HAL
open science

Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion

Fennie Wang, Primavera de Filippi

To cite this version:

Fennie Wang, Primavera de Filippi. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain | www.frontiersin.org, 2020, 2, 10.3389/fbloc.2019.00028 . hal-02445189

HAL Id: hal-02445189

https://hal.science/hal-02445189v1

Submitted on 20 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

frontiers in Blockchain

HYPOTHESIS AND THEORY
published: xx December 2019
doi: 10.3389/fbloc.2019.00028

Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion

Fennie Wang[1] *and Primavera de Filippi*[2]*

[1] *Independent Researcher, New York, NY, United States,* [2] *Harvard University, Cambridge, MA, United States*

After introducing key concepts and definitions in the field of digital identity, this paper will investigate the benefits and drawbacks of existing identity systems on the road toward achieving self-sovereign identity. It will explore, in particular, the use of blockchain technology and biometrics as a means to ensure the "unicity" and "singularity" of identities, and the associated challenges pertaining to the security and confidentiality of personal information. The paper will then describe an alternative approach to self-sovereign identity based on a system of blockchain-based attestations, claims, credentials, and permissions, which are globally portable across the life of an individual. While not dependent on any particular government or organization for administration or legitimacy, credentials and attestations might nonetheless include government-issued identification and biometrics as one of many indicia of identity. Such a solution—based on a recorded and signed digital history of attributes and activities—best approximates the fluidity and granularity of identity, enabling individuals to express only specific facets of their identity, depending on the parties with whom they wish to interact. To illustrate the difficulties inherent in the implementation of a self-sovereign identity system in the real world, the paper will focus on two blockchain-based identity solutions as case studies: (1) Kiva's identity protocol for building credit history in Sierra Leone, and (2) World Food Programme's Building Blocks program for delivering cash aid to refugees in Jordan. Finally, the paper will explore how the combination of blockchain-based cryptocurrencies and self-sovereign identity may contribute to promoting greater economic inclusion. With digital transactions functioning as identity claims within an ecosystem based on self-sovereign identity, new business models might emerge, such as identity insurance schemes, along with the emergence of value-stable cryptocurrencies ("stablecoins") functioning as local currencies.

Keywords: blockchain, self-sovereign identity, migrants, credentials, digital identity

OPEN ACCESS

Edited by:
Oskar Josef Gstrein,
University of Groningen, Netherlands

Reviewed by:
Michael Cooper,
Emergence, United States
Nichola Cooper,
University of the Sunshine Coast, Australia

***Correspondence:**
Primavera de Filippi
pdefilippi@gmail.com

Specialty section:
This article was submitted to Blockchain for Good, a section of the journal Frontiers in Blockchain

Received: *19 September 2019*
Accepted: *20 December 2019*
Published: *xx December 2019*

Citation:
Wang F and de Filippi P (2019) Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Front. Blockchain 2:28. doi: 10.3389/fbloc.2019.00028

INTRODUCTION TO IDENTITY MANAGEMENT SYSTEMS

Q3 In this section, we will introduce a set of principles and terminology relevant in the identity space, particularly as applied Q5 to technologies used to implement identity management systems Q28 such as web standards, cryptography, blockchain ledgers, and cryptocurrency applications.

Preliminary Definitions

There is currently much confusion in the identity space with regard to specific core terms such as "identity" and "identifier," "attributes" and "persona," which are often used interchangeably and ambiguously, without properly defining the meaning and scope of each term. We provide here a preliminary distinction between these terms, along with a tentative definition that will be used in the remainder of this paper.

An "**identity**" has been defined in different manners, depending on the field of endeavor. In psychology, it is generally used to refer to all the psychological traits of a person, inclusive of the personality, beliefs and other personal attributes (Strohminger et al., 2017). In sociology, it includes the culture, history, religion and tradition that an individual is part of Côté (1996). From a legal standpoint, an identity can be associated to the concept of a "natural person" (i.e., an actual human being), or a "legal person" (which might refer to a company, a trust, a partnership, or another collective of people identified as a single person under the law).

For the purpose of this paper, we use the terminology of "identity" to describe all attributes of a person that uniquely defines the person over the course of a lifetime, providing sameness and continuity despite varying aspects and conditions. As such, we distinguish between the notion of "*numerical identity*" which describes the relationship that holds exclusively between a thing and itself[1], and the notion of "*qualitative identity*" which merely describes the properties that different things have in common (Garrett, 2002): only when there is total qualitative identity between two things, can these two things be regarded as being numerically identical.

Yet, even in the context of numerical identity, it is important to note that the attributes of an identity can evolve over time. Identity formation is an ongoing process, whereby a person's identity is developed over the course of the years, and constantly evolves as a result of the interactions with the person's environment (Eakin, 1999). Accordingly, identity is dynamic and multifaceted, and every identity management system must therefore be designed in such a way as to be sufficiently flexible, resilient, and dynamic to accommodate the variable and complex nature of human identity. However, regardless of the sophistication of these systems, no identity management system will ever be able to categorically capture all aspects of one's identity. Indeed, insofar as we attempt to design a system to manage and categorize a variety of different identities, it is important to understand from the outset that such categorization will necessarily be a reduction of the specific facet or use case of each identity it comprises[2].

A "**persona**" is a specific facet of an identity that is expressed in a particular context. While the identity uniquely defines a person, the same person can hold multiple personas, depending on the social context that is taken in consideration (Suler, 2002). For instance, Alice might be a dedicated mom for her daughter, and a loving wife for her husband. She might be a trusted friend to some of her peers, and strict manager to her employees. All these personas are part of the same identity but might display slightly modified features or psychological traits. From a technical standpoint, they can be described as pseudonyms or practical identities (Christman, 2013). While an identity is an abstract concept that relates to the individual as a whole, a persona is a crucial component of any identity management system, because it relates to the way in which individuals "authenticate" themselves to the system (Toth and Subramanium, 2003).

An "**attribute**" describes an essential, definitional property of a person that qualifies it as a member of a given set (or class) of persons. As such, an attribute is generally not unique to that person. Each person can have an indefinite number of attributes: elements like gender, height, weight, handicaps or capabilities which are inherent to the person, or elements like nationality and citizenship, which have been assigned (and could potentially be revoked) by a third-party, with a view to distinguish or organize people into specific categories (e.g., U.S. vs. French citizens). Of course, most of these categories are abstract classes that can be arbitrarily defined, even if they refer to an inherent property. Consider the attribute of having "red hair" that qualifies a person as part of the red-hair people set. Clearly, it is a natural, non-revocable attribute, yet the class of red-hair people is somewhat arbitrarily defined (what is the exact shade of red that qualifies someone as such?). Similarly, the "gender" category which had been for a long time limited to "male" or "female" is recently being expanded with the advent of people who identify as "non-binary." Finally, one of the key characteristic of attributes is that, because they are intended to classify an entity into a particular category, they are not unique to it: multiple entities may share the exact same attributes.

An "**identifier,**" conversely, is not intended to describe or qualify a person, but rather to be used as a "reference" to a real-world identity (or a specific persona). As such, identifiers are often assigned (arbitrarily) by a third-party, with regard to a particular use case or domain (e.g., the legal name of a person, a social security number, or a simple username). In other cases, they can be a particular representation of an observable property of an entity (like fingerprints or other biometric data). It is important to note that both attributes and identifiers are, from a strictly technical perspective, mere data strings that can be used as a means to authenticate a particular individual (or persona). Depending on the domain at hand, the same data string can be used to qualify an entity as a member of a set,

[1] As its name indicates, numerical identity describes the relation through which things can be counted: x and y can be counted as one only if they are numerically identical (Geach, 1973).

[2] This is mostly due to the gap that exists between a first person knowledge of self, and a third party knowledge of a person by description (Burge, 1988).

distinguish from members of different sets, or uniquely identify them within a set. Yet, attributes and identifiers differ with regard to their purpose: an attribute (as a "qualifier") is aimed at classifying people within a particular category, whereas an identifier (as a "reference") is intended to identify someone within a particular domain. Accordingly, even though some identity management systems allow for multiple individuals to share the same identifier (e.g., many individuals share an identical name), or for one individual to have more than one identifier (e.g., in the case of pseudonyms), in order to facilitate the process of identification and authentication, it is often desirable that an identifier be able to identify a person in a *unique* and *unambiguous* way (Jøsang and Pope, 2005). This requires an identity management system to fulfill at least two basic criteria: (1) no two people should have the same identifier (*unicity*), and (2) no one person should have more than one identifier (*singularity*) in the same domain.

In light of this, most identifiers are comprised of a random string of characters that are unique in a particular domain. These are generally issued by a centralized entity, such as a government agency or administrative body, as in the case of a passport number or social security number; or by a company or organization, as in the case of a bank account or an email address. Centralization, in this context, helps ensure a degree of confidence that the identifier is *unique* (i.e., that the same social security number has not been assigned to two different persons) and *singular* to one identity (i.e., that no one may have more than one social security number).

Alternatively, an identifier can be generated directly by the person, as in the case of a pair of cryptographic keys used to access a cryptocurrency wallet. In this case, *unicity* is guaranteed by mathematics—at least at a very high degree of probability (Schartner and Schaffer, 2005), but *singularity* cannot be guaranteed (i.e., the same person can generate more than one identifier). Similarly, decentralized identifiers (DIDs) are an open source web-based standard, which uses a web address (URL) as the unique identifier that contains or points to public identifying information about the identity subject. The public identifying information linked to a DID may include publicly viewable credentials or attestations, or the public key/address of a cryptocurrency wallet. In this way, DIDs may be used in conjunction with blockchain technology and public-private key pairs (Mühle et al., 2018).

Finally, recent technological advances made it possible to develop biometric identifiers that are directly related to the physicality of a person, as in the case of a fingerprint, iris scan or face recognition. If we discount possible errors and inaccuracies related to the technology (Proença and Alexandre, 2010; Canham, 2018), biometric identifiers are often touted as being both *unique* and *singular* to one identity. However, biometric templates are limited to the extent that even the most sophisticated scanning tolls only provide approximate representations (Nagar et al., 2010). This is somewhat mitigated by multimodal biometrics (iris scan, combined with fingerprints, face recognition, etc.) that provide higher degree of rarity (Ross and Jain, 2004). Ultimately, it all depends on the size of a population set (Duta, 2009): given a small population, such identifiers can be said to be unique—although this creates serious privacy problems (see below for more details on the matter).

The Interplay of Identifiers, Personas, and Key Pairs on the Web

With respect to the Internet, the most fundamental identifier, at the network layer, is the IP address, which makes it possible to route packets from one machine to another, until it reaches the right machine. The IP address does not communicate any information about the machine it refers to (i.e., it is not an attribute of it), however, in some cases, it is possible to link an IP address back to a particular individual or organization, whose identity can be ascertained by the relevant Internet Service Provider (ISP)[3].

At the application layer, user accounts and passwords are used to identify specific personas (which may be persons, companies, machines or other entities) interacting on an online service. While these also do not provide, as such, any personal information about the persona, many online service providers require users to communicate additional attributes or identifiers (e.g., real name, age, etc.) in order to ensure that only legitimate individuals can access the service.

Yet, it is worth mentioning that both in the case of an IP address and a user account, only a subset of these identifiers may actually resolve to a natural person. De facto, these identifiers merely refer to a particular endpoint interacting with an online service, but there is no guarantee that this endpoint can be uniquely associated with an individual identity. For instance, an IP address might be used by a multiplicity of persons, and many user accounts are nowadays controlled by bots, rather than persons.

In the context of a blockchain-based system, identifiers are generally managed with public/private key pairs, which uniquely identify the wallet holder (De Filippi and Wright, 2018). Yet, these also do not communicate any personal identifying information about the person, unless additional information is associated with them (Androulaki et al., 2013). Therefore, the same entity (a person, a computer or bot) may own or control multiple key pairs, as key pairs do not necessarily refer to an individual identity. For example, Mary owns a key pair to her Bitcoin wallet, and a different key pair to her Ether wallet.

From a technical perspective, the public-private key pairs are proof of both custody and ownership to any cryptocurrency or tokenized asset held in a particular digital address, or wallet. The private key is necessary to execute transactions to and from the blockchain address identified by the public key. A transaction is not limited to the transfer of a crypto-asset such as a Bitcoin or Ether, but may also represent the transfer or issuance of a cryptographic token through a smart contract transaction (Wright and De Filippi, 2015). An example would be a data access

[3]The European General Data Protection Regulation 2016/679 (GDPR) states that IP addresses should be considered personal data, to the extent that the ISP has a record of the IP address and knows to whom it has been assigned. See recital 30 of the GDPR, which clarifies "online identifier" as mentioned in the Article 4 definition of personal data: "*Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers*".

token, which the owner of a dataset (such as a health record or credit history) issues to a third party wishing to access some of the data. The token functions like a key to the datastore, and transactions of that token are recorded on a blockchain ledger to keep track of who has been granted permission and access (Maesa et al., 2017).

In a public and permissionless[4] blockchain like Bitcoin or Ethereum, which operates without any centralized authority or intermediary operator (De Filippi and Loveluck, 2016), the nodes maintaining the network (e.g., the "miners") operate without association to a particular given identity (El Haddouti and El Kettani, 2019). In a permissioned blockchain, where a centralized entity or consortium is in charge of identifying or policing the nodes that maintain the blockchain ledger, the key-pairs controlled by each miner are generally associated with real world identities (Hardjono and Pentland, 2019). Reliance on real-world identities provides the additional ability to police (and punish), thereby enabling permissioned blockchains to dispense with some of the security measures that anonymous (or pseudonymous) permissionless public chains must employ, e.g., Proof of Work or Proof of Stake (Shrier et al., 2016). The caveat is that users must trust the governance practices of the central entity or consortium policing the permissioned blockchain (Davidson et al., 2016).

Centralized Identification System Based on Unique Identifiers vs. Multifaceted Web of Trust Claims and Credentials System

As previously discussed, the key tenets of any properly functioning identity system are the properties of "unicity" and "singularity." Unicity refers to the fact that each identifier is used to uniquely identify one (and only one) individual, i.e., no two persons should have the same identifier. Singularity refers to the fact that each individual possesses one (and only one) identifier in a particular domain, i.e., no two identifiers should refer to the same individual.

Unicity can be achieved without a centralized authority, because mathematical primitives can ensure that no two people get the same identifier, even if there is no central authority to coordinate the identifiers. Each identity provider can issue an identifier using very large random numbers, and even though there is a theoretical possibility that two actors issue the same identifier to different beneficiaries, the probability is so low to be negligible.

In order to fulfill these the singularity requirements, however, most of the existing identity systems rely on a central authority to ensure that each unique and unambiguous identifier is linked to a singular identity (Kulkarni et al., 2012). The centralized authority must collect personal information to ensure the singularity of any given identifier issued into the system. Such a system is generally expensive and bureaucratic, likely politically impractical for the use case of migrants (especially for vulnerable populations on the move), and subject to high privacy, data abuse, and cybersecurity risks (Whitley and Hosein, 2010). For instance, in 2012, India has launched the Aadhaar identity management system, using biometric data to identify its 1.3 billion inhabitants—many of whom do not have any formal identification (Sarkar, 2014). Participation into the Aadhaar system has become a requirement for Indians to receive welfare benefits, sign up for mobile phones or register at school. However, such a system has raised concerns from civil liberties groups (Jain and Nandakumar, 2012), with multiple lawsuits before India's Supreme Court whether such a system violates India's constitutional right to privacy[5].

Ideally, an identity system should respect the multifaceted nature of identity and look at the different attributes or personas depending on the use cases. Only a small handful of use cases actually require a unique and singular link between an individual and its identifier (i.e., that an individual be identified by a single and unique identifier in a particular domain). This might be the case of voting, whereby a single person should be excluded from voting multiple times under multiple identifiers (Cap and Maibaum, 2001; Alvarez et al., 2009).

An alternative to an identity system based on unique and singular identifiers is a claims and credentials based system (Rannenberg et al., 2015). In such a system, identity is not reduced to an *authoritative* identifier, such as biometric or government issued identification numbers; rather, identity is defined through a network of claims and credentials based on a *web of trust*[6] authentication (Khare and Rifkin, 1997). Such a system better mirrors the multifaceted nature of human identity, allowing for different *profiles* and *personas* to emerge through a combination of different claims and credentials depending on the use cases. A profile that is appropriate for a loan application may be different than the one used in public forums. While such a system would not necessarily guarantee the singularity of individuals using the system, it would suit a large majority of day-to-day use cases.

THE ROLE OF IDENTITY FOR SOCIO-ECONOMIC INCLUSION

For many years, the World Bank has stressed the need for every citizen to be endowed with a valid proof of identity, as identification has become a necessity for financial inclusion and access to essential services and rights. Specifically, from a

[4]A "permissionless" blockchain is a blockchain that anyone can join, and where every node is entitled to both read the current state of the blockchain, and add new blocks to the blockchain. A "public" blockchain, conversely, refers only to the ability to read the blockchain, which can be either permissioned or permissionless based on the rights for who may add information to the blockchain.

[5]Since 2012, Aadhaar was the object of more than 30 petitions and its constitutionality has been repeatedly challenged in courts. In September 2018, the Indian Supreme Court held that, in spite of these claims, Adhaar was legitimate, although with a limited scope and restrictions on data storage. For more information, see https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[6]The "web of trust" concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0: "As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys."

development perspective, a recent report of the World Bank[7] identifies three overarching goals for any identification system:

- ***Inclusion and access to essential services*** *such as health care and education, electoral rights, financial services, and social safety net programs;*
- ***Effective and efficient administration of public services****, transparent policy decisions and improved governance—particularly to reduce duplication and waste;*
- ***More accurate measure of development progress*** *in areas such as reduction in maternal and infant mortality.*

Yet, still today, more than 1.5 billion people are excluded from accessing basic services due to their inability to prove their identity[8]. A large majority of these people are located in Asia and Africa, in areas that lack the proper infrastructure to register births and other life events (e.g., in South Asia and Sub-Saharan Africa, respectively, only 39 and 44% of children have births registered[9]) and generally belong to some of the poorest segments of the population.

At the same time, according to the UNHCR[10], there are currently over 70 million forcibly displaced people as a result of conflict or persecution, 25 million of which are refugees—mostly from Syria, Afghanistan, and South Sudan. There are also approximately four million stateless people, who have been denied a nationality, and therefore have been cut off access to basic services and rights. These numbers are expected to grow in the years to come, especially in light of the growing impact of climate change—which has been recognized as a key contributing factor to political conflicts[11], and as a significant driver to both internal and international migration[12].

In light of this, the UN has recently launched the ID2020 Alliance[13], a multi-stakeholder partnership that brings together multinational organizations, non-profits, businesses and government, all geared toward the objective of ensuring that digital identity is responsibly implemented and widely accessible. The goals of the Alliance are twofold: on the one hand, it is in charge of defining the parameters for good and ethical digital identity systems, and, on the other hand, it is responsible for funding and implementing digital identity projects with a social good mindset. Among other things, the ID2020 Alliance has also created a Certification Mark[14], used to label technological solutions that meet the technical standards and requirements established by the Alliance and that satisfy the principles of portability, persistence, privacy, and user-control.

Many proof-of-concepts are currently being developed by public and private institutions to provide digital identity to those currently lacking formal means of identification[15]. Yet, when devising these identity solutions, it is important to ensure that one single actor does not hold and control the personal identity records of every identified individual, which may raise significant privacy concerns. In the case of refugees lacking proper identification, in particular, digital identity could be used as a means to identify specific individuals or families which are eligible for cash aid or other type of benefits. Yet, because of the fragility of these populations, it is particularly important to find ways to identify these individuals in a unique and unambiguous way, while simultaneously ensuring that their privacy is protected. This requires devising an identity management system that minimizes the control of one single actor over the personal information of a refugee's population.

Hence, while it remains technology-neutral, the ID2020 Alliance has shown particular interest in blockchain technology, as a possible solution to provide digital identities in a way that is both traceable and immutable, and potentially not under the control of one single company or organization. One of the fundamental requirements defined by ID2020 for digital identities is, in fact, that identities remain portable, and that people retain control over their personal data by choosing with whom it can be shared and for what purposes.

Several non-profit organizations in the humanitarian sector are also involved in the definition of best practices and guidelines to ensure that people dealing with migrants and refugees respect their fundamental right of privacy and data protection. Core documentation has been developed in that regard, including the "Handbook on Data Management" (Blazewicz et al., 2012), the Privacy International's report (2018) on the "Humanitarian Metadata Problem,"[16] and the International Committee of the Red Cross' Handbook on "Data Protection in Humanitarian Action" (ICRC, 2017), which specifically addresses the additional privacy requirements that must be put in place when interacting with vulnerable persons. All these guidelines invite organizations providing humanitarian assistance to take all the necessary measures to protect the personal data of all concerned individuals, while focusing on the core humanitarian principles of "do no harm" and the promotion of human dignity.

[7] In 2016, the World Bank's Identification for Development (ID4D) Initiative issued a Strategic framework, recognizing the transformational potential of modern identification systems for the delivery of basic services and rights for the poor. The report is available at the following address: http://pubdocs.worldbank.org/en/215714605674816 55/April-2016-ID4D-Strategic-RoadmapID4D.pdf

[8] World Bank's 2016 ID for Development (ID4D) report showed that ∼1.5 billion people around the world (over 21% of the world's population) cannot prove their identity. See *Ibid.*

[9] *Ibid.*

[10] UNHCR, Statistical Yearbook, available at https://www.unhcr.org/en-us/figures-at-a-glance.html

[11] See e.g., Gleick (2014), describing the extreme drought in Syria as a driving factor for the 2011 civil war, and Werz and Conley (2012), associating the success of al-Qaida's recruiting strategies with the overall decline of agricultural and pastoral livelihoods.

[12] The UN's Global Compact on Refugees recognized that "climate, environmental degradation, and natural disasters increasingly interact with the drivers of refugee movements." According to the Internal Displacement Monitoring Centre, there were 18.8 million new disaster-related internal displacements recorded in 2017. While most disaster displacement linked to natural hazards and the impacts of climate change is internal, displacement across borders also occurs, and may be interrelated with situations of conflict or violence.

[13] https://id2020.org/

[14] https://id2020.org/technical-certification-mark

[15] See e.g., McMullen et al. (2019) analyzing the various blockchain-based initiatives for digital identity, and their various degrees of decentralization and privacy compliance.

[16] https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era

Yet, even if the organization collecting the data respects all of these privacy guidelines, any centralized institution holding such a large amount of personal data inevitably constitutes a single point of failure, which might inadvertently lead to significant data leaks. A true decentralized solution would enable people to maintain full control over their personal data (with a real self-sovereign identity solution), but the lack of a centralized database of identities would make it difficult to guarantee the "unicity" and "singularity" of these identities.

One identified solution to offer a persistent identity from birth, without the need for a centralized authority in charge of assigning a particular identifier to each person, is to rely on biometric data to generate a unique identifier (a biometric hash) associated to every individual. Indeed, in the absence of a centralized authority capable of ensuring that no same person registers twice for an identity, the only way to ensure the singularity of identifiers, without publicly disclosing any sensitive data about the individual concerned, is for these identifiers to be linked to cryptographically-hashed biometric information. This biometric hash can be used as a means of authentication, as it can be verified easily by comparing it with another biometric hash, but it cannot be used to retrieve the biometric information of the individual concerned.

Yet, while such a model is likely to provide important privacy benefits, it comes with the caveat that the singularity of an identifier is inversely correlated with the reliability of the system[17]. Indeed, unicity and singularity are a matter of degree: different identifiers with different characteristics may situate themselves on different points on that continuum. While biometric data could be used to create unique and unambiguous identifiers, whether or not they pass a sufficient threshold of singularity will ultimately depend on the degree of technological sophistication and the size of the population (Bhargav-Spantzel et al., 2010; Unar et al., 2014). We analyze below the benefits and the risks of these systems, in order to assess the extent to which they can be legitimately used for the purpose of refugee's identification and aid disbursement.

BENEFITS AND RISKS OF BIOMETRIC IDENTITY SYSTEMS

Using biometrics as part of an identity management system comes with a few advantages. If people can identify themselves through their biometrics, they no longer need to use passwords (often weak passwords which are easier to remember but very easy to breach). Insofar as a biometric is difficult to forge (or more expensive to forge compared to breaking weak passwords), biometrics may be relatively more secure than existing authentication systems. However, the use of biometrics within an identity management system may raise significant security and privacy risks, depending on how biometrics are used, stored, and permissioned (Prabhakar et al., 2003). For example, biometrics stored in centralized systems, without mitigating data access policies or security design measures, may be subject to greater security risk than if the data were stored locally on the user's device (Muller, 2010).

Hence, in recent years, there has been an increasing amount of research and initiatives exploring the use of decentralized infrastructures, mostly based on blockchain technology, to bootstrap new types of self-sovereign identity management systems (Baars, 2016; Jacobovitz, 2016; Tobin and Reed, 2016; Dunphy and Petitcolas, 2018) and combining them with biometrics as a means to ensure the singularity of identities within these systems (Hammudoglu et al., 2017; Garcia, 2018; Othman and Callahan, 2018).

Without going into the merits of these solutions, we describe below the basic operations and procedural aspects of these identity management systems, focusing on the key issues that must be taken into account when designing an identity system that relies on a blockchain-based infrastructure and on biometric information as part of the identification and authentication process.

Decentralized Infrastructure vs. Centralized Custody of Keys

All blockchain-based systems rely on a public-private key pair to record information (including, but not limited to, financial transactions) on a shared and decentralized ledger. Hence, one important aspect of any blockchain-based identity system is who ultimately possesses or controls the private keys necessary to execute a transaction. On that point, an important distinction needs to be made between the decentralized blockchain-based infrastructure, and the mechanism by which the blockchain-based identity system manages the keys associated with each individual entity.

A blockchain is decentralized insofar as its transaction history is immutably recorded and maintained by a distributed network of computer nodes, in order to prevent systemic theft (i.e., rewriting the transaction history to enable double spending). The decentralized nature of a blockchain network does not, however, apply to the custody and secure storage of the keys that control the individual wallets on that network (Hileman and Rauchs, 2017). Centralized control and storage of these keys is a major security hole that explains numerous high-profile cryptocurrency exchange heists. From a purely technical perspective (notwithstanding legal and contractual obligations), ownership of assets on the blockchain is equated with control of the assets, which is managed through the private keys associated with a wallet that contains the assets.

[17]Biometric information is normally stored in its raw form, rather than hashed, as hash functions require the exact same input each time. While hashing works well for inputs such as passwords that are exact in nature, biometric inputs are variable by nature; as such exact inputs cannot be guaranteed. For example, an iris photographed under slightly different lighting conditions will produce a different input such that the hashed results do not match exactly. Biometric inputs are compared against templates through comparing the number of stable bits extractable from each biometric scan. While it may be possible to hash a biometric input by reducing the number of stable bits required to the minimum, it would make the biometric authentication less reliable. If the number of stable bits required for a match is increased, reliability is improved; however, it will be more difficult to authenticate given the increased difficulty of achieving the required number of stable bits.

To the extent that cryptocurrency exchanges control the private keys associated with the wallets (or accounts internal to the exchange) containing customer funds, they also effectively control these funds, because custody of these keys ultimately implies full control of the funds stored in that account—much like physical paper cash (De Filippi, 2014). Hence, because the customer's private keys were not properly stored and secured in a decentralized fashion, these centralized exchanges rapidly became valuable "honey pots" attracting attackers (Gerard, 2017).

When marrying biometrics with cryptocurrency, it is important not to use biometric data as the seed of the private key unlocking access to cryptocurrency funds. Otherwise, anyone who can acquire access to an individual's biometric data would be able to derive that individual's private key, and therefore unlock the cryptocurrency funds. From a security and privacy perspective, such a system is more dangerous than an ordinary centralized cryptocurrency exchange, as biometric data contain the most sensitive and immutable personal identifying information (van der Ploeg, 2003). In short, even if a decentralized blockchain infrastructure like Bitcoin or Ethereum is used as the backbone of an identity system (De Filippi and Mauro, 2014), the security benefits of decentralization do not transfer insofar as custody of keys remain centralized without mitigating security design factors.

Identification vs. Verification

Next, when assessing an identity system, it is important to identify the types of information that must be provided at the different steps of the process, as individuals enroll into a particular identity system, and as they authenticate themselves within that system. We analyze below the various steps with regard to a biometrics-based identity system based.

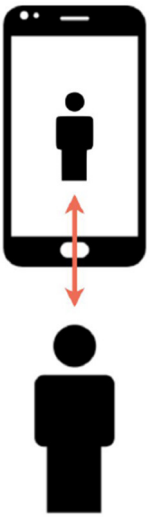
Enrollment

Enrollment is the process of creating a new user identity on the biometric system. Each user must provide relevant biometric samples (e.g., fingerprint, iris, or face) that will be captured by a biometric scanner or similar device. The collected biometric data will be used to generate a biometric template and biometric identifier, associated with personal information (such as demographic data) for subsequent authentication purposes (Araújo et al., 2005).

Authentication

Authentication is the process by which, after individuals have enrolled into the system, the system checks whether these individuals have the proper permissions to access a particular service or to benefit from a particular type of aid, by matching a new biometric sample against the biometric template created during enrollment (O'Gorman, 2003). The authentication stage can be subdivided into two different steps: *identification* and *verification*.

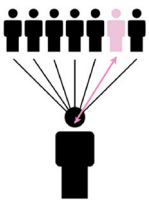
Verification



Verification is the process of verifying one's identity. It provides an answer to the question: are you who you say you are? It is a one-to-one matching process, whereby a new biometric sample is matched against an authenticated record. This is the case of using a fingerprint or face scan to access devices like computers or mobile phones. Currently, the standard practice is that the biometric record is stored locally and in encrypted format on the actual device (Schneier, 1999). Thus, neither mobile app developers nor device manufacturers have access to the template. The original scan used to create the template for matching purposes is destroyed, and so are the new scans made upon each new login, once the matching process is complete (Uludag et al., 2004).

Local storage of the biometric template on the device (rather than a central server) is a form of decentralized data storage, which can be further decentralized by breaking the biometric template into multiple pieces that must come together in order to be readable. This method protects privacy and improves security (Zibran, 2012).

Identification



Identification is the process of retrieving the identity of a particular individual, based on an identifier. It provides an answer to the question: who are you? It is a one-to-many matching process, whereby a new biometric sample is matched against many templates in an identity database in order to retrieve the specific identity it has been associated with (Jain et al., 2007).

Ideally, the sample scan should be destroyed once the transaction is complete. However, the original biometric template must necessarily be stored on a server, or be otherwise accessible

to the operator of the identity system, for matching purposes. Therefore, as opposed to the verification process which can be done locally on a user's device, in the identification process, biometric templates need to be accessible online. In order to minimize security risks, it is thus important to identify mechanisms for secure decentralized storage and processing of data (Ganapathy et al., 2011), such as secure multi-party computation (Goldreich, 1998) or emerging solutions based on homomorphic encryption (Gentry and Boneh, 2009).

Individual Control vs. Organizational Control of Personal Data

Except for the case where the biometric template is stored locally on the user's device (mostly for verification purposes), in all other cases described above, the biometric and personal identifying information is not under the possession of the data subject, but rather that of the organizations that collect, store and administer the data for a particular identity system. While data protection regulations—especially in Europe—enable the data subjects to restrict the collection and processing of personal data (Tikkinen-Piri et al., 2018), once collected, such data might remain under the control of whoever owns the hardware (servers, devices) where the data is stored. The same is true for behavioral and social data that corporations collect about their users, which are statistically compiled as identity profiles that may be used for purposes of advertisements, alternative credit scoring, identity verification, and so on (Bygrave, 2012).

Privacy laws and data protection regulations provide some protection in terms of how information may be stored, used or collected. However, data protection regulations merely impose an obligation for data collectors and processors to obtain *informed and explicit consent* from the data subjects before they can engage in the collection or use of personal data for a particular purpose (Kosta, 2013). Some jurisdictions—such as Europe with the newly enacted General Data Protection Regulation[18]—have introduced additional rights, including the right to data portability[19] and the right to erasure[20] (better known as the right to be forgotten). Yet, where such protections do not exist, there is a risk that personal data (including biometric templates or samples) will remain siloed by the organizations that control them, with no real possibility for the data subject to request the deletion or the portability of such data—unless such organizations implement their own privacy policies that enforce these requirements.

[18]The General Data Protection Regulation (GDPR) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.

[19]Article 20 of the GDPR stipulates that: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided"

[20]Article 17 of the GDPR stipulates that: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed."

Biometrics vs. Other Types of Identifiers

While biometrics provide interesting benefits to an identity management system, they are not devoid of any drawback. First of all, using biometric data to create a singular and unique identifier obliges individuals to identify themselves as one and only one persona—even when it is not necessary for a particular use case (Jain et al., 2004)—which may present significant privacy issues, especially in the case of political refugees.

Biometrics can also be significantly more problematic than traditional forms of authentication (e.g., passwords and other identifiers such PIN codes, hardware devices, etc.) because one cannot change his or her biometric data (Prabhakar et al., 2003). Importantly, biological information is effectively public information: we are leaving biological information everywhere, e.g., fingerprints, DNA, recordings of our gait, photographs of our faces or irises—from which advanced computer algorithms can extract a biometric template (Mordini and Massari, 2008). Fingerprints are easily stolen, copied, or lifted. Facial recognition can be easily spoofed through photographs or videos. Iris scans or behavioral biometrics such as gait may be more difficult or expensive to spoof or copy, but are not foolproof (e.g., contact lenses can fool iris scans). Accordingly, because of their inherently public nature, biometrics should only be used as the username (i.e., public key) rather than the password (i.e., private key). Whenever biometrics are used, some form of second factor authentication should be required, such as a PIN or a physical token, verification of photo ID or a physically present person (Rane et al., 2013).

Moreover, our bodies are subject to physical change. Iris scans become clouded due to cataracts. Fingerprints may disappear due to hard labor or burns. Gait may change due to aging, accidents, or illness. According to a study[21] by the National Institute of Standards and Technology (NIST), even in healthy people, the error rate for single iris scans can range from 2.5% to up to 20% in some cases—a significant percentage given the world's population of 7.5 billion people. As identity practitioners like Vinay Gupta have argued, because of the complex variation and nuance of biological forms, it is fundamentally impossible to rely on biometric measures as singular and unique identifiers for human beings[22] Indeed, if biometrics are used as a universal identifier of one's identity and rights, the consequences for those in the three percent baseline error rate may be paralyzing and dire. For instance, in the case of India's biometric ID system, one study showed that 20 percent of the households in Jharkand state had failed to get their food rations due to biometrics errors—which is five times higher than the failure rate of ordinary ration cards[23].

Finally, because of the public perception of biometrics as being more "scientific" and therefore more authoritative, the downside errors of biometrics is often overlooked. Yet, if a biometric identifier is used as the backbone of an identity management

[21]https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910385

[22]https://medium.com/humanizing-the-singularity/a-blockchain-solution-for-identity-51fbcae94caa

[23]https://www.independent.co.uk/news/world/asia/india-tech-fingerprint-eye-scan-id-food-benefits-bank-accounts-a8297391.html

system used for the protection of fundamental rights and privileges, it cannot fail disastrously, even if the probability of a failure is very small. Ideally, a properly functioning identity system must be resilient against low probability but highly consequential negative events and gains value from increased input and interactions with the world. However, an identity system that relies on biometrics as the only authoritative identifier is not only a brittle and fragile system (Friedman et al., 2011), it is also highly problematic from a cybersecurity and privacy perspective (Prabhakar et al., 2003; Campisi, 2013)—which is particularly relevant for vulnerable populations such as migrants and refugees.

SELF-SOVEREIGN IDENTITY AND CREDENTIAL MANAGEMENT SYSTEMS

The notion of self-sovereign identity has emerged in the past few years, although there is no agreed upon definition yet on what the terminology really means (van Wingerde, 2017). On a general level, self-sovereign identity is intended to preserve the right for the selective disclosure of different aspects of one's identity and the various components thereof, in different domains and contextual settings. This right should apply irrespectively of whether these aspects and components have been issued by a particular government, company, or organization. More specifically, self-sovereign identity also refers to the idea that individuals shall retain control over their personal data and, to a certain degree, over the representations of their identities (or personas) within a particular identity management system. This requires giving them the ability to establish (and control) who has the right to access specific pieces of information about them, with a high degree of granularity (Der et al., 2017).

From a technical perspective, self-sovereign identity is generally regarded as a new paradigm of online identity management, whereby individuals and entities can manage their identity-related information (i.e., identifiers, attributes and credentials, or other personal data) by storing them locally on their own devices (or remotely on a distributed network) and selectively grant access to this information to authorized third parties, without the need to refer to any trusted authority or intermediary operator to provide or validate these claims (Mühle et al., 2018). This enables greater control over personal identifying information, or other relevant data about an individual or entity. Because digital identifiers can be in a variety of formats, an important requirement for a global identity system is the establishment of technical standards for interoperability. We describe below the most prevalent standard, the Decentralized Identifier (DID), that we mentioned earlier in the paper.

Open Source Digital Identity and Verifiable Claims Web Standards

The World Wide Web Consortium (W3C) is a technical standards body for the open internet, working on a decentralized identifier (DID) standard[24] DIDs are a new type of identifier for verifiable, self-sovereign digital identity that is universally discoverable and interoperable across a range of systems[25] The DID standard is supported by the Decentralized Identity Foundation, a consortium of companies that are developing and building applications using the DID standard, including Microsoft, IBM, Hyperledger, Accenture, Mastercard, RSA, and all the major blockchain identity and data companies such as Civic, uPort, BigChainDB, Sovrin, and many others[26].

DIDs are URLs (i.e., unique web addresses) that resolve to a DID Document, which provides information on how to use that specific DID[27]. For example, a DID Document can specify that a particular verification method (such as a cryptographic public key or pseudonymous biometric protocol) can be used for the purpose of authentication. The DID document might also reference a series of service endpoints, enabling further interactions with the DID controller. For instance, a DID can reference the location of associated personal data, which a requester would need to ask the DID controller for permission to access (McMullen et al., 2019).

A DID by itself is only useful for the purpose of authentication. It becomes particularly useful when used in combination with verifiable claims or credentials—another W3C standard that can be used to make any number of attestations about a DID subject (Dunphy and Petitcolas, 2018). These attestations include credentials and certifications that grant the DID subject access rights or privileges. For example, a verifiable claim can attest that an individual has been Know-Your-Customer (KYC) approved and therefore eligible to open a bank account, that the same individual has been certified as eligible to drive, or authorized to access certain programs as a system administrator (Aydar and Ayvaz, 2019).

A verifiable claim contains the DID of its subject (e.g., a bank customer), the attestation (e.g., KYC approval), and must be signed by the person or entity making the claim using the private keys associated with the claim issuer's DID (e.g., the bank). Verifiable claims are thus methods for trusted authorities, such as banks, to provably issue a certified credential associated to a particular DID. DID claims remain under the control of the DID subject and can be used to prove a particular attribute of the DID subject, independently from a certificate authority, an identity provider or a centralized registry (Baars, 2016). Proving to be the actual subject of that DID (through a specified authentication method) will enable an individual or entity to benefit from access privileges associated with these credentials.

While DIDs are independent of and do not require blockchain technology, they are designed to be compatible with any distributed ledger or blockchain network. Since a DID may be associated with a particular private/public key pair used to sign

[24]W3C is led by internet industry pioneer Tim Berners-Lee, who invented the World Wide Web. W3C has 479 members including all the major internet and technology companies such as Amazon, Apple, Boeing, Cisco, Microsoft, Google, Facebook, Alibaba, Tencent, Baidu, along with research universities and governments. See https://www.w3.org/

[25]See W3C DID primer for introduction: https://github.com/w3c-ccg/did-primer

[26]https://identity.foundation/

[27]https://w3c-ccg.github.io/did-spec/

identity claims, it is possible to associate that key pair (i.e., the key pair linked to the DID) with key pairs used to sign financial transactions on a blockchain. Most importantly, the DID specification also makes it possible to associate particular methods to a DID, which specifies the procedures for key registration, replacement, rotation, recovery, and expiration. Several method schemes have been implemented so far that leverage the resilience and tamper-resistance of blockchain technology to manage DIDs (e.g., BTCR DID, Blockstack DID, Ethereum ERC725 DID)[28]. The W3C group is working to ensure technical interoperability between different DID methods.

It is important to note, however, that given the transparency and immutability of a blockchain, personal information should never be stored on the blockchain itself (De Filippi, 2016). Yet, a blockchain can be used to track permissioning and access of personally identifying data that is stored off-chain, thereby creating an auditable trail of information access. Therefore, in addition to the standardized DID methods, a blockchain can also be used for the recording and eventual revocation of claims or attestations, for the granting and revocation of access to personal data stores[29], and other functions that may be specific to particular identity system (e.g., claims filed and resolved as part of a dispute resolution system regarding false attestations).

A Road-Map Toward Self-Sovereign Identity

The road toward true self-sovereign identity is still long, as we are only at the early stages of understanding how to implement a digital identity system that provides full control and autonomy to the individuals. Yet, in light of the refugee crisis in Europe, and the increasing number of displaced people who lack a formalized form of identification, today—perhaps more than ever—the quest toward self-sovereign identity has become of crucial importance.

As described earlier, self-sovereign identity solutions are designed to give individuals control over their own identity—that is, people should have the possibility to decide precisely what information to disclose about themselves, to whom, and under what circumstances. Under a self-sovereign identity model, identity providers should not have the possibility to prevent individuals from exercising basic human rights, such as the right to be oneself, the right to freedom of expression and the right to privacy. While this does not necessarily require individuals to be the sole holders of any information regarding themselves, an important precondition for self-sovereign identity is that digital identities are not locked into any given platform, nor controlled by a given operator, but rather remain portable and interoperable across multiple platforms, so that individuals are free to choose the identity operator that they trust the most, and to move from one operator to another, if so desired.

While a precise definition of what constitutes a self-sovereign identity does not currently exist, a series of criteria have been identified as the underpinning principles of self-sovereign identity[30]. These principles can be regarded as a preliminary benchmark to assess existing self-sovereign identity solutions:

1. **Existence**: individuals must have an independent existence, independently of the digital identifiers that merely serve as a reference to them.
2. **Control**: individuals must control their identities, they should always be able to refer to it, update it, or even hide it—even if others can make claims about these identities.
3. **Access**: individuals must have access to all the data related to their identities, and should be able to retrieve them claims whenever needed.
4. **Transparency**: systems and algorithms used to administer and operate digital identities must be open and transparent, with regard to both their operations and maintenance.
5. **Persistence**: identities must be long-lived, preferably they should last forever, or at least for as long as the user wishes to maintain them.
6. **Portability**: information and services about identity must be transportable, and not be held by a single third-party entity, even if it's a trusted entity.
7. **Interoperability**: identities should be as widely usable as possible, as opposed to being framed only to work in siloed environments.
8. **Consent**: individuals must agree to the use of their identities, sharing user data must only occur with the consent of the data subject.
9. **Minimization**: disclosure of claims must be limited to the minimum necessary to accomplish the task at hand
10. **Protection**: the rights of users must be protected at any cost, even if doing so would go counter to the interests of the identity providers.

Most digital identity projects will not meet all of these criteria—and many do not even purport to qualify as "self-sovereign" identity projects—we will discuss in this paper two case studies that make use of biometrics in combination with blockchain technology to provide users with a certain degree of sovereignty over their digital identities. The first case study is the *Kiva Protocol*, which focuses on identity for credit scoring and secure sharing of credit history amongst microfinance institutions. The second case study is the World Food Programme's *Building Blocks* and its biometric identity solution for delivering services to beneficiaries in need—particularly in providing better delivery of services to beneficiaries served by multiple UN agencies.

These two initiatives were chosen because of their higher degree of technological readiness with respect to other alternatives, their credibility and their potential impact in terms of future large-scale deployment, and, finally, because of the previous experimentations they have undertaken, which enabled us to collect valuable data points concerning the extent to which their current implementation fulfills the criteria of a self-sovereign identity system.

[28] A list of currently available DID method schemes is available at: https://w3c-ccg.github.io/did-method-registry/

[29] For a general overview of the different blockchain-based self-sovereign identity solutions and their characteristics, see (McMullen et al., 2019).

[30] The Path to Self-Sovereign Identity, written by Chris Allen and the Rebooting Web of Trust community: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md

As the following sections describe, these two projects have prioritized specific principles of self-sovereign identity that are most relevant to their use cases. In both of the cases, it appears that the identity solutions focus, first and foremost, on principles relating to interoperability and the secure sharing of identity claims between parties. The principles of minimization, consent, portability, and persistence are also given significant importance. The use of a blockchain ledger is useful because it enables data to be shared securely across multiple parties, and parties must be granted permission in order to access and append information to the blockchain. From an identity perspective, a persistent and portable digital identity and digital history is highly valuable to vulnerable populations who are often on the move. The validity of the attestations, especially from trusted organizations such as Kiva and UN agencies, are important for the identity subject to establish or re-establish credibility and access to resources.

However, the principles of control and access remain difficult to achieve from a technical perspective in developing economies, as smartphone penetration and technical knowledge necessary for self-custody is still nascent. The lack of proper connectivity and hardware infrastructure (e.g., while most refugees do have a mobile phone, they do not always have a smartphone) is a key obstacle to overcome in the roadmap toward self-sovereign identity. Both Kiva and the Building Block initiatives therefore had to implement custodial models for their identity solutions, significantly reducing the degree of control that individuals can exercise over their digital identities. However, that may change over time as smartphones become cheaper and users become more technically knowledgeable. In any event, both case studies provides valuable lessons concerning the multiple obstacles associated with the implementation of self-sovereign identity solutions in the humanitarian context, and the different approaches adopted by each of these initiatives, as an attempt to overcome these obstacles in the short term while focusing on the immediate user needs.

KIVA CASE STUDY: SOLVING FOR CREDIT HISTORY[31]

Kiva[32] is building an identity protocol that is expected to be rolled out across the whole country of Sierra Leone—this is a testament to the strength of the programme and the significance of provisioning vulnerable persons with a digital identity system.

Kiva is based on the DID and credentials model described above, using Hyperledger Indy as the underlying blockchain layer. It relies on a credential-based identity system, whose basic identifier is a public/private key pair, to which multiple claims and attestations can be associated. In the Kiva protocol, issuers of verifiable credentials are called "trust anchors" who have real world reputations at stake. The Kiva identity protocol is currently designed as a private permissioned system, whereby all trust anchors must be approved by Kiva and/or the Sierra Leone government in order to issue credentials, sign attestations, and read identity claims. In the future, trust anchors may be broadened to include NGOs, technology companies such as Facebook and Google, and other organizations that can provide information relevant to a particular identity[33].

Currently, trust anchors are limited to the Sierra Leone government bodies and microfinance institutions, because of the immediate goal of solving the problem facing the microlending industry—whereby many constituents are ineligible for loans due to lack of any formal identity and history (data for underwriting loans). In fact, the government of Sierra Leone, through the influence of the Central Bank which issues bank licenses, will *require* that all microfinance institutions, banks and other financial institutions, participate as credential issuers for Kiva's identity system. This is particularly relevant for microlending in developing economies that do not have national credit bureaus, making it difficult for lenders to check cross indebtedness. Without the ability to check the total indebtedness of a borrower, it is difficult to properly price default risk and underwrite these loans.

The Kiva protocol functions like a credit bureau with greater privacy and control by the individual compared to traditional credit bureaus. The credit profile, comprised of linked credit attestations and claims, is portable by the individual, rather than locked within a centralized credit bureau. Importantly, individuals have control over who can access their profiles, whereas currently anyone can perform a credit check without permission. Under the Kiva model, an individual may decide whether to provide a lender access to her credit history.

Kiva will provide every Sierra Leone citizen eligible for a government issued ID with a DID and associated public/private key pair to sign identity claims, along with a first attestation from the Sierra Leone government (in the form of a verifiable credential containing hashes of the citizen's biometrics and other government-issued identifiers). In the Kiva framework, biometrics are simply another attribute that is attached to the DID, similar to a date of birth, place of birth, or any other piece of identity information. This reduces much of the systemic risk of using biometrics as an exclusive form of identification, as described above. In this system, because biometric data do not serve as an identifier, biometrics will be used primarily for verification rather than for identification purposes.

Anyone seeking to access the information linked to that profile must request the DID subject (i.e., the Sierra Leone citizen) to grant permission. The Hyperledger blockchain is used to record that a third party (as identified by its public key linked to a DID) requested, was granted, and was eventually revoked access to the relevant verifiable claims or credentials, according to timestamps. Each citizen will have a root-DID that maps to an unlimited number of sub-DIDs that are generated for each new loan transaction or relationship with a lender. Sub-DIDs can also

[31] Most of the information in this section has been drafted as a result of several calls and interviews with kevin o'brien and aaron goldsmid from kiva.

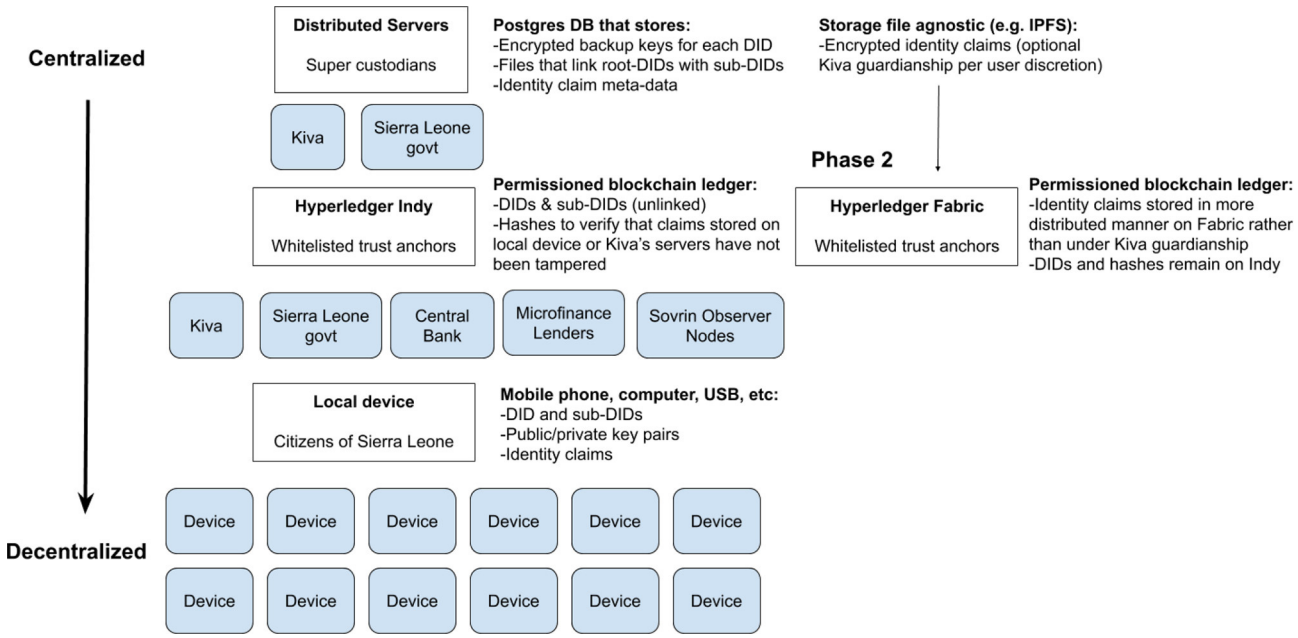
[32] https://www.kiva.org/protocol

[33] A future identity protocol may enable permissionless trust anchors that do not need to be centrally approved *ex ante*; or else, trust anchors may be automatically approved according to a set of programmable rules e.g., number of credentials or types of credentials associated with a particular trust anchor to establish their reputation.

be created for different purposes i.e., each sub-DID represents a different persona or profile. The use of sub-DIDs enables a degree of privacy (see below section on privacy).

Kiva Protocol Architecture

The following is a high-level architecture of the Kiva identity protocol:



In an ideal model, all sensitive information, such as private keys, the files that link root-DIDs with sub-DIDs, identity claims and other information are stored only locally on devices controlled by the identity subject, such as mobile phones and computers. Thus, control and storage of personal information is structurally decentralized. In developing countries, however, this will take time as smartphone penetration is still low (though growing rapidly in many markets) and many people may not necessarily own individual devices i.e., a phone may be shared amongst a family. Currently, it is not possible to securely store private keys on feature phones. Therefore, it is likely that third parties such as non-profits or commercial businesses may serve as proxies that help manage private keys or shared devices. Ideally, private keys are never shared and remained locked in wallets on shared devices, whereby users can unlock their individual private keys using biometrics, PIN or password when they access the shared device.

Even if non-profits and other community organizations serve as trustees or proxies to help users manage their private keys, backups of identity claims and private keys will be necessary. In light of the practical difficulties of managing the public/private key pairs associated with a particular DID, the Kiva identity protocol deploys a guardianship model, whereby Kiva and the Sierra Leone government serve as the super custodians in the system. Kiva will escrow the key pairs on behalf of the identity subject, who may take the key pairs out of escrow at any time. Under Kiva's guardianship model, backup keys in custody are encrypted and can only be restored through a multi-factor process e.g., biometrics and/or PIN.

Kiva's servers also store the data files that map the links between root-DIDs and related sub-DID, as well as backup copies of encrypted identity claims (with accompanying meta-data) on a separate data storage format such as IPFS. In the next phase of the protocol, the encrypted identity claims may be stored in a more distributed manner on a permissioned ledger such as Hyperledger Fabric, which is better designed to store data, whereas Hyperledger Indy is fit-for-purpose for validating DIDs.

The most private and sensitive data is held in guardianship on Kiva's distributed servers in a Postgres database. A local copy of the database (or parallel database) may be maintained by the Sierra Leone government, pursuant to Sierra Leone data localization regulations that require sensitive citizen data to be stored in-country.

Beneath the Kiva guardianship layer is the private permissioned blockchain ledger running on Hyperledger Indy. The Central Bank of Sierra Leone would be a permissioned node, along with Kiva and the Sierra Leone government. Because the Central Bank is requiring all lending institutions to report loan transactions on the protocol, the microfinance lenders and other financial institutions that fall under the Central Bank's mandate will be required to register as nodes. In addition, other parties such as non-profits, may apply to be Trust Anchors or Stewards (Sovrin observer nodes), which helps increase the security and resiliency of the ledger by diversifying nodes away from entities domiciled in Sierra Leone.

The nodes store copies of the unlinked DID and sub-DIDs, as well as hashes of the associated identity claims. As noted above, Hyperledger Indy is not designed to store actual claims data, which identity subjects will have the choice to store in Kiva's guardianship, and later those claims can be migrated to

Hyperledger Fabric, which is built to support claims data, as described above.

Interacting With the Kiva Protocol: Step-by-Step

We describe here the intended step-by-step operations of the Kiva protocol, and how a Sierra Leone citizen might interact with the Kiva protocol, once fully deployed. The Sierra Leone government will deploy campaigns to enroll citizens into the identity protocol. Citizens will register at polling stations, where they will receive both a physical ID card with biometrics and a digital ID, in the form of a DID and associated private keys held in a wallet, ideally on the individual's device. In many cases, as described above, the individual may not own a phone or have a phone with the capability to hold private keys in a wallet. In this case, the keys and future identity claims will be held in guardianship by Kiva. The government of Sierra Leone will make the first attestation by signing an identity claim that the individual is a citizen of Sierra Leone with official identity information such as biometric string, date of birth and other data.

When the individual, whom we will call Mary, goes to the local microfinance lender to ask for a loan, the bank will first ask for Mary's identity claim signed by the government of Sierra Leone (the official state ID). Mary will access an application (either on her phone or on a device at the bank) that grants the bank permission to validate the government's signed claim. Ideally, to preserve privacy, a bank does not actually read the contents of the claim (e.g., the biometric, the date of birth) if such information is not actually relevant for purposes of KYC or credit underwriting. All the bank needs to know is that the government has signed a valid claim attesting to Mary's identity, which fulfills the bank's minimum KYC obligations.

Next, the bank will ask Mary for permission to disclose her credit history. If Mary says yes, Mary will then unlock her identity claims using her private key. The bank will then validate the identity claims against the hashes in Hyperledger Indy to confirm that the identity claims are both complete and authentic. If there is an error, the bank will receive a failure message.

If Mary is unable to use her own device to manage identity claims and keys, the bank will ask for permission to retrieve the identity claims from Kiva's servers directly. In order to sign this permission using her keys in Kiva's custody, Mary would need to provide a second factor authentication such as her biometrics or PIN.

Once a loan is approved, the bank would sign identity claims relating to the loan disbursement and repayment. Mary would receive messages to her mobile phone application informing her that the bank is writing a claim e.g., regarding repayment, and Mary could accept this action[34]. The claim would be sent to Mary's device, if she chooses to only keep data on her local device; or else the claim would be encrypted and stored in Mary's wallet in guardianship on Kiva's servers (Kiva may also store a backup copy if Mary so chooses even if she manages her data on her own device).

Mary may also initiate a dispute resolution action if she believes the bank has written an incorrect claim or failed to provide a claim for a repayment. The dispute resolution process will likely be off-chain, whereby Mary would file a ticket with the facts to be decided by an arbitral body. If the arbitral body decided in Mary's favor that she did indeed pay the bank in cash for her monthly installment, the arbitral body would then require the bank to sign such a claim, or else the arbitral body could sign such a claim with its own keys.

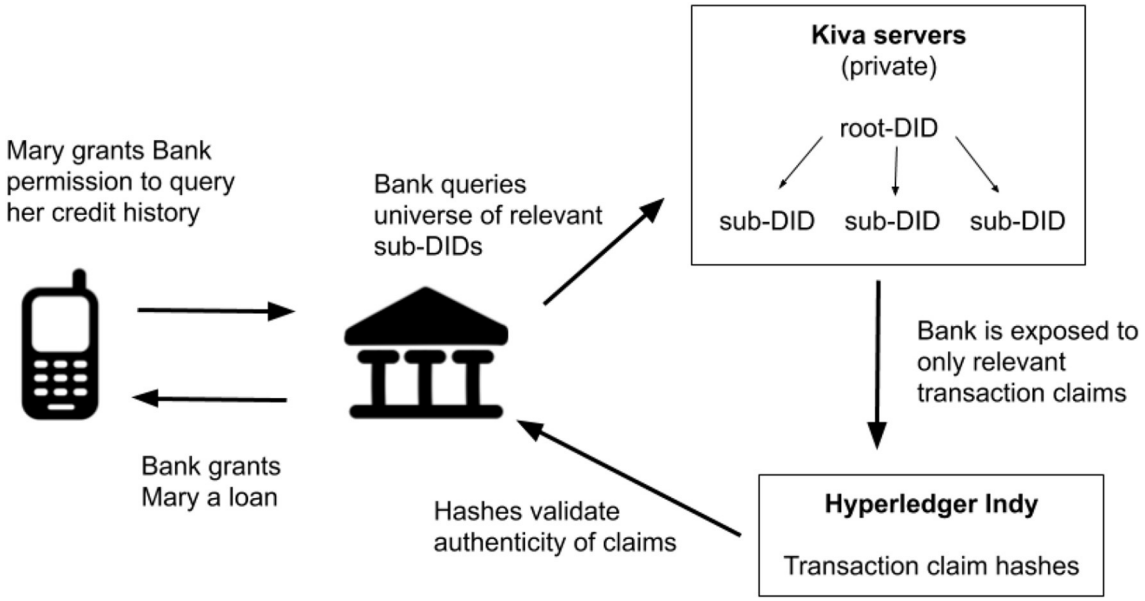
Where loans are made and repaid in cash, Mary would need to trust her bank to make the repayment claim. She would likely receive a physical receipt for her cash repayment, which she could present to the bank to request a repayment claim (or to an arbitrator if her bank fails to do so). In a future model, if the loans were disbursed as digital currency, disbursements, and repayments could be automatically recorded as identity claims, with the blockchain transactions appended as proof of payment.

Privacy Considerations vs. the Problem of Selective Disclosure

In order to maintain privacy and reduce fallout from security breaches, the Kiva protocol strives to operate under the principles of zero knowledge proofs, whereby only the absolute necessary information is exposed and measures are taken to ensure that no one can seek information in the system without permission. Accordingly, each loan that Mary takes will be associated with a new sub-DID, rather than directly tied to her root-DID. This prevents banks from being able to monitor future credit activity tied to a root-DID without asking the identity subject for permission, as future credit transactions will be associated with newly generated sub-DIDs, and banks do not have access to the file that maps sub-DIDs to the root-DID.

Privacy is countered with the problem of selective disclosure, whereby lenders must check for cross-leverage. During the underwriting process, Mary's bank can see the full credit history across her sub-DIDs because during the validation process, the bank will first query Kiva's servers to get the universe of sub-DIDs tied to Mary's root-DID. As described above, the file that maps sub-DIDs to a root-DID is only available on Kiva's servers. However, at no time is the bank exposed to the actual sub-DIDs or root-DID; the bank is only exposed to the transaction claims associated with the sub-DIDs. The bank will then proceed to match the transaction claims against the hashes in Hyperledger Indy to authenticate the claims, as described above.

[34] Initially, Mary will give permission at the outset for her bank to write *all* claims related to her loan for the duration the loan remains outstanding. In the future, Kiva hopes to provide even greater control to users (especially as technology penetration improves), such that Mary would be able to grant permission for *each* claim that the bank wishes to append to her profile.



Even in the case of a fully self-sovereign identity system, not all data will be owned and controlled by the individual, as some of the data may be produced and maintained by third parties making attestations. For example, a bank will retain control over its own records regarding an individual's lending history with that bank. However, compared to a centralized credit bureau, information will not be centrally aggregated and communicated to a single operator. Data can remain stored by third parties, while the associated attestation (in the form of a verifiable claim) is assigned and controlled by the individual and stored on the blockchain. Hence, even though the citizens of Sierra Leone may not control all the information regarding them, they nonetheless control the set of verifiable credentials that represent their attributes, which they can freely combine into a useful identity or set of profiles and personas.

Finally, it is important to note that Kiva's identity system is, at its root, a repository of verifiable claims data, which does not discriminate against politically sensitive identity claims. While it has been designed for Sierra Leone, the same identity system may be applied, for example, to Syrian refugees, allowing the Syrian government to issue attestations concerning the identity of a particular refugee, with a signature and time stamp. If the Syrian government that issued the identity no longer exists, the refugee will nonetheless be able to prove his or her identity at that particular point in time.

In returning to our list of self-sovereign identity principles, the Kiva identity system focuses first on consent, interoperability, and minimization. This serves the primary use case of enabling microfinance institutions to share information and create a persistent record of credit history, in a way that still preserves the privacy of the borrower by revealing only the necessary information for a microfinance institution to make a decision. While most users will not be self-custodying their identity information from the outset due to technical challenges, the system is designed such that users may opt out of Kiva serving as a super custodian. Over time, self-custody and control will become more prevalent, and identities remain globally portable and persistent.

WORLD FOOD PROGRAMME CASE STUDY: SOLVING FOR OPTIMIZATION AND HARMONIZATION OF AID ACROSS U.N. AGENCIES[35]

Background

The World Food Programme (WFP)[36] is the food assistance branch of the United Nations and the world's largest humanitarian organization addressing hunger and promoting food security. WFP provides food assistance to more than 80 million people in more than 80 countries.

In the past several years, the trend has been to enable the people served to make their own purchasing decisions through Cash-Based Interventions (CBI) rather than in-kind food distributions. In 2018, WFP distributed more than USD 1.7 billion in CBI, more than half of the global cash aid distributions[37]. In the right conditions, CBI programs can be more cost-effective and beneficial to the local economies as well as providing an increased element of dignity to the people served.

WFP has pioneered innovation amongst UN agencies, recognizing the potential for blockchain technology in CBI as fourfold: (1) improved efficiencies such as reductions in costs and risks and enhancements in accountability and control, (2) creating a unified view of the people served thereby reducing duplication and fragmentation, creating

[35]MOST OF THE INFORMATION IN THIS SECTION HAS BEEN DRAFTED AS A RESULT OF SEVERAL CALLS AND INTERVIEWS WITH HOUMAN HADDAD FROM THE WORLD FOOD PROGRAMME.

[36]https://www1.wfp.org/overview

[37]https://www.economist.com/free-exchange/2014/03/03/giving-generously

opportunities for optimization and harmonization, and linking various aid actors through a single connection to the blockchain, (3) multiplying the redemption options (such as ATMs, food stores, health networks, and schools) available to the participating organizations and the people served, and (4) paving the way for blockchain based digital identities by demonstrating the underlying technology in practice and bringing key stakeholders together around a neutral blockchain network.

Building Blocks

In this section, we describe WFP's blockchain-based CBI project called "Building Blocks"[38] Building Blocks was born in January 2017 with a 100-person Proof-of-Concept (PoC) in Pakistan's Umerkot village. At the time, the aim was to demonstrate that blockchain can be used beyond the cryptocurrency application.

For the PoC, beneficiary accounts were created on the blockchain and loaded with tokens representing cash or food and each beneficiary was assigned a random identifier between 1 and 100, which was linked to their public key one-to-one. To redeem their entitlements, beneficiaries would present themselves at cash or food merchants and provide their random identifier. The merchant would then insert the beneficiary's identifier along with the redemption amount into a web application. The web application would send the request to Building Blocks which would then send a One-Time Password (OTP) to the beneficiary's feature phone via SMS as the authentication mechanism. The beneficiary would then provide the OTP to the merchant who would insert it into the web application and send it to Building Blocks. If the OTP was valid, Building Blocks would check the requested redemption amount against the available blockchain entitlements and, if sufficient, trigger the beneficiary private key held in custody to record a transaction and send a confirmation back to the merchant. Upon seeing the confirmation, the merchant would distribute the requested quantity of cash or food to the beneficiary. WFP would then, based on the Building Blocks record, determine the amount owed to each merchant and settle with them directly.

For the PoC, Building Blocks used the public Ethereum blockchain. This decision was based on the fact that public chains are self-sustaining through crypto-economic incentives and a public network of validators, and therefore not dependent on WFP or the UN. However, the project team observed that major public chains have low transaction throughput and expensive transaction costs due to the prevalence of the Proof-of-Work (PoW) consensus mechanism, which is based on computational power in order to secure transactions to the public ledger.

Jordan Implementation

Having demonstrated the concept of using a blockchain ledger, and incorporating the learnings from the PoC, in May 2017 Building Blocks initiated a large-scale pilot with 10,000 Syrian refugees in Jordan. The concept was similar to the Pakistan PoC. However, for the Jordan pilot, Building Blocks switched to a private, permissioned blockchain using the Parity Ethereum client with a Proof-of-Authority (PoA) consensus algorithm.

The private PoA network provides Building Blocks with a very high transaction throughput at no cost per transaction. The private network also provides higher assurances for data protection privacy. The main downside of the private network is that it is not self-sustaining. However, the smart contract code is identical between private and public networks. Therefore, when the public networks have adequately addressed the throughput, cost, and privacy issues, Building Blocks can switch by merely copy-pasting its code. Another downside is that a private network is less resilient and tamperproof than public networks due to the fewer nodes. However, with each additional independent node on the blockchain, a private chain becomes increasingly closer to the characteristics of public chains in terms of resilience and immutability.

In contrast to the Pakistan PoC whereby authentication was provided through OTP SMS, in Jordan Building Blocks integrated with the existing iris biometric authentication system enabled by the UN Refugee Agency (UNHCR)[39]. Through Building Blocks, refugees only need to scan their irises at the point-of-sale to receive food assistance. All transactions are recorded on a private blockchain-based infrastructure, used as a registry to calculate the balance of every refugee, as well as the amount of funds that must be disbursed by the WFP to the relevant merchants[40] The advantage of this system is that beneficiaries can access and transfer funds by merely presenting themselves in front of the biometric-based identification system, without the need for a device such as a mobile phone. Indeed, given the precarious situations of Jordan refugees, it is not possible to assume constant internet connectivity or that beneficiaries will always own sufficiently sophisticated phones to handle key management. Facilitating seamless access to critical resources such as food or funds is particularly important for refugees in critical need.

Like Kiva, WFP faces issues with end user smartphone ownership and data connectivity. Hence, Building Blocks also has a guardianship model for custody of keys used to sign transactions. WFP functions as a custodian of the beneficiaries' private keys, which, through the biometric iris authentication, are triggered to sign blockchain transactions related to CBI. Like the Kiva model, the WFP model is also designed to enable self-custody should a user elects to do so when sufficient infrastructure is in place to make this feasible e.g., availability of affordable smartphones with key management capabilities. Eventually, the aim is to provide all the beneficiaries with a new set of public-private key pairs (which they will create and have full control over) and transfer their aid credits to these new wallets.

[38] https://innovation.wfp.org/project/building-blocks

[39] https://www.unhcr.org/en-us/

[40] https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

As noted earlier, WFP's Building Blocks uses the UNHCR's Biometric Identity Management System (BIMS)[41] for authentication. Biometric data in BIMS may include original digital scans (such as the iris photographs), feature sets (i.e., biometric template abstracted from the digital scans), and the reduction of feature sets into a data string that functions as a unique identifier. During the registration process, UNHCR collects an individual's biometrics and associates the biometric data (reduced to a data string) with a unique random identifier in the BIMS database. Individuals are then grouped into family units (as a second level abstraction), each with their unique identifier (a 12 characters string).

Authentication in the context of the UNHCR cash aid system requires a beneficiary to provide an iris scan at the point of sale (POS) for every transaction. The process operates as follows: first, the biometric system at the POS is used to collect the biometric data through an iris scan. The scan is then converted to a template and communicated to the UNHCR and matched against the universe of templates in the BIMS database to retrieve the unique identifier associated with the beneficiary's family unit. This identifier is then sent to the WFP's Building Block system to retrieve the public-private key pairs associated with that identifier. The public key will be used to check if the beneficiary's balance is sufficient to make the transaction. If the balance is sufficient to cover the transaction, the private key will be triggered to sign the transactions on the blockchain, on behalf of the beneficiary. Each communication leg in the entire process is end-to-end encrypted.

For the time being, the system has implemented a series of best practices to mitigate the risk of centralized biometrics, by separating the custody of keys (done by the WFP) from the registry of biometric information linked to the individual's identity (managed by the UNHCR). Hence, from a privacy and security standpoint, WFP's Building Blocks incorporates the necessary safeguards to ensure that the merchant, the bank, the payment processor, the payment network, and other intermediaries are not exposed to information that is not relevant to their function. Indeed, the POS payment processor simply needs to know whether an individual has been enrolled in the system and whether the corresponding account balance is sufficient. It does not need to know the real-world identity, nor even the exact account balance of that individual[42].

Moreover, for reduced security risks, the UNHCR does not store any personal identifying information (such as name, nationality, birthdate, sex, family relations, etc.) together with the biometric data in the BIMS database. All biometrics data is securely stored and completely segregated from any other personal information. Likewise, BIMS does not store the information regarding the beneficiary's private keys—which are only accessible from the WFP's Building Blocks system. The privacy of refugees is therefore protected, since the WFP does not know the actual identity of the individuals whose transactions it processes, and the UNHCR does not have access to the transactions of the individuals it identifies.

Based on the success of the pilot, in January 2018, Building Blocks was scaled to serve all 106,000 Syrian refugees assisted by WFP in the Jordan camps. It is currently the largest implementation of blockchain technology for humanitarian aid in the world. To date, Building Blocks has processed USD 60 million of CBI through 3 million transactions and saved USD 900,000 in banking fees [43].

Next Steps

Everything described in the previous sections could be achieved with traditional databases. However, as blockchain is a relatively new and often theoretical concept in the humanitarian aid world, Building Blocks was a first step in demystifying some aspects of blockchain technology by demonstrating how the technology works at scale in the humanitarian context. As such, the Building Blocks programme was one of the first of its kind.

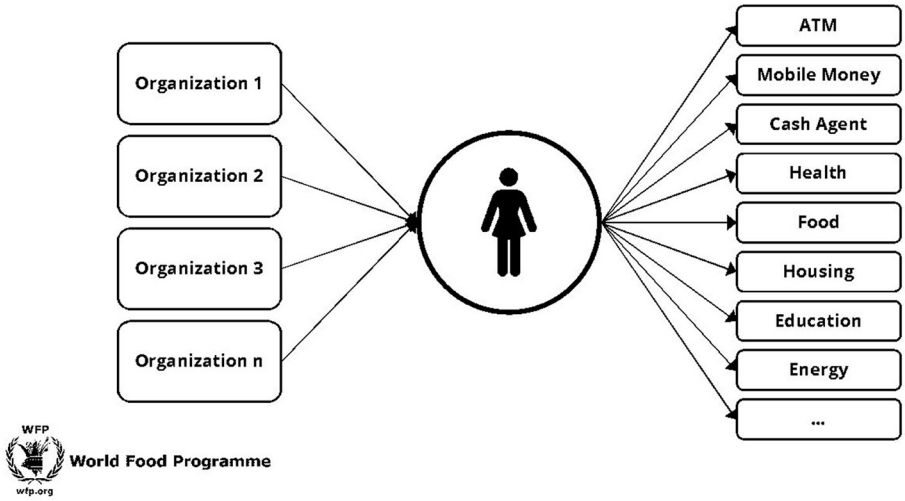
Having achieved that preliminary goal, Building Blocks now aims to take the next step by welcoming new members to the network, in order to facilitate seamless interaction with a variety of different agencies. Non-Governmental Organizations (NGOs) have particular security requirements in humanitarian contexts, and international NGOs are often struggling to reconcile the collection of large swathes of personal data for the issuance of digital identities across multiple agencies. In the Jordan refugee camps, for example, more than 45 organizations assist the same beneficiaries. Yet, the various systems are not meaningfully connected and interoperable. This results in duplication of effort and a somewhat fragmented view of the people served, who need to repeatedly disclose their personal information as they move between agencies.

If these organizations channeled their entitlements to each beneficiary's public key, there would be a unified view of the people served, creating opportunities for optimization and harmonization. Program designs and needs targeting could also become more equitable. Furthermore, all actors could be linked through a single connection to the blockchain, and the various outlets (such as food, cash, health, and education) could be combined. The elegance of the solution is that each organization could maintain its proprietary systems for registration, targeting, and entitlements manage, while still avoiding fragmentation.

[41] https://www.unhcr.org/en-us/protection/basic/550c304c9/biometric-identity-management-system.html

[42] Note that in the Building Blocks system, the balance is printed at the bottom of beneficiary transaction receipts; and this is a feature that is much valued by the beneficiaries. However, because the transaction must be biometrically authorized by the beneficiary, the cashier cannot randomly query beneficiary balances, unless the beneficiary has triggered a transaction.

[43] The savings are achieved by performing all the "accounting" on the blockchain and only using the bank for making payments to merchants. The savings may or may not be replicable in other contexts depending on the operational realities on the ground.



UN Women[44] is the first organization to join the Building Blocks network, and a joint pilot was launched in June 2019 to demonstrate precisely how two or more organizations can collaborate to assist the same people on a shared blockchain network. The model is intended to serve as the blueprint for broader collaboration.

UN Women (and each subsequent new member) operates an independent Building Blocks node, and each node validates and records every transaction on the network. Given that it cannot currently be assumed that all beneficiaries have smartphones and connectivity, Building Blocks has developed an innovative solution that allows each humanitarian provider on Building Blocks to be the custodian for the private keys related to their entitlements, while still maintaining a unified view of the people served on the blockchain. Building Blocks does not store any personally identifiable information on-chain.

Once the concept of entitlements unification on the blockchain is well-demonstrated and accepted, it is an easy step to move to identity attestations. One organization could, for example, attest that the owner of the public key is a nursing mother. Another organization could then search all the public keys for a "nursing mother" attestation and target services to those beneficiaries that fall within their mandate all without needing to know the sensitive personal information of the underlying people.

As the different pieces of a person's identity puzzle are held by different actors, gaining collaboration based on a shared understanding of the technology and its potential for empowering the people served is fundamental in achieving meaningful blockchain-based identity by bringing all the pieces in one place. Building Blocks is taking the approach that the path to a full-fledged blockchain-based identity system is best started with the less sensitive components of identity. For example, insofar as CBI entitlements are determined and distributed in a siloed manner, the related transaction details are also fragmented across various systems and Financial Service Providers (FSP). In such a scenario, if a credit agency wished to analyze the transaction data to assign a credit score for underwriting a loan, they would likely have access to only a portion of all the data. With fewer data points, statistical risk can be determined to a lower degree of accuracy, resulting in beneficiaries being charged a higher interest rate. Instead, if all entitlements were channeled to the unified blockchain wallet for each beneficiary and transactions were authorized from there, the financial transaction histories would also be unified. Based on this, an organization like Kiva, using a zero-knowledge-proof protocol, for example, could establish a credit rating for a beneficiary using all the data, resulting in a more favorable interest rate on the eventual loan. Furthermore, with Building Blocks, the data is portable, so if a Syrian refugee returns home, she could use the data generated in Jordan to get a small business loan in Syria and become self-sustaining again. Otherwise, the data is likely to stay behind with the FSPs in Jordan and would be inaccessible to the refugee back in Syria (or a new destination).

Like the Kiva protocol, Building Blocks also focuses first on the principles of interoperability and minimization, whereby multiple UN agencies can collaborate securely to have a unified view of the same beneficiary, but no personal identifying information is revealed on-chain, thereby protecting the privacy of the identity subject. Also like Kiva, given the conditions of the user population, self-custody is difficult and therefore not a priority at the start. In both cases, a blockchain-based identity infrastructure enables portability of attestations for migrant populations. Over time, additional use cases can be built on top of the identity system, such as using CBI transaction details across multiple UN agencies as data points to predict credit quality.

A question for the future is whether Kiva protocol may be interoperable with Building Blocks. Thus far, interoperability has been focused on actors within the use case e.g., microfinance institutions in Sierra Leone for Kiva and UN agencies for Building Blocks. The users of each identity system may overlap in the future, as these projects scale. For example, a participant (or former participant) in the Building Blocks program may seek microfinance loans in a jurisdiction that uses the Kiva

[44]http://www.unwomen.org/en

protocol. In bootstrapping her credit worthiness, would her CBI transactions and attestations from Building Blocks be recognized by the microfinance institutions participating in the Kiva protocol? Recognition requires both policy agreements off-chain and technical standards interoperability on-chain. Conversely, a participant in the Kiva protocol may become a participant of Building Blocks. Could her attestations from the Kiva protocol be used in Building Blocks for various UN agencies to better serve her needs? Could both of these identity systems allow other trusted parties outside the initial set of permissioned nodes to become attestors and nodes? Robust interoperability, technical standards and policy alignments enable these identity systems to have *composability* and *stackability*, whereby new applications could be built on top of the base identity layer.

FUTURE PERSPECTIVES

As people become more and more mobile, a working identity system that can operate on a global scale has become a precondition for ensuring equal opportunities in the global economy. As developing economies are rebuilding their identity systems anew, it is important to be mindful of the consequences that an improperly designed system might cause. The current approaches of centralized governmental-based identity systems relying on biometrics have serious limitations with regard to both security and privacy (Prabhakar et al., 2003). A more decentralized and self-sovereign identity system using verifiable credentials and access controls is not only more flexible and efficient, but can contribute to securing fundamental human rights, especially in countries with unstable governments and fragile institutions (Lemieux, 2017). Given their critical situation, migrants, refugees and other vulnerable populations might benefit from a system that enables them to selectively disclose some attributes but not others, depending on the use cases.

Dependence of Self-Sovereignty on Technology Infrastructure

A true self-sovereign identity system would require a certain level of infrastructure, primarily high penetration of affordable smartphones that can securely store private keys and reliable connectivity. Practitioners in the field, such as Kiva and the WFP, recognize the realities of their constituents, who are vulnerable populations in low infrastructure environments, many of whom live below the poverty line. Therefore, it is not possible to assume wide availability of the technical infrastructure and sophistication for self-management of private keys.

Another problem with localized key storage—beyond hardware affordability—is the larger issue of key recovery, since, in a self-managed environment, losing one's phone necessarily entails losing one's private key. Hence, perhaps the most important obstacle to achieving full self-sovereignty is the problem of key recovery, combined with the price of hardware.

In light of these issues, there is a consensus that the best practice at the moment is a custody or guardianship model, whereby program administrators like Kiva or WFP can manage keys on behalf of constituents, but constituents always have the ability to opt-out of guardianship should they choose to self-manage.

To address these challenges, some companies are moving into building the first generation of blockchain smartphones. HTC Exodus[45] is one of the first blockchain phones on the market, released in October 2018. The Exodus phone has its own trusted execution environment for secure key management and transaction signing. It deploys a social key recovery mechanism to recover private keys when the phone or passphrases are lost, whereby the user splits the private key among three to five trusted contacts[46]. HTC is issuing a cheaper blockchain phone in Q3 of 2019 called Exodus 1, which will be priced in the $250–300 range[47]. While this would still be prohibitively expensive for many of Kiva's or WFP's constituents, it is a step in the right direction[48].

Digital Money and the Importance of Self-Sovereign Identity

The use of blockchain ledgers for peer-to-peer money transfer has numerous implications in development economics, further highlighting the need for self-sovereign identity solutions. One interesting application of blockchain technology is the digitization of local or complementary currencies as a natively digital cryptocurrency. Community currencies are usually softly pegged to the national currency, and therefore primarily function as a medium of exchange, rather than a store of value or unit of account.

For instance, Grassroots Economics[49] is a non-profit in Kenya that has been implementing a local currency program called Sarafu Credit with rural farmers since 2010. The Sarafu currency is softly pegged to the Kenyan shilling and is accepted by a local community of farmers, traders and schools. In communities where access to cash (Kenyan shillings) is difficult, bank accounts are inaccessible due to lack of identity documents, and mobile money providers like M-Pesa charge exorbitantly high fees, farmers are increasingly relying on local community currencies, as a complementary solution to the national currency (Dissaux and Ruddick, 2017).

Since October 2018, Grassroots Economics has turned Sarafu Credit into a stablecoin transacted on simple feature phones. A stablecoin is a cryptocurrency that is transacted on a blockchain ledger whose value is pegged to a national currency or a reference basket of assets. With the digitization of Sarafu credit as a stablecoin pegged to the Kenyan shilling, the transactions costs are significantly lower than both the paper version of Sarafu, and M-Pesa transactions. For instance, a 101 Kenyan shilling transaction will have a transaction fee of 11 shillings on M-Pesa, but only 2 shillings with Sarafu (the cost of two SMS, a USSD connection and negligible fees to run crypto transactions on an Ethereum side chain).

[45] https://www.htcexodus.com
[46] https://www.wired.com/review/review-htc-exodus/
[47] https://mashable.com/article/htc-exodus-1s-blockchain-phone/
[48] By comparison, the first cell phone from Motorola retailed for $3,995 in 1982. Today, HTC, Samsung and others sell much more powerful smartphones for <$200. See https://www.timetoast.com/timelines/history-of-cellphones-prices
[49] https://www.grassrootseconomics.org/

Most interestingly, transaction information which would otherwise be owned and controlled by M-Pesa, or remain untraceable with paper money, can now be recorded to a blockchain. This data includes statistics on what kinds of goods and services each wallet is spending its funds on, the transaction sizes, and so forth. Such open source transaction data, when tied to a self-sovereign identity system, would provide rich behavioral information for purposes of underwriting microloans, micro-insurance or other humanitarian applications such as needs assessment planning to determine the amount of cash aid to provide to beneficiaries. Traditionally, needs assessment is done through focus groups and surveys. Dynamic data from live transactions would be far more accurate, timely, and insightful in ensuring that beneficiaries receive an adequate amount of cash aid. Furthermore, as described under the Kiva model, if the loans were disbursed and repaid using cryptocurrency, disbursement and repayment claims could be automatically added to the Kiva's identity protocol, thereby strengthening users' credit profile and enhancing the richness of their digital identities.

Grassroots Economics, Sempo (an Australian startup) and the Red Cross are now working together on a new project called Community Inclusion Currencies (CICs), which is a model for channeling cash aid and other sources of philanthropic or private sector cash as reserves that fractionally issue these local currencies. Through a fractional reserve model, cash donations and aid is effectively levered. For example, $100 worth of cash donation may be issued as $120 worth of CICs. If the CICs are circulated within the community at a high velocity, that further amplifies the initial impact of the $100 of cash aid. In order to maintain price stability of the CICs, redemption of CICs for the underlying cash can be gated algorithmically relative to the existing supply of CICs, the issuance and redemption rates of CICs, and the reserve ratio. The CICs would be issued as a stablecoin pegged to the national currency, and ideally the reserve would also be stored as a fiat-pegged stablecoin, with issuance and redemption automated through smart contracts. The CIC model could enable a scalable alternative mechanism to community banks. For example, women's savings and loan groups could deposit their collective savings into a reserve, and whenever members need loans, the smart contract would issue new CICs. Over time, interest and savings rates could be added in order to make various CIC projects economically sustainable. The CIC project was awarded a two year grant from Innovation Norway, an arm of the Norwegian government, to pilot and scale in Kenya and other locations globally[50].

Stablecoins point to a future where money becomes predominantly global and digital, but bankless (Balvers and McDonald, 2017). Until the advent of cryptocurrency, digital money necessarily meant bank-facilitated transactions, with banks or other financial institutions (the gateways to the banking rails) performing KYC and AML checks. Thus, those without identity documents have been left out of the global digital economy (Borio and Disyatat, 2010). As money becomes increasingly global, there may be a concomitant opportunity for the establishment of an equally global and digital identity management system that preserves the privacy of users (Vigna and Casey, 2016), while adhering to compliance of global regulatory regimes for KYC and AML. In particular, a synergy might emerge between digital money and digital identity, mediated through a blockchain-based infrastructure, whereby transaction data can function as attestations that increase the richness of a digital identity profile. This could contribute to better credit underwriting, humanitarian needs assessment, and more accurate (and ultimately more inclusive) risk assessments for KYC/AML compliance.

Identity Insurance as Backstop and Revenue Stream for Identity Providers?

Innovative ideas and new markets around digital identity have yet to be realized. One interesting proposal explores creating an insurance marketplace for consequential damages related to identity claims[51], which could be built on top of a digital identity management system similar to Kiva's architecture. Such a marketplace could provide the "last mile" assurance against identity errors (e.g., bad data coming into the identity system) and provide a market mechanism for evaluating the accurateness, trustworthiness and usefulness of various claims associated with an identity (Tang et al., 2003). This would enable lenders to feel more comfortable underwriting a loan—particularly to an individual with no formal credit history, if the claims associated with that individual's profile were insured for consequential losses toward the cost of the loan. Over time, traction in lending activity would result in new attestations from the lender, thereby increasing trust and lowering insurance premiums for that particular individual.

Identity insurance could also become a new revenue stream for identity providers such as banks and microfinance lenders, who are, in any case, required by law to conduct diligent KYC checks. In such a semi-decentralized identity management systems, banks, and lenders could underwrite the risk associated with issuing an identity credential on the blockchain, thereby helping subsequent lenders de-risk and creates economic incentives for the lenders of "first resort"—(i.e., the lenders willing to lend or issue identity credentials earlier in a borrower's digital history).

Refugees with little to no attestations might be subject to higher risk premiums (because they have no track history) until the refugees acquire more quality attestations so as to make them more trustworthy. Such a model could encourage refugees to engage as much as possible with specific institutions or organizations, in order to collect a positive track record of verifiable credentials, and therefore reduce the insurance premium associated with their identity. In some cases, risk premiums may even be subsidized by agencies like UNHCR or other relevant organizations. Although such an insurance model might ultimately be beneficial to refugees and displaced individuals, who do not have a strong government to guarantee for their identity, it should only be experimented after extensive research has been done to mitigate any potential downside or systemic risks of such an identity insurance, such as introducing

[50] http://news.trust.org/item/20191126123058-xtxvz/

[51] https://identityinsurance.org/

illegal biases, discrimination or arbitrary value judgment into the underlying identity system.

CONCLUSION

Self-sovereign identity is a relatively new area of research, which is only now starting to materialize into real-world applications of new digital identity management systems. This is particularly valuable for applications that have the ability to scale and greatly improve financial and social inclusion of vulnerable populations (Blakstad and Allen, 2018). Yet, it is important to keep in mind that while there are emerging best practice standards and primitives for self-sovereign identity (McMullen et al., 2019), there is no generic identity protocol that solves all use cases. As demonstrated by the Kiva and WFP case studies, identity is inherently use case dependent. Interoperability and standardization will be important for scale, but the success of a particular identity application will depend on how its deployment is tailored to the use cases and local conditions. A successful identity management system will therefore need to be sufficiently flexible to adapt to the inherently malleable nature of human identity.

The development of cryptocurrencies as a new type of open source mobile money, particularly stablecoins, will enable users to benefit from an increased range of economic opportunities brought about by the new financial services built on top of these systems (Thomason et al., 2018). Verifiable credentials issued by trusted actors can function as identity claims. As described above, credentials signed by WFP to specific beneficiaries can serve as alternative credit scores, while organizations like Kiva can provide identity attestations. Likewise, Grassroots Economics, which currently manages the Sarafu program in Kenya, could sign identity claims on behalf of its participants based on Sarafu transactions, which could help its constituents graduate into Kiva's identity protocol and microfinance ecosystem.

Ultimately, Kiva could provide loan capital in a stablecoin to its microfinance partners, via a peer-to-peer transaction that is cheaper and faster compared to international money transfer via correspondent banking (Darlington, 2014). The microfinance lenders could directly disburse loans in a stablecoin denominated in the local currency of the borrower. The microfinance lenders on Kiva's identity protocol would then automatically sign identity claims in regards to disbursements and loan repayments, as such transactions are now verifiable on-chain, thereby reducing potential disputes. Borrowers could subsequently use these loans for their business needs: purchasing inventory for their shop, paying wages to their employees, and so on. As a result, previous and successfully repaid loans would function as identity attestations, further enriching the digital history and credit profile of the borrowers, and creating a virtuous circle for financial inclusion. These new identity business models, such as identity insurance, would likely arise out of this mobile money/identity ecosystem, further enhancing the robustness of the ecosystem as a whole. And while we are still far from having a truly digital, global and self-sovereign identity system, we believe that blockchain technology could be one of the key building blocks to instantiate this vision.

DATA AVAILABILITY STATEMENT

No datasets were generated or analyzed for this study.

AUTHOR'S NOTE

FW is a lawyer and entrepreneur, currently serving as Associate General Counsel at the Maker Foundation, which supports the blockchain project, MakerDAO. She co-founded ixo, a blockchain protocol for tokenizing social impact outcomes as digital assets. She started her career on Wall Street before practicing law in New York and London. She received her law degree from Columbia University and her undergraduate degrees from UC Berkeley. She can be reached at fennie@makerdao.com. PF is a legal scholar, whose work focuses on the legal challenges and opportunities of blockchain technology. She is a permanent researcher at the CNRS, Faculty Associate at the Berkman-Klein Center for Internet & Society at Harvard University, and cofounder of the Coalition for Automated Legal Applications (COALA). She can be reached at pdefilippi@cyber.harvard.edu.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

FUNDING

Open Access fee has been waived by Frontiers.

ACKNOWLEDGMENTS

The authors would like to thank Kevin O'Brien and Aaron Goldsmid of Kiva, Houman Haddad of the World Food Programme and Nick Williams of Sempo for invaluable input and feedback, as well as Georgy Ishmaev for his comments on a preliminary version of the paper.

REFERENCES

Alvarez, R. M., Hall, T. E., and Trechsel, A. H. (2009). Internet voting in comparative perspective: the case of Estonia. *Pol. Sci. Polit.* 42, 497–505. doi: 10.1017/S1049096509090787

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., and Capkun, S. (2013). "Evaluating user privacy in bitcoin," in *International Conference on Financial Cryptography and Data Security* (Berlin; Heidelberg: Springer), 34–51. doi: 10.1007/978-3-642-39884-1_4

Araújo, L. C., Sucupira, L. H., Lizarraga, M. G., Ling, L. L., and Yabu-Uti, J. B. T. (2005). User authentication through typing biometrics features. *IEEE Trans. Signal Process.* 53, 851–855. doi: 10.1109/TSP.2004.839903

Aydar, M., and Ayvaz, S. (2019). Towards a Blockchain based digital identity verification, record attestation and record sharing system. *arXiv preprint arXiv*:1906.09791.

Q17 Baars, D. S. (2016). *Towards self-sovereign identity using blockchain technology* (Master's thesis). University of Twente.

Balvers, R. J., and McDonald, B. (2017). *Designing a Global Digital Currency*. Available online at SSRN: https://ssrn.com/abstract=3049000

Bhargav-Spantzel, A., Squicciarini, A., Bertino, E., Kong, X., and Zhang, W. (2010). Q18 "Biometrics-based identifiers for digital identity management," in *Proceedings of the 9th Symposium on Identity and Trust on the Internet* (ACM), 84–96. doi: 10.1145/1750389.1750401

Q19 Blakstad, S., and Allen, R. (2018). "Leapfrogging banks in emerging markets," in *FinTech Revolution* (Cham: Palgrave Macmillan), 121–132. doi: 10.1007/978-3-319-76014-8_7

Blazewicz, J., Kubiak, W., Morzy, T., and Rusinkiewicz, M. (eds.). (2012). Q18 *Handbook on Data Management in Information Systems*. Springer Science and Business Media.

Borio, C., and Disyatat, P. (2010). Global imbalances and the financial crisis: reassessing the role of international finance. *Asian Econ. Policy Rev.* 5, 198–216. doi: 10.1111/j.1748-3131.2010.01163.x

Burge, T. (1988). Individualism and self-knowledge. *J. Philos.* 85, 649–663. doi: 10.5840/jphil1988851112

Q18 Bygrave, L. A. (2012). *The Data Difficulty in Database Protection*. University of Oslo Faculty of Law Research Paper (2012-18).

Côté, J. E. (1996). Sociological perspectives on identity formation: the culture–identity link and identity capital. *J. Adolescence* 19, 417–428. doi: 10.1006/jado.1996.0040

Campisi, P. (2013). *Security and Privacy in Biometrics, Vol. 24*. London: Springer. doi: 10.1007/978-1-4471-5230-9

Canham, J. (2018). Biometrics: leap of faith or fact of life?. *Biometr. Technol. Today* 2018, 8–10. doi: 10.1016/S0969-4765(18)30024-9

Cap, C. H., and Maibaum, N. (2001). "Digital identity and its implication for Q19 electronic government," in *Towards the E-Society* (Boston, MA: Springer), 803–816. doi: 10.1007/0-306-47009-8_59

Christman, J. (2013). Social practical identities and the strength of obligation. *J. Soc. Philos*. 44, 121–123. doi: 10.1111/josp.12024

Q20 Darlington, J. K. III. (2014). *The future of Bitcoin: mapping the global adoption of world's largest cryptocurrency through benefit analysis.*

Davidson, S., De Filippi, P., and Potts, J. (2016). *Economics of Blockchain*. Available online at SSRN: https://ssrn.com/abstract=2744751

Q21 De Filippi, P. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Rev.* 3. doi: 10.14763/2014.2.286

Q22 Q23 De Filippi, P. (2015). "Translating commons-based peer production values into metrics: toward commons-based cryptocurrencies," in *Handbook of Digital Currency* (Academic Press), 463–483. doi: 10.1016/B978-0-12-802117-0.00023-0

Q16 De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies. *J. Peer Prod.* 7:al-01382006.

Q21 De Filippi, P., and Loveluck, B. (2016). The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. *Internet Policy Rev.* 5. doi: 10.14763/2016.3.427

Q24 De Filippi, P., and Mauro, R. (2014). Ethereum: the decentralised platform that might displace today's institutions. *Internet Policy Rev.* 25.

Q18 De Filippi, P., and Wright, A. (2018). *Blockchain and The Law: The Rule of Code*. Harvard University Press. doi: 10.2307/j.ctv2867sp

Der, U., Jähnichen, S., and Sürmeli, J. (2017). Self-sovereign identity Q16 $-$ opportunities and challenges for the digital revolution. *arXiv preprint arXiv:*1712.01767.

Dissaux, T., and Ruddick, W. (2017). "Challenges of collective organization and institution building around community currencies in Kenyan slums," in *4th International Conference on Social and Complementary Currencies* (Barcelona).

Dunphy, P., and Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* 16, 20–29. doi: 10.1109/MSP.2018.3111247

Duta, N. (2009). A survey of biometric technology based on hand shape. *Pattern Recogn*. 42, 2797–2806. doi: 10.1016/j.patcog.2009.02.007

Eakin, P. J. (1999). *How Our Lives Become Stories: Making Selves*. Cornell Q18 University Press.

El Haddouti, S., and El Kettani, M. D. E. C. (2019). "Analysis of identity management systems using blockchain technology," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (Rabat: IEEE), 1–7. doi: 10.1109/COMMNET.2019.8742375

Q23 Q22 Freund, A. (2018). "Automated, decentralized trust: a path to financial inclusion," in *Handbook of Blockchain, Digital Finance, and Inclusion, Vol. 1* (Academic Press), 431–450. doi: 10.1016/B978-0-12-810441-5.00030-0

Friedman, A., Crowley, P., and West, D. (2011). *Online Identity and Consumer Q17 Trust: Assessing Online Risk*. The Brookings Institution, 11.

Ganapathy, V., Thomas, D., Feder, T., Garcia-Molina, H., and Motwani, R. (2011). Q18 "Distributing data for secure database services," in *Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society* (ACM), 8. doi: 10.1145/1971690.1971698

Garcia, P. (2018). Biometrics on the blockchain. *Biometr. Technol. Today* 2018, 5–7. doi: 10.1016/S0969-4765(18)30067-5

Garrett, B. (2002). *Personal Identity and Self-Consciousness*. Routledge. Q18 doi: 10.4324/9780203015667

Geach, P. (1973). "Ontological relativity and relative identity," in *Logic and Q21 Ontology*, ed. M. K. Munitz (New York, NY: New York University Press).

Gencer, M. (2011). The mobile money movement: catalyst to jump-start emerging Q22 markets. *Innovations* 6, 101–117. doi: 10.1162/INOV_a_00061

Gentry, C., and Boneh, D. (2009). *A Fully Homomorphic Encryption Scheme, Vol. 20, No. 09*. Stanford, CA: Stanford University.

Gerard, D. (2017). Attack of the 50 foot blockchain: bitcoin, blockchain, Ethereum Q20 and smart contracts.

Gleick, P. (2014). *Water, Drought, Climate Change, and Conflict in Syria*. Oakland, CA: Pacific Institute. Available online at: https://journals.ametsoc.org/doi/full/10.1175/WCAS-D-13-00059.1 (accessed July 1, 2014).

Goldreich, O. (1998). *Secure Multi-Party Computation. Preliminary version*, 78. Q25

Guides, T. S. (2019). *How Do Stablecoins Work*. Q20

Hammudoglu, J. S., Sparreboom, J., Rauhamaa, J. I., Faber, J. K., Guerchi, Q22 L. C., Samiotis, I. P., et al. (2017). Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems. *arXiv preprint arXiv:*1706.03744. Q16

Hardjono, T., and Pentland, A. (2019). Verifiable anonymous identities and access control in permissioned blockchains. *arXiv preprint arXiv:*1903.04584. Q16

Hileman, G., and Rauchs, M. (2017). Global cryptocurrency benchmarking study. *SSRN Electron. J.* 33. doi: 10.2139/ssrn.2965436 Q21

Jacobovitz, O. (2016). *Blockchain for Identity Management*. The Lynne and William Q18 Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva Google Scholar, 9.

Jain, A. K., Flynn, P., and Ross, A. A. (Eds.). (2007). *Handbook of Biometrics*. Q18 Springer Science and Business Media. doi: 10.1007/978-0-387-71041-9

Jain, A. K., and Nandakumar, K. (2012). Biometric authentication: system security and user privacy. *IEEE Comp*. 45, 87–92. doi: 10.1109/MC.2012.364

Jain, A. K., Ross, A., and Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video technol.* 14. Q21 doi: 10.1109/TCSVT.2003.818349

Jenkins, B. (2008). *Developing Mobile Money Ecosystems*. Washington, DC: Q22 International Finance Corporation and Harvard Kennedy School.

Jøsang, A., and Pope, S. (2005). "User centric identity management," in *AusCERT Q18 Asia Pacific Information Technology Security Conference*, 77.

Khare, R., and Rifkin, A. (1997). Weaving a web of trust. *World Wide Web J.* 2, 77–112.

Kosta, E. (2013). *Consent in European Data Protection Law*. Martinus Nijhoff Q18 Publishers. doi: 10.1163/9789004232365

Kulkarni, M. H., Yadav, A., Shah, D., Bhandari, P., and Mahapatra, S. (2012). Q16 Unique id management. *Int. J. Comp. Technol. Appl.* 3, 520–524.

Lee, S. (2018). *Explaining Stable Coins, The Holy Grail of Cryptocurrency*. Available Q22 online at: https://www.forbes.com/sites/shermanlee/2018/03/12/explaining-stable-coins-the-holygrail-of-crytpocurrency

Lemieux, V. L. (2017). "In blockchain we trust? Blockchain technology for identity Q18 management and privacy protection," in *Conference for E-Democracy and Open Government*, 57.

Maesa, D. D. F., Mori, P., and Ricci, L. (2017). "Blockchain based access control," in *IFIP International Conference on Distributed Applications and Interoperable Systems* (Cham: Springer), 206–220. doi: 10.1007/978-3-319-59665-5_15

McMullen, G., De Filippi, P., and Choi, C. (2019). *Blockchain Identity Services: Q18 Technical Benchmark of Existing Blockchain-Based Identity Systems*. COALA and BRI Big Idea Whitepaper.

Mordini, E., and Massari, S. (2008). Body, biometrics and identity. *Bioethics* 22, 488–498. doi: 10.1111/j.1467-8519.2008.00700.x

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* 30, 80–86. doi: 10.1016/j.cosrev.2018.10.002

Q18 Muller, B. J. (2010). *Security, Risk and the Biometric State: Governing Borders and Bodies*. Routledge. doi: 10.4324/9780203858042

Q23 Nagar, A., Nandakumar, K., and Jain, A. K. (2010). "Biometric template transformation: a security analysis," in *Media Forensics and Security II, Vol. 7541* (International Society for Optics and Photonics), 75410O. doi: 10.1117/12.839976

Q22 Ngugi, B., Pelowski, M., and Ogembo, J. G. (2010). M-pesa: a case study of the critical early adopters role in the Rapid adoption of mobile money banking in Kenya. *Electron. J. Inform. Syst. Dev. Ctries*. 43, 1–16. doi: 10.1002/j.1681-4835.2010.tb00307.x

Q22 Q18 Nguyen, Q. K. (2016). "Blockchain-a financial technology for future sustainable development," in *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD)* (IEEE), 51–54. doi: 10.1109/GTSD.2016.22

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 2021–2040. doi: 10.1109/JPROC.2003.819611

Q18 Othman, A., and Callahan, J. (2018). "The Horcrux protocol: a method for decentralized biometric-based self-sovereign identity," in *2018 International Joint Conference on Neural Networks (IJCNN)* (IEEE), 1–7. doi: 10.1109/IJCNN.2018.8489316

Prabhakar, S., Pankanti, S., and Jain, A. K. (2003). Biometric recognition: security and privacy concerns. *IEEE Secur. Priv.* 1, 33–42. doi: 10.1109/MSECP.2003.1193209

Proença, H., and Alexandre, L. A. (2010). Iris recognition: analysis of the error rates regarding the accuracy of the segmentation stage. *Image Vision Comput*. 28, 202–206. doi: 10.1016/j.imavis.2009.03.003

Rane, S., Wang, Y., Draper, S. C., and Ishwar, P. (2013). Secure biometrics: concepts, authentication architectures, and challenges. *IEEE Signal Process. Mag.* 30, 51–64. doi: 10.1109/MSP.2013.2261691

Q18 Rannenberg, K., Camenisch, J., and Sabouri, A. (2015). *Attribute-Based Credentials for Trust. Identity in the Information Society*. Springer. doi: 10.1007/978-3-319-14439-9

Q18 Ross, A., and Jain, A. K. (2004). "Multimodal biometrics: an overview," in *2004 12th European Signal Processing Conference* (IEEE), 1221–1224.

Sarkar, S. (2014). The unique identity (UID) project, biometrics and re-imagining governance in India. *Oxf. Dev. Stud*. 42, 516–533. doi: 10.1080/13600818.2014.924493

Schartner, P., and Schaffer, M. (2005). "Unique user-generated digital pseudonyms," in *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security* (Berlin; Heidelberg: Springer), 194–205. doi: 10.1007/11560326_15

Schneier, B. (1999). The uses and abuses of biometrics. *Commun. ACM*. 42, 136–136. doi: 10.1145/310930.310988

Q16 Shrier, D., Wu, W., and Pentland, A. (2016). Blockchain and infrastructure (identity, data security). *Mass. Inst. Technol. Connect. Sci*. 1, 1–19.

Strohminger, N., Knobe, J., and Newman, G. (2017). The true self: a psychological concept distinct from the self. *Perspect. Psychol. Sci*. 12, 551–560. doi: 10.1177/1745691616689495

Suler, J. R. (2002). Identity management in cyberspace. *J. Appl. Psychoanal. Stud*. 4, 455–459. doi: 10.1023/A:1020392231924

Tang, F. F., Thom, M. G., Wang, L. T., Tan, J. C., Chow, W. Y., and Tang, X. (2003). Using insurance to create trust on the internet. *Commun. ACM* 46, 337–344. doi: 10.1145/953460.953519

Q22 Team, M. (2017). *The Dai Stablecoin System*. Available online at: https://makerdao.com/whitepaper/DaiDec17WP.Pdf

Q18 Thomason, J., Ahmad, M., Bronder, P., Hoyt, E., Pocock, S., Bouteloupe, J., et al. (2018). "Blockchain—powering and empowering the poor in developing countries," in *Transforming Climate Finance and Green Investment with Blockchains* (Academic Press), 137–152. doi: 10.1016/B978-0-12-814447-3.00010-0

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). EU general data protection regulation: changes and implications for personal data collecting companies. *Comput. Law Sec. Rev*. 34, 134–153. doi: 10.1016/j.clsr.2017.05.015

Q18 Tobin, A., and Reed, D. (2016). *The Inevitable Rise of Self-Sovereign Identity*. The Sovrin Foundation, 29.

Toth, K., and Subramanium, M. (2003). "The persona concept: a consumer-centered identity model," in *3rd International Workshop on Emerging Applications for Wireless and Mobile Access (MobEA)* (Budapest).

Uludag, U., Ross, A., and Jain, A. (2004). Biometric template selection and update: a case study in fingerprints. *Pattern Recogn*. 37, 1533–1542. doi: 10.1016/j.patcog.2003.11.012

Unar, J. A., Seng, W. C., and Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recogn*. 47, 2673–2688. doi: 10.1016/j.patcog.2014.01.016

Q26 van der Ploeg, I. (2003). "Biometrics and the body as information," in *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, 57–73.

Q17 van Wingerde, M. (2017). *Blockchain-enabled self-sovereign identity* (Doctoral dissertation, Master's thesis). Tilburg University, School of Economics and Management.

Q18 Vigna, P., and Casey, M. J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*. Macmillan.

Q18 Werz, M., and Conley, L. (2012). *Climate Change, Migration, and Conflict in Northwest Africa*. Center for American Progress, 8.

Whitley, E. A., and Hosein, G. (2010). Global identity policies and technology: do we understand the question?. *Global Policy* 1, 209–215. doi: 10.1111/j.1758-5899.2010.00028.x

Wright, A., and De Filippi, P. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Available online at SSRN: https://ssrn.com/abstract=2580664

Q18 Zibran, M. F. (2012). *Biometric Authentication: The Security Issues*. University of Saskatchewan.

Conflict of Interest: FW was employed by the Maker Foundation at the time of writing this article.

Q27 The remaining author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright © 2019 Wang and de Filippi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.