of biometrics within a self-sovereign identity solution, see John Callahan et al., "Six Principles for Self-Sovereign Biometrics," Rebooting the Web of Trust, last updated April 25, 2018, github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/draft-documents/Biometrics.md, accessed October 3, 2018.

136 "Home," Everest, accessed September 25, 2018, everest.org/; "Team," Everest, accessed September 25, 2018, everest.org/#team.

137 "Our Team," Evernym, accessed June 18, 2018, http://www.evernym.com/our-team/; "Evernym," Crunchbase, accessed June 18, 2018, http://www.crunchbase.com/organization/evernym.

138 Comment from Rouven Heck, co-founder and Product Lead, uPort (June 26, 2018).

139 Bob Reid and Brad Witteman, EverID Whitepaper, Everest, May 4, 2018, 6.

140 "Products," Evernym, accessed June 18, 2018, http://www.evernym.com/products/.

141 "Products," uPort, accessed June 19, 2018, http://www.uport.me/#products.

142 "Home," uPort, accessed September 25, 2018, http://www.uport.me/.

143 Bob Reid and Brad Witteman, Everest Whitepaper , Everest, July 2018, everest.org/wp-content/uploads/2018/08/wp_15.08.pdf, 7, 28.

144 Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, Sovrin Foundation, January 2018, sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf, 2, 15.

145 A decentralized application, or dApp, is a digital application that runs on a blockchain or a peer-to-peer network of computers rather than a single computer. dApps are designed to exist on the internet in a way that is not controlled by a single entity ("Decentralized Applications or dApps," Investopedia, accessed September 24, 2018, http://www.investopedia.com/terms/d/decentralized-applications-dapps.asp; "Decentralized Applications - dApps," BlochchainHub, accessed September 24, 2018, blockchainhub.net/decentralized-applications-dapps/).

146 Reid and Witteman, Everest Whitepaper, 16.

147 "Products," Evernym.

148 "About," uPort, accessed September 25, 2018, http://www.uport.me/#about.

149 Reid and Witteman, Everest Whitepaper, 23.

150 "Gas" refers to the unit of measurement used to represent the cost of conducting a transaction or executing a smart contract in the Ethereum network ("Gas (Ethereum)," Investopedia, accessed June 21, 2018, http://www.investopedia.com/terms/g/gas-ethereum.asp; Everett Muzzy, "A Guide to Gas," Medium (blog), ConsenSys, May 23, 2018, media.consensys.net/a-guide-to-gas-12b40d03605d, accessed September 14, 2018).

151 Ethereum is a decentralized software platform that enables smart contracts and decentralized applications to be built and implemented within an open-source, blockchain-based ecosystem. The platform is also the basis for its own cryptocurrency, Ether ("Ethereum," Investopedia.com, accessed July 19, 2018, http://www.investopedia.com/terms/e/ethereum.asp).

152 An initial coin offering, or ICO, refers to the sale of digital tokens to the public. People could be interested in a token because it has an inherent benefit --such as access to a service-- or because there is speculation that it will increase in value. As a type of "digital crowdfunding," ICOs enable startups to raise funds without giving up equity, and also encourage the adoption of a project by incentivizing its use by token holers (Noelle Acheson, "What is an ICO?," CoinDesk, last updated March 16, 2018, http://www.coindesk.com/information/what-is-an-ico/, accessed September 20, 2018).

153 "Token," Everest, accessed June 22, 2018, everid.net/token/.

154 "Sovrin," ICODrops.com, accessed June 22, 2018, icodrops.com/sovrin/.

155 Victoria van Eyk, "Ethereum Launches Own 'Ether' Coin, With Millions Already Sold," CoinDesk, July 23, 2014, http://www.coindesk.com/ethereum-launches-ether-coin-millions-already-sold/, accessed September 26, 2018.

156 Comment from Elizabeth Renieris (July 27, 2018).

157 A prediction market is a collection of people speculating on a variety of events --exchange averages, election results, commodity prices, quarterly sale results, or even gross movie receipts-- and trading outcomes. Prediction markets usually represent a wide variety of thoughts and opinions, and have proven to be quite effective as prognostic tools

("Prediction Market," Investopedia, accessed August 22, 2018, http://www.investopedia.com/terms/p/prediction-market.asp).

158 "Home," Everest; "Team," Everest.

159 "About Us," Everest, accessed June 18, 2018, everid.net/about/.

160 Reid and Witteman, EverID Whitepaper, 5.

161 "01 --The Identity Network Foundation," Everest, accessed August 27, 2018, everest.org/#step-1.

162 "About Us," Everest; Reid and Witteman, EverID Whitepaper, 5.

163 "Road map," Everest, accessed August 24, 2018. everest.org/.

164 Reid and Witteman, EverID Whitepaper, 11.

165 "Road map," Everest.

166 Reid and Witteman, Everest Whitepaper, 3.

167 To provide more detail, "the EverID Datagram is the proprietary storage file of the user's identity information. The EverID Datagram is resident on the user's mobile device and in the Everest Supernode. Any updates to the Datagram are mirrored / synchronized with the other copies of that individual's Datagram on their devices or in the Everest Supernode as soon as the devices come online." Also, only "an Everest DApp, Agent DApp, or Everest-enabled device can create an EverID Datagram." Finally, "the EverID Datagram, and its storage are in the control of the user at all times, allowing them to decide who has access to what information and how that information is stored in the long-term" (Reid and Witteman, Everest Whitepaper, 14-15).

168 InterPlanetary File System (IPFS) is a new hypermedia distribution protocol, addressed by content and identities, as opposed to traditional location addressing. IPFS is designed to decentralize the web while simultaneously increasing the speed and security of the internet. IPFS connects all computing devices with the same system of files via a network of nodes, and does not have a single point of failure (Peter Vowell, "What is the InterPlanetary File System?," MaxCDN One, last updated June 15, 2016, http://www.maxcdn.com/one/visual-glossary/interplanetary-file-system/, accessed June 26, 2018).

169 "Find Out More," Everest, accessed September 26, 2018, everest.org/#find-out-more.

170 A digital wallet is a decentralized application that can store, send, and receive cryptocurrency. A digital wallet also includes a user's public/private key pair (EW, "An introduction to cryptocurrency wallet," Etherworld, July 27, 2017, etherworld.co/2017/07/27/an-introduction-to-cryptocurrency-wallet/, accessed March 28, 2018; Reid and Witteman, Everest Whitepaper, 41).

171 Reid and Witteman, Everest Whitepaper, 4-5.

172 Reid and Witteman, EverID Whitepaper, 32.

173 "In the future, the CRDT may be pegged to a basket of stable fiat currencies or commodities, or simply evolve into a stable token itself" (Reid and Witteman, Everest Whitepaper, 25).

174 Utility tokens provide users with access to a software platform (Josiah Wilmoth, "The Difference Between Utility Tokens and Equity Tokens," Strategic Coin, accessed September 10, 2018, strategiccoin.com/difference-utility-tokens-equity-tokens/). Pegged tokens are linked to the specific value of a bank-issued currency or another commodity (Nathan Reiff, "Gold-Pegged Vs. USD-Pegged Cryptocurrencies," Investopedia, June 7, 2018, http://www.investopedia.com/tech/goldpegged-vs-usdpegged-cryptocurrencies, accessed September 19, 2018).

175 The "ID is a utility token enabling access to the network and a myriad of applications and services that are the conduit for every exchange of value in the

economy. Varying levels of access to network resources are granted to the holders of the ID tokens" (Reid and Witteman, Everest Whitepaper, 23).

176 Reid and Witteman, Everest Whitepaper, 23-26.

177 "The EverID Token Sale," Everest, accessed July 19, 2018, everid.net/#token-sale.

178 Reid and Witteman, Everest Whitepaper, 25.

179 Ibid, 24-26.

180 A testnet, or test network, is a network where new decentralized applications (dApps) and smart contracts can be tested and developed. In contrast, the mainnet, or main network, is a network wherein actual transactions occur on the distributed ledger ("Definition of "Mainnet,"" ETHNews, accessed August 30, 2018, http://www.ethnews.com/glossary/mainnet).

181 "Road map," Everest.

182 "Everest, WAH Foundation and the Cambodian Health Ministry Improve Healthcare for Mothers," Everest, August 22, 2018, everest.org/everest-wah-foundation-and-the-cambodian-health-ministry-improve-healthcare-for-mothers-in-cambodia-via-blockchain-technology/, accessed August 30, 2018; "Everest, ID2020 and the Government of Indonesia (TNP2K Secretariat) Announce Innovative Identity and Blockchain Pilot Solution to Enhance the National LPG Subsidy Program," GlobeNewswire, September 14, 2018, http://www.globenewswire.com/news-release/2018/09/14/1571269/0/en/Everest-ID2020-and-the-Government-of-Indonesia-TNP2K-Secretariat-Announce-Innovative-Identity-and-Blockchain-Pilot-Solution-to-Enhance-the-National-LPG-Subsidy-Program.html, accessed September 17, 2018.

183 "Solutions and Use Cases," Everest, accessed June 28, 2018, everid.net/solutions/.

184 All information within this text box is derived from an interview with Brad Witteman, co-founder and Chief Product Officer of Everest, on July 13, 2018 unless cited otherwise.

185 "Everest, WAH Foundation and the Cambodian Health Ministry Improve Healthcare for Mothers," Everest.

186 Comment from Bob Reid, co-founder and CEO, Everest (August 3, 2018).

187 Ibid.

188 "Everest, ID2020 and the Government of Indonesia (TNP2K Secretariat) Announce Innovative Identity and Blockchain Pilot Solution to Enhance the National LPG Subsidy Program," GlobeNewswire.

189 "Our Team," Evernym; "Evernym," Crunchbase.

190 "Products," Evernym.

191 Sovrin: A Protocol and Token, Sovrin Foundation, 15.

192 Ibid.

193 Comment from Kaliya Young (July 27, 2018).

194 Sovrin: A Protocol and Token, Sovrin Foundation, 15.

195 Interview with Peter Simpson, Executive Director, iRespond (September 27, 2018).

196 The Linux Foundation is a non-profit organization created to build sustainable ecosystems around open source projects in order to accelerate technology development and industry adoption. The Linux Foundation provides support for open source communities through financial and intellectual resources, infrastructure, services, events, and training ("About," The Linux Foundation, accessed July 19, 2018, http://www.linuxfoundation.org/about/).

197 Sovrin: A Protocol and Token, Sovrin Foundation, 15. Also, version one --or the Sovrin Provisional Trust Framework-- was published by the Sovrin Foundation

Board of Trustees on June 28, 2017, and can be accessed here.

198 Drummond Reed, "Relationship between Sovrin and Evernym [Message 3]," Sovrin Foundation Forum, October 2, 2017, forum.sovrin.org/t/relationship-between-sovrin-and-evernym/390/3, accessed June 29, 2018.

199 Comment from Elizabeth Renieris (September 20, 2018).

200 Comment from James Monaghan, Vice President, Product, Evernym (May 29, 2018); "Products," Evernym.

201 Ibid.

202 Sovrin: A Protocol and Token, Sovrin Foundation, 25.

203 Ibid, 2.

204 "Sovrin," ICODrops.com.

205 Comment from James Monaghan (May 29, 2018).

206 "Welcome to MyCUID," MyCUID, accessed July 19, 2018, http://www.mycuid.com/; "Illinois Partners with Evernym to Launch Birth Registration Pilot," Medium (blog), IL Blockchain Initiative, August 31, 2017, illinoisblockchain.tech/illinois-partners-with-evernym-to-launch-birth-registration-pilot-f2668664f67c, accessed July 19, 2018; "Evernym and R3 partner to apply self-sovereign identity to financial services," GlobeNewswire, January 29, 2018, http://www.globenewswire.com/news-release/2018/01/29/1313374/0/en/Evernym-and-R3-partner-to-apply-self-sovereign-identity-to-financial-services.html, accessed July 19, 2018; comment from Elizabeth Renieris (July 27, 2018).

207 All information within this text box is derived from an interview with Peter Simpson, Executive Director of iRespond, on July 5, 2018 unless cited otherwise.

208 "Using biometrics and blockchain technology, iRespond provides personal identification to vulnerable populations," Crowd360, FHI 360, May 4, 2018, crowd360.org/biometrics-blockchain-identification-vulnerable-populations/, accessed July 5, 2018.

209 iRespond asserts that an iris signature does not change significantly over the course of a lifetime.

210 "Our Solution," iRespond, accessed September 20, 2018, http://www.irespond.org/our-solution/.

211 "Using biometrics and blockchain technology, iRespond provides personal identification to vulnerable populations," Crowd360.

212 "Projects," iRespond, accessed July 6, 2018, http://www.irespond.org/projects/.

213 Comment from Rouven Heck (June 26, 2018).

214 "About," uPort; comment from Alice Nawfal, Strategy and Operations, uPort (August 29, 2018).

215 Bernard Marr, "Blockchain: A Very Short History of Ethereum Everyone Should Read," Forbes, February 2, 2018, http://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/#119e63ac1e89, accessed September 26, 2018.

216 StopandDecrypt, "The Ethereum-blockchain size has exceeded 1TB, and yes, it's an issue," Medium (blog), Hackernoon, May 23, 2018, hackernoon.com/the-ethereum-blockchain-size-has-exceeded-1tb-and-yes-its-an-issue-2b650b5f4f62, accessed August 29, 2018.

217 "Blockchain by the Numbers: 33 Stats on Ethereum and ConsenSys," Medium (blog), ConsenSys, July 20, 2018, media.consensys.net/blockchain-by-the-numbers-33-stats-on-ethereum-and-consensys-738cb1637cb3, accessed August 29, 2018.

218 "Overview," uPort Developer Portal, uPort, accessed June 29, 2018, developer.uport.me/overview.

219 Interview with Paul Kohlhaas, Director of Business Development, ConsenSys (May 23, 2018); "Overview," uPort Developer Portal, uPort.

220 "Overview," uPort Developer Portal, uPort.

221 Pelle Braendgaard, "Next Generation uPort Identity App released," Medium (blog), uPort, September 26, 2018, medium.com/uport/next-generation-uport-identity-app-released-59bbc32a83a0, accessed October 4, 2018.

222 "About," uPort.

223 "Overview," uPort Developer Portal, uPort.

224 ERC20 is a widely-used token standard for the Ethereum ecosystem. In short, ERC20 defines a common list of rules for all Ethereum tokens --meaning that developers and users can accurately predict how newly created tokens will function in the ecosystem (Nathan Reiff, "What is ERC-20 and What Does it Mean for Ethereum?," Investopedia, June 20, 2017, http://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/, accessed June 26, 2018).

225 Interview with Robby Greenfield, Global Social Impact Technical Lead, ConsenSys (May 18, 2018).

226 Comment from Rouven Heck (July 13, 2018).

227 "Partners," uPort, accessed July 2, 2018, http://www.uport.me/#partners; comment from Alice Nawfal (August 29, 2018).

228 Interview with Paul Kohlhaas (May 23, 2018); comment from Alice Nawfal (August 29, 2018).

229 Paul Kohlhaas, "Zug ID: Exploring the First Publicly Verified Blockchain Identity," Medium (blog), uPort, December 17, 2017, medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702, accessed July 2, 2018.

230 During our research, we also interviewed Titus Capilnean, the Director of Marketing at Civic. Founded in 2016, the San Francisco-based firm states online that it is "spearheading the development of an ecosystem that is designed to facilitate on-demand, secure, low-cost access to identity-verification services via the blockchain." It became clear during our conversation with Titus that the Civic platform was optimized for purposes related to KYC/AML and data storage rather than self-sovereign identity. Because of our focus on SSI, we decided to omit Civic from the analysis. We are grateful to Titus for his time and insights ("About Civic," Civic, accessed June 18, 2018, http://www.civic.com/company/; interview with Titus Capilnean, Director of Marketing, Civic (April 18, 2018)).We spoke with Arjun Raman, the Managing Director at Mooti, as well. The firm was launched in 2016, and is headquartered in New York. Its website states that "Mooti is the new standard for cryptographic identification and validation." Mooti is not attempting to construct a global ecosystem for SSI, but helps client organizations adopt digital identity solutions via blockchain technology and advanced cryptography. Mooti is not open source, and views diffusion of decentralized identity through a long-term business-to-business perspective. The company is omitted from our analysis due to its business model. We are grateful to Arjun and the rest of the Mooti team for their time and insights ("Mooti," Crunchbase, accessed July 3, http://www.crunchbase.com/organization/mooti#section-recent-news-activity; "What's mooti digital identity?," Mooti, accessed July 3, 2018, mooti.co/; Interview with Arjun Raman (June 20, 2018)).Unfortunately due to lack of staff availability, we were unable to include the self-sovereign identity firm Veres.One within our report. According to the company website, the Veres.One platform is "a globally interoperable blockchain for identity." Despite its omission here, we believe that Veres.One could be an important actor within the digital identity space ("Home," Veres.One, accessed August 24, 2018, veres.one/).

231 Sovrin: A Protocol and Token, Sovrin Foundation, 15.

232 Chris Hoffman, "Android Is "Open" and iOS Is "Closed" - But What Does That Mean To You?," How-To Geek, May 24, 2015, http://www.howtogeek.com/217593/android-is-open-and-ios-is-closed-but-what-does-that-mean-to-you/, accessed September 25, 2018.

233 Laura Shin, "How Joseph Lubin Cofounded Ethereum And Scored A Billion-Dollar Fortune," Forbes , February 7, 2018, http://www.forbes.com/sites/laurashin/2018/02/07/joseph-lubin-ethereum-ether-consensys-crypto-cryptocurrency/#6539a0df3575, accessed September 4, 2018.

234 "ConsenSys," ConsenSys, accessed September 4, 2018, new.consensys.net/.

235 Sindhu Hariharan, "How Dubai's Blockchain Advisor ConsenSys Is Creating A Community For The Emerging Tech," Entrepreneur Middle East, December 6, 2017, http://www.entrepreneur.com/article/305701, accessed September 14, 2018. See also, J. Michael Graglia and Christopher Mellon, "Blockchain and Property in 2018: At the End of the Beginning," paper presented at the 2018 World Bank Conference on Land and Poverty, Washington, DC, March 19-23, 2018.

236 Data leakage refers to the "unauthorized transfer of classified information from a computer or data center to the outside world" ("data leakage," PC Magazine, accessed September 21, 2018, http://www.pcmag.com/encyclopedia/term/61834/data-leakage).

237 Interview with Kaliya Young (July 3, 2018). See also, Tech2 News Staff, "Aadhaar Faces Yet Another Data Leak Allowing Access to Personal Data to "All" Enrolled in the system: Report," Firstpost.

238 The information below is derived from interviews and written answers provided by company leadership and employees of the three firms unless cited otherwise. We are grateful for their time and insights.

239 The "Bottom of the Pyramid" is a socio-economic concept grouping together the world's poorest citizens --billions of people. A member of the "Bottom of the Pyramid" lives on less than $2.50 a day and is excluded from the modernity of globalized societies, including consumption patterns and access to organized financial services ("Definition of bottom of the pyramid (BOP)," ft.com/lexicon, Financial Times, accessed September 26, 2018, lexicon.ft.com/Term?term=bottom-of-the-pyramid-(bop)).

240 Reid and Wittmean, Everest Whitepaper, 3.

241 Sovrin: A Protocol and Token, Sovrin Foundation, 18 (underline and bold in original).

242 Of note, jurisdiction-specific legislation and organizational bylaws will most likely need to be updated to account for "agent" responsibilities and "guardianship."

243 See Poushter, Bishop, and Chwe, "Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones."

244 Savita Bailur, Bryan Pon, and Emrys Schoemaker, Identities: New Practices in a Connected Age, Caribou Digital, 2017, http://www.identitiesproject.com/report/, accessed July 8, 2018.

245 "Edge Device," Techopedia, accessed August 23, 2018, http://www.techopedia.com/definition/6978/edge-device; Margaret Rouse and Jessica Scarpati, "Definition: edge device," WhatIs.com, TechTarget, last updated December 2017, searchnetworking.techtarget.com/definition/edge-device, accessed August 23, 2018.

246 Poushter, Bishop, and Chwe, "Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones."

247 Ibid.

248 Simon Sharwood, "Developing world has 98.7 per cent mobile phone adoption," The Register, August 3,

2017, http://www.theregister.co.uk/2017/08/03/itu_facts_and_figures_2017/, accessed July 9, 2018.

249 Roxanne Bauer, "Media (R)evolutions: Convergence around mobile phones in sub-Saharan Africa," People, Spaces, Deliberation (blog), World Bank Group, March 23, 2016, blogs.worldbank.org/category/tags/mobile-phone-penetration, accessed August 23, 2018.

250 Ibid.

251 Brad Witteman and Mike Kail, of Everest, noted that implementation of their solution was possible on feature phones --or "dumbphones"-- through the use of multimedia messaging service (MMS) and standard built-in cameras. However, they cautioned that the global use of feature phones may diminish over the next few years, as relatively cheaper smartphones -- such as Android devices costing less than USD $75 and possibly less than USD $25-- may soon be available on the market (interview with Brad Witteman and Mike Kail, Chief Technology Officer, Everest (September 27, 2018)).

252 Everest infrastructure will operate on a series of "supernodes" within the larger network. These supernodes will host the various software services and servers required to create and operate the Identity Network (Reid and Witteman, EverID Whitepaper, 20).

253 At the time of writing, the Evernym social key recovery feature has been designed, but is not deployed. Evernym will provide another option -- offline key recovery (comment from Elizabeth Renieris (July 27, 2018)). Offline key recovery might involve the use of a "paper wallet," or a physical document containing all of the data necessary to generate a private key online. It could also involve a "hardware wallet," which generally looks like a USB stick and holds private keys electronically. A "hardware wallet" usually connects to a computer via a USB port, enabling the upload of a private key online (EW, "An introduction to cryptocurrency wallet.").

254 "How to Import and Export Bitcoin Private Keys," Bitcoin.com, August 8, 2017, http://www.bitcoin.com/guides/how-to-import-and-export-bitcoin-private-keys, accessed June 28, 2018.

255 Interview with Robby Greenfield (May 18, 2018).

256 A seed phrase is essentially a multi-word password. For example, uPort utilizes a 12-word seed phrase. This list of words stores all the information needed to recover a wallet. Digital wallet software will typically generate a seed phrase and instruct the user to write it down on paper. If the user's computer breaks or if their hard drive becomes corrupted, they can re-download the same wallet software, and use the paper backup to recover the wallet ("Seed phrase," Bitcoin Wiki, last updated August 2, 2018, en.bitcoin.it/wiki/Seed_phrase, accessed September 21, 2018).

257 Bailur, Pon, and Schoemaker, Identities.

258 Gregory Scruggs, "'Everything we've heard about global urbanization turns out to be wrong' - researchers," place, July 10, 2018, http://www.thisisplace.org/i/?id=0150beca-e3f5-47e0-bc74-9ccc5ef1db8a, accessed July 10, 2018.

259 A decentralized identifier (DID) is a globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or any other form of a decentralized network ("Decentralized Identifiers (DID) v0.10," W3C Community Group, May 31, 2018, w3c-ccg.github.io/did-spec/, accessed June 21, 2018). Every public key can now have its own address, or DID, through blockchain technology (Sovrin: A Protocol and Token, Sovrin Foundation, 10).

260 Interview with Brad Witteman (August 30, 2018).

261 "A trust framework is a legally enforceable set of specifications, rules, and agreements that governs an identity system" (Esther Makaay, Tom Smedinghoff, and Dan Thibeau, Trust Framework for Identity Solutions, Open Identity Exchange, June 2017, http://

www.openidentityexchange.org/wp-content/uploads/2017/06/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf).

262 "Road map," Everest.

263 Reid and Witteman, Everest Whitepaper, 9.

264 Ibid., 20.

265 A software development kit (SDK) is a set of tools used for developing applications. SDKs usually include APIs, sample code, and documentation ("Software Development Kit," Techopedia, accessed July 19, 2018, http://www.techopedia.com/definition/3878/software-development-kit-sdk). An application programming interface (API) is code that allows two software programs to communicate with each other (Margaret Rouse, Tom Nolle, and Thomas Li, "Definition: application program interface," WhatIs.com, TechTarget, last updated April 2017, searchmicroservices.techtarget.com/definition/application-program-interface-API, accessed June 21, 2018).

266 Reid and Witteman, Everest Whitepaper, 41.

267 See Sovrin Provisional Trust Framework, Sovrin Foundation Board of Trustees, June 28, 2017, sovrin.org/wp-content/uploads/2018/03/Sovrin-Provisional-Trust-Framework-2017-06-28.pdf.

268 Sovrin: A Protocol and Token, Sovrin Foundation, 16.

269 A validator node will validate and write new transactions to the Sovrin ledger (Sovrin Provisional Trust Framework, Sovrin Foundation Board of Trustees, 19).

270 Sovrin Provisional Trust Framework, Sovrin Foundation Board of Trustees, 18-19.

271 Mitchell Baker and Ankit Gadgil, "Aadhaar isn't progress --it's dystopian," Business Standard, last updated May 25, 2017, http://www.business-standard.com/article/opinion/aadhaar-isn-t-progress-it-s-dystopian-117052401709_1.html, accessed July 10, 2018.

272 See Thomas, "Tagged, tracked and in danger."

273 See Sovrin Provisional Trust Framework, Sovrin Foundation Board of Trustees, 2.

274 A hash function is a type of cryptographic security measure that produces a hash value --a unique number at fixed length-- to evaluate the integrity of data, authenticate control, and provide other security measures. If data is altered, the hash value changes. A data object's integrity may be evaluated by comparing past and present hashes ("Cryptographic Hash Function," Techopedia, accessed June 26, 2018, http://www.techopedia.com/definition/27410/cryptographic-hash-function).

275 Reid and Witteman, Everest Whitepaper, 3, 18.

276 Interview with Brad Witteman (September 27, 2018).

277 "Everest One Pager," Everest, accessed September 27, 2018, everest.org/wp-content/uploads/2018/09/Everest-One-pager-September-2018-v2-1.pdf.

278 Reid and Witteman, Everest Whitepaper, 23-27.

279 See "Stewards," Sovrin, accessed June 25, 2018, sovrin.org/stewards/. Of note, Elizabeth Renieris mentioned that the number of Sovrin stewards is continuously growing. At the time of her review on July 27, 2018, the number was 41.

280 See Maria Korolov, "Open source software security challenges persist," CSO, April 2, 2018, http://www.csoonline.com/article/3157377/application-development/open-source-software-security-challenges-persist.html, accessed September 21, 2018.

281 "Stewards," Sovrin Foundation, accessed August 24, 2018, sovrin.org/stewards/.

282 Luke Graham, "Cybercrime costs the global economy $450 billion: CEO," CNBC, February 7, 2017, http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html, accessed September 27, 2018.

283 Sovrin: A Protocol and Token, Sovrin Foundation, 25.

284 Ibid.

285 Comment from Elizabeth Renieris (September 20, 2018).

286 Everest leadership also asserts that the INF is designed to "safeguard the independence, transparency, security and longevity of the network so that it exists for humanity forever" (Reid and Witteman, EverID Whitepaper, 44).

287 Noam Levenson, "Beyond Bitcoin: Why Ethereum Could Change the World," Medium (blog), November 30, 2017, medium.com/blockchain-for-grandma/beyond-bitcoin-why-ethereum-could-change-the-world-1b24a8ba1aef, accessed July 11, 2018.

288 "Ethereum (ETH)," CoinMarketCap, accessed September 24, 2018, coinmarketcap.com/currencies/ethereum/; "Explore Decentralized Applications," State of the DApps, accessed September 24, 2018, / http://www.stateofthedapps.com/; Joseph Young, "Ethereum Co-Founder: We Have the Most Active Developer Community, Optimistic Price Indicator," CoinJournal, December 18, 2017, coinjournal.net/ethereum-co-founder-active-developer-community-optimistic-price-indicator/, accessed September 24, 2018.

289 Interview with Paul Kohlhaas (May 23, 2018).

290 Comment from Mike Kail (September 18, 2018).

291 Of note, the distributed character of DLT does mitigate against a single point of failure. As long as at least two nodes are active, a blockchain ecosystem will persist.

292 The Decentralized Identity Foundation (DIF) is a consortium dedicated to "building an open source decentralized identity ecosystem for people, organizations, apps, and devices." The pillars of this proposed ecosystem are "decentralized identities anchored by blockchain IDs linked to zero-trust databases that are universally discoverable" ("Home," Decentralized Identity Foundation, accessed June 26, 2018, identity.foundation/).

293 The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the web ("Home," World Wide Web Consortium (W3C), accessed June 26, 2018, http://www.w3.org/).

294 Sovrin Provisional Trust Framework, Sovrin Foundation Board of Trustees, 4.

295 Comment from Rouven Heck (July 13, 2018).

296 As stated above, exportation of a private key usually involves the creation of a file containing private key data and its transfer to a new or different wallet. An individual can generally import a private key into a digital wallet via a text file or QR code scanning.

297 Interview with Kaliya Young (August 24, 2018).

298 Everest claims that its Conduit System will allow users to integrate disparate sources of information from existing systems into their personal EverID. Inbound information might come from national identity registers, healthcare systems, online services, or refugee databases (Reid and Witteman, Everest Whitepaper, 22).

299 Braendgaard, "Next Generation uPort Identity App released."

300 Elizabeth Renieris notes that the Sovrin Foundation, Evernym, and uPort are active members in the DIF. (comment from Elizabeth Renieris (July 27, 2018)).

301 See "Home," TheLedger, accessed October 1, 2018, theledger.be/.

302 Michiel Mulders, "Decentralized Identifiers - the internet's "missing identity layer," Coin Intelligence, January 28, 2018, http://www.cointelligence.com/content/decentralized-identifiers-dids-internets-missing-identity-layer/, accessed October 1, 2018.

303 Ibid.

304 Mulders, "Decentralized Identifiers."

305 Sovrin: A Protocol and Token, Sovrin Foundation, 10.

306 Interview with Brad Witteman and Mike Kail (September 27, 2018).

307 "Universal Identifier," Decentralized Identity Foundation, accessed September 24, 2018, uniresolver.io/.

308 Sabadello, "A Universal Resolver for self-sovereign identifiers."

309 "Everest One Pager," Everest.

310 Sovrin: A Protocol and Token, Sovrin Foundation, 18.

311 Reuben Jackson, "Scalability is Blockchain's Biggest Problem But it Can Be Solved," CryptoSlate, August 10, 2018, cryptoslate.com/scalability-is-blockchains-biggest-problem-but-it-can-be-resolved/, accessed October 1, 2018.

312 "Blockchain Scalability: The Issues, and Proposed Solutions," Medium (blog), BitRewards, April 25, 2018, medium.com/@bitrewards/blockchain-scalability-the-issues-and-proposed-solutions-2ec2c7ac98f0, accessed October 1, 2018.

313 Reid and Witteman, Everest Whitepaper, 4.

314 Proof-of-Authority is a consensus algorithm in which transactions and blocks are validated by pre-approved nodes. The mechanism delivers "instant transactions and seamless consensus over a truly distributed network" (Zana Witherspoon, "A Hitchhiker's Guide to Consensus Algorithms," Medium (blog), Hackernoon, February 13, 2018, hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3, accessed July 17, 2018; Alicia Naumoff, "Why Blockchain Needs 'Proof of Authority' Instead of 'Proof of Stake,'" Cointelegraph, April 26, 2017, https://cointelegraph.com/news/why-blockchain-needs-proof-of-authority-instead-of-proof-of-stake, accessed July 17, 2018).

315 Sovrin: A Protocol and Token, Sovrin Foundation. 17.

316 See Brian Curran, "Plasma & The Raiden Network: Ethereum Scaling Solutions Explained," Blockonomi, September 8, 2018, https://blockonomi.com/plasma-raiden-ethereum-scaling, accessed October 2, 2018.

317 Braendgaard, "Next Generation uPort Identity App released."

318 "About VON," Verifiable Organization Network, accessed July 16, 2018, von.pathfinder.gov.bc.ca/aboutvon/; Baker and Gadgil, "Aadhaar isn't progress - it's dystopian."

319 A replay attack occurs if and when an attacker detects a data transmission and fraudulently has it delayed or repeated. Participants are fooled into believing that their transmission was successfully completed. Replay attacks help attackers gain access to a network, gain information not easily accessible otherwise, or complete a duplicate transaction ("Replay Attack," Techopedia, accessed June 27, 2018, http://www.techopedia.com/definition/21695/replay-attack).

320 Sovrin Provisional Trust Framework, Sovrin Foundation Board of Trustees, 3.

321 Tony Romm, "California legislators just adopted tough new privacy rules targeting Facebook, Google, and other tech giants," Washington Post, June 28,

2018, http://www.washingtonpost.com/technology/2018/06/28/california-lawmakers-just-adopted-tough-new-privacy-rules-targeting-facebook-google-other-tech-giants/, accessed September 28, 2018.

322 Thomas, "Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database."

323 James Griffiths, "UN calls for genocide tribunal over Rohingya crisis," CNN, September 18, 2018, http://www.cnn.com/2018/09/18/asia/myanmar-united-nations-report-intl/index.html, accessed September 25, 2018.

324 Thomas, "Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database."

325 Dell Cameron, "Identity Theft Is Exploding in Developing Countries," Gizmodo, May 3, 2018, gizmodo.com/identity-theft-is-exploding-in-developing-countries-1825745097, accessed July 17, 2018.

326 Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel, "Unique in the Crowd: The privacy bounds of human mobility," Sc ientific Reports 3 (March 25, 2013), 2.

327 Comment from Mike Kail (September 18, 2018).

328 Sovrin: A Protocol and Token, Sovrin Foundation, 21.

329 Michael Sena, "Privacy Preserving Identity System for Ethereum dApps," Medium (blog), uPort, April 26, 2018, medium.com/uport/privacy-preserving-identity-system-for-ethereum-dapps-a3352d1a93e8, accessed September 28, 2018.

330 Secure Hash Algorithms (SHAs) are part of new encryption standards. All Secure Hash Algorithms (SHAs) are related to the general functions of hash encryption that shield data. SHA-2 and SHA-3 are top-level secure hash algorithms, developed through crowdsourcing and part of new encryption standards ("Secure Hash Algorithms (SHA)," Techopedia, accessed June 26, 2018, http://www.techopedia.com/definition/10328/secure-hash-algorithm-sha).

331 Sena, "Privacy Preserving Identity System for Ethereum dApps."

332 "What if people were paid for their data?," The Economist.

333 Reid and Witteman, Everest Whitepaper, 8.

334 See Sovrin Provisional Trust Framework, Sovrin Foundation Board of Trustees, 4.

335 "Overview," uPort Developer Portal, uPort.

336 Christoffer Olausson, "Importance of key management," Symantec Connect, January 9, 2014, http://www.symantec.com/connect/blogs/importance-key-management, accessed July 18, 2018.

337 George Crump, "Why is Encryption Key Ownership So Important?," StorageSwiss, May 16, 2017, storageswiss.com/2017/05/16/why-is-encryption-key-ownership-so-important/, accessed July 18, 2018.

338 Olausson, "Importance of key management."

339 A DID document is a digital document, usually stored in an universally accessible location, that often includes: a timestamp of when it was created; a cryptographic proof that the DID document is valid; a list of cryptographic public keys; a list of ways that the DID can be used to authenticate; and a list of services where the DID can be used (Adam Powers, "Understanding Decentralized IDs (DIDs)," Medium (blog), July 2, 2018, medium.com/@adam_14796/understanding-decentralized-ids-dids-839798b91809, accessed September 28, 2018.

340 "Data Protection and Privacy Legislation Worldwide," United Nations Conference on Trade and Development, April 1, 2018, unctad.org/en/Pages/DTL/

STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx, accessed July 18, 2018.

341 Baker and Gadgil, "Aadhaar isn't progress - it's dystopian."

342 See Ananya Bhattacharya, "Companies can't ask for Aadhaar anymore --or can they?," Quartz India, September 27, 2018, qz.com/india/1402827/supreme-court-verdict-can-companies-ask-for-aadhaar-anymore/, accessed September 28, 2018; and "Government may bring legal backing for private companies to use Aadhaar," The Economist Times, September 27, 2018, economictimes.indiatimes.com/news/economy/policy/government-may-bring-legal-backing-for-private-companies-to-use-aadhaar/articleshow/65973597.cms, accessed September 28, 2018.

NEW AMERICA