Distributed ledger identification systems in the humanitarian sector

I4A Council

Aiden Slavin

May 2019

sovrin
identity for all

sovrin
identity for all

Abstract

This report examines identification management systems in the humanitarian sector that use distributed ledger technology (DLT). Humanitarian assistance is increasingly managed and delivered remotely via digitized administrative and operational systems that center on “beneficiary management” software to manage the identification of individuals being served. Specifically, this report analyzes systems that use DLT to perform these functions, offering insight into their potential benefits and risks. It assesses arguments for and against the use of DLT-based systems and digs into the implications, for individuals and institutions, of shifting to a distributed paradigm. It also explores several of the most commonly cited use cases for DLT-based identification systems: cash transfer programming, land registration, health services, and identification provision for refugees, stateless individuals, and internally displaced persons (IDPs). It then offers a summary and analysis of two case studies in identification management: IFRC-KRCS Blockchain Open Loop Cash Transfer Pilot Project and WFP Building Blocks. It concludes with a discussion of the advantages and risks common to DLT-based identification management systems. As an appendix, we include a partial inventory of relevant systems providers, describing their technologies and services for identification management.

Foreword

The Identity for All (I4A) Council leads Sovrin Foundation's efforts in developing more inclusive and ethical identification systems. We believe that while the decentralized, privacy-preserving nature of Sovrin is a tremendous step forward for the agency of individuals, that technical architecture alone does not guarantee that it will be accessible or fair to the marginalized and underserved populations most in need of robust identification. Part of our remit is thus to help the broader community understand the distinct needs and opportunities in serving these populations, and facilitate efforts at designing appropriate best practices, standards, and solutions.

In doing so we occasionally support the work of other organizations or individual contributors that are working in this space. We aim to support work that is objective, critical, and empirically grounded, and believe this report fits that description. As with all external contributors, the views expressed herein are those of the author, and may not reflect the views of Sovrin Foundation.

About the author

Aiden Slavin is an independent consultant working at the intersection of the technology and humanitarian sectors. He is Visiting Fellow for Humanitarian Innovation at the Institute of International Humanitarian Affairs at Fordham University, where he co-organizes the Humanitarian Blockchain Summit, and Chief of Stuff at ID2020. His past work includes consultancies with IFRC, PeaceTech Lab at the US Institute of Peace, CNN, and CNN Arabic.

Table of Contents

Executive summary

Decentralized identification systems using distributed ledger technology (DLT) are purported to solve a wide range of challenges in the humanitarian sector[1]. The digitalization of humanitarian aid, driven by use cases like cash transfer programming, is in part responsible for this phenomenon. However, DLTs are complex and still emergent, and—despite the hype—there is significant uncertainty around how to operationalize these systems in the humanitarian context.

This research explores the value that DLT-based identification systems offer organizations seeking improved identification management. In an effort to ground the analysis in the real-world application of DLT, we examine these systems in the context of specific use cases and in contrast to legacy identification management systems. Apart from the case of refugees, stateless persons, and internally displaced persons (IDPs), the distribution of identification to humanitarian beneficiaries is rarely seen as an end in and of itself. Instead, humanitarians understand identification as a way of enhancing the distribution of aid. This report focuses on identification management. However, it also recognizes that, increasingly, systems designed for identification management are being deployed for a variety of uses through integration with a multiplicity of technologies. As such, this report examines identification management in practice to accurately depict the entanglement of identification technologies and processes with disbursement, recording, and other technologies.

Through interviews and case studies of pilot projects, we found a range of perceived advantages of DLT-based systems, which we categorize broadly in two groups: traditional benefits and decentralized benefits.

We categorize some of the oft-cited advantages of DLT-based systems[2] as "traditional benefits" because these outcomes are not unique to distributed ledger-based identification management systems. Some of the most commonly cited traditional benefits were enhanced security, auditability, and cost-effectiveness. While there are many variations and degrees of nuance in these functions, alternative technologies—like encrypted databases for security and partially persistent data structures for immutability—can achieve similar ends in most cases. Neither are data security, program auditability, and cost-effectiveness concerns new or unique to DLT. Each has been a fixture of debates about digital technologies for decades.

The second category, "decentralized benefits," comprises those functions that derive directly from decentralized architectures and processes. Shifting the locus of control from the institution to the individual is foundational to realizing these benefits. This structural change has significant potential benefits, and risks, at both the individual and organizational levels.

---

1 We follow Rauchs in defining DLT as "[a]n umbrella term to designate multi-party systems that operate in an environment with no central operator or authority, despite parties who may be unreliable or malicious" (Rauchs et al., "Distributed Ledger Technology Systems: A Conceptual Framework").

2 We use the terms "distributed ledger based identification management system" and "distributed ledger identification management system" interchangeably throughout to describe identification management systems that make use of distributed ledger technology.

DLT could enable individuals to control their information at a granular level on an ongoing basis by storing verified claims about their identity in a repository known as a "hardware wallet." This hardware wallet would make it possible for individuals to release the minimal viable information to service providers rather than providing a full identity datum. However, shifting the locus of control also shifts responsibility, potentially abrogating some degree of institutional liability. These systems also de facto mandate that individuals be literate (digitally, linguistically, numerically) enough to manage their data. Furthermore, the shift to a distributed paradigm spreads security risk across the network, increasing the number of potential points of failure.

At the organizational level, DLT could enable interoperability throughout the sector by offering access to standardized and verified identity data and program operations across a number of different organizations. Perhaps more importantly, DLT could make intra-operability within organizational programming possible. Rather than registering an individual several times within a single organization—or across several (iNGO, NGO, CBO) organizations—humanitarian organizations could establish trust in third parties to independently verify identity claims, obviating the need to repeatedly register the same beneficiary.

Though theoretically possible, inter- and intra-operability are often more questions of political will than technical feasibility. Even at the technical level, intra-operability poses challenges: attempts to change data recording practices across organizations with radically different information architectures will confront significant barriers. Furthermore, legal limitations (including the development of intellectual property agreements and point-to-point trust frameworks) pose a challenge to implementing any sort of technological change in the humanitarian sector.

Although several systems for DLT-based identification management have been proposed, few have been piloted and none have achieved scale so how DLT-based identification management systems will affect the humanitarian sector remains to be seen. Moreover, the lack of understanding of DLT is not unique to the humanitarian sector. Regulatory bodies, standards organizations, and norms-setting groups are far behind the curve. The existence of pilot programs leveraging DLT-based identification management systems in the humanitarian sector necessitates a careful consideration of their benefits and risks. Recipients of humanitarian aid are often at the height of their vulnerability and the recording of their information poses a serious threat to the security and rights of individuals and groups.

Introduction

Humanitarian assistance is increasingly managed and delivered remotely via digitized administrative and operational systems, which often have center on “beneficiary management” software to manage the identifications of individuals being served[3]. Several factors are driving increased interest and investment in digital identification systems, including the expanding role of cash transfer programs, which carry specific identification requirements, such as fulfillment of KYC/AML criteria[4]; increased demand from donors for improved transparency and auditability; increased demands, and regulations, for privacy and data protection; increased need for operational optimization and reduced waste; an ongoing need for business intelligence and internal reporting; and an increased interest in developing standardized and interoperable systems.

Although beneficiary management systems often support a wide range of operational data and reporting functions, this analysis focuses on the identification management components of these systems. That is, the processes and data related to the registration, verification, authentication, and authorization of individual beneficiaries.

Verification is the initial enrollment of a beneficiary. Typically, humanitarian organizations make use of a breeder document (e.g., a national ID card) from a trust anchor (e.g., a national government) to register beneficiaries and, establish trust in their attested identity. When a beneficiary attempts to access a service, aid organizations authenticate their identity by establishing a correspondence between an identification presented at the point of interaction and an existing record. Once authenticated, the beneficiary is authorized to access a service. An identification management system facilitates each of these three processes (verification, authentication, authorization). Other systems layered on top of identification management systems can perform functions like initiating cash disbursements, and other technologies, like biometry, can be used to enhance any one of the three processes. A biometric, a biological attribute (like a fingerprint) or behavioral trait (like walking gait), can be used to establish uniqueness, facilitating verification and, subsequently, authentication[5]. Notably, an identification management system is any structure or process that facilitates any one (or any multiple) of these three processes, but this report deals specifically with identification management systems that make use of DLT.

While humanitarian organizations use a wide range of identification systems globally, there are a few notable systems at scale. UNHCR's proGres is used in over 70 countries and is in the midst of a transition from a local data store (there are more than 500 databases globally with all data stored in-country) to a centralized cloud architecture. Given UNHCR’s legal mandate to assign refugee status

[3] Duffield, "Challenging environments: Danger, resilience and the aid industry."

[4] That is, know-your-customer and anti-money laundering regulations for due diligence of the identities of people involved in sending and receiving financial payments

[5] Gelb and Metz, Identification Revolution: Can Digital ID Be Harnessed for Development?

and “improve the situation of refugees,”[6] progress is generally considered the gold standard for refugee identification. Other notable systems include WFP's SCOPE, which currently houses the data of over 20 million aid recipients and is being licensed to other NGOs; IOM's Personal Identification and Registration System (PIRS), which holds beneficiary data for each of the organization’s country operations; and World Vision's Last Mile Mobile Solution (LMMS), which is used by more than 20 NGOs across 29 countries, where it houses the data of more than eight million beneficiaries[7]. Beyond the humanitarian sector, various other consortia, such as the Europeans Union’s eIDAS Framework[8] and the Health Sector’s hI7, are taking up identification management with renewed interest[9].

Apart from the case of refugees, stateless persons, and IDPs—the distribution of identification to humanitarian beneficiaries is rarely seen as an end in and of itself. Instead, humanitarians understand identification as a way of enhancing the distribution of aid. While this report deals with identification management, it recognizes that, increasingly, systems designed for identification management are deployed for a variety of uses through integration with a multiplicity of technologies. Accordingly, this report examines identification management in practice to more accurately depict the entanglement of identification technologies and processes with disbursement, recording, and other technologies.

The humanitarian sector is abuzz with conversations on the potential of blockchain technology[10]. While blockchain-based solutions are typically attributed several advantages over traditional approaches, very few DLT projects are beyond pilot stage, and there is little evidence to support these claims.[11] This analysis does not attempt to evaluate any specific claims, but instead looks at a limited set of use cases and explores the potential benefits and risks of DLT-based systems. The goal is to provide a more objective evaluation of where ledger-based identification systems are most likely to provide value in the humanitarian sector. [12]

---

[6] UN General Assembly Resolution 428 (V), 14 December 1950.

[7] Schoemaker, Currion, and Pon, “Identity at the Margins: Identification Systems for Refugees.”

[8] Turner, “Understanding eIDAS.”

[9] FHIR, “About.”

[10] We follow NIST by defining “blockchain” as “immutable digital ledger systems implemented in a distributed fashion” (Yaga, Mell, Roby, and Scarfone, “Blockchain Technology Overview”). See also Ko and Verity, "Blockchain for the Humanitarian Sector: Future Opportunities"; UN Blockchain, “Blockchain for Humanity”; and Brown, “Humanitarian Blockchain: Coding for a Humane, Sustainable World.”

[11] Orlowski, “Blockchain study finds 0.00% success rate and vendors don't call back when asked for evidence.”

[12] One might look to the recently released ID2020 "Technical Requirements" for “Good” Digital Identity Systems for an elaboration of several commonalities among (current and future) identification management systems.

Potential use cases for DLT identification systems

Humanitarian organizations are exploring several use cases of DLT including cash transfer programming, land registration and titling, health services, and identification for refugees, stateless individuals, and internally displaced persons (IDPs). Each use case, explored below, features different requirements for identification management systems, yet there are commonalities, including: low levels of beneficiary literacy (digital, linguistic, numerate); low-connectivity and low-power environments; and populations with limited access to mobile/computing devices. The need for technologies suited to these challenges, along with enhanced informed consent processes and fit-for-purpose guardianship models, is clear and general to all identification management systems in the sector.

CASH TRANSFER PROGRAMMING

The 2006 formation of the Cash Assistance Learning Partnership marked the arrival of cash transfer programming (CTP) as a widely recognized assistance mechanism.[13] Instead of offering in-kind aid through on-the-ground distributions, cash transfers enable humanitarian organizations to disburse resources directly to beneficiaries, often more quickly and with minimal local presence. Many humanitarian organizations prefer cash transfers to in-kind assistance, citing its ability to buoy local economies, give beneficiaries greater agency, and reduce overhead.[14] As CTPs become increasingly prevalent in the aid sector, humanitarian organizations are investigating new technologies to optimize aid distribution. In recent years, this has included using blockchain technologies for financial applications (e.g., using a shared ledger to facilitate the transfer of funds between financial organizations and/or beneficiaries) as well as identification applications (e.g., using a shared ledger to enable the exchange of trusted identification credentials such as identifying numbers, ID cards, and digital certificates).

Traditional approaches

A wide range of organizations are implementing cash transfer programs, with many different operational models (e.g., vouchers, cash-for-hire, electronic money), and consequently many different approaches to verifying, authenticating, and authorizing the disbursement of funds to beneficiaries. Smaller organizations may manage a limited CTP using spreadsheets and paper vouchers, while a larger NGO may partner with a mobile operator and bank to facilitate mobile money payments directly to beneficiaries' devices. While this wide range of approaches makes it hard to generalize, common challenges across cash transfer programs include security, efficiency, auditability, and interoperability.

---

[13] The Cash Learning Partnership, "About Us."

[14] Oxfam International, "Cash Learning Partnership (CaLP)"; Mercy Corps, "Cash Transfer Programming: toolkit."

The operation of cash transfer procedures can be labor-intensive and require a high-touch approach, straining limited resources and increasing the chance of human error. Mercy Corps, for example, advises that, during physical verification, a participant signs and present ID in order to confirm identity at point of interaction.[15] This necessitates a single locus of distribution and delimits the reach of cash transfer programs in both time and space.

Internal and external audits, which often involve the reconciliation of several distinct records, track the successes and failures of CTP. It is not uncommon for third parties, like technology firms and financial service providers, to maintain proprietary records of a CTP. The proliferation of recording not only creates redundancy but can also generate disputes when records differ. Auditors must integrate distinct records in an attempt to produce an authoritative report of organizational accountability to beneficiaries, partners, and donors.

Traditional cash transfer programs also usually lack interoperability. The duplication of data sets and sharing among a variety of organizations—international NGOs, national NGOs, community based organizations (CBOs), financial service providers, third-party technology providers, and others[16] —creates new security concerns and introduces major inefficiencies. Several steps in a cash transfer program, including registration, distribution, post-distribution monitoring, and audit, depend on the integration of the efforts of several distinct actors. For instance, under traditional CTP mechanisms, identity data must be duplicated and shared among a variety of organizations, creating inefficiencies. Similarly, aid organizations often do not coordinate assistance efforts in non-disaster contexts. Instead, most aid organizations operate with few partners to implement programs according to donor pressures. This can create redundant programming and inefficient assistance.

Applications for DLT

Ledger-based identification systems promise to address some of these challenges. Although not unique to blockchain platforms like MultiChain, cryptographic techniques can improve data security, but security needs depend on the type of data being recorded. In distributed ledger identification management systems, the data recorded can be limited to timestamps and linkages to information stored off-chain in traditional databases. Still, the type of data recorded, irrespective of the technology used, depends on the program and providers.

Ledger-based identification systems also enable greater auditability by offering write-only timestamped lists of transactions to humanitarian organizations. Indeed, an append-only list updated in real time and that integrates the actions of all actors presents a major opportunity for audit and

[15] Mercy Corps, "Cash Transfer Programming: toolkit."

[16] Parties in a cash transfer program can include: staff and volunteer members of humanitarian organizations, humanitarian organizations, host government officials, domestic service providers, domestic companies and other parties to transaction, domestic enforcement agencies, domestic metadata collection units, other local or transnational third parties, mobile phone operating systems and app stores, global service providers, foreign government agencies, foreign intelligence agencies, transnational communication service providers, third-party data processing companies in another jurisdiction, adtech firms, and of course, the communities and individuals themselves.

accountability. Rather than comparing the proprietary lists of several actors, auditors could trace the entire life cycle of a CTP through a single authoritative list enabling greater ease of audit.

Similarly, ledger-based identification systems could enhance programmatic efficiency by enabling automatic distribution and recording mechanisms. After identification and verification, organizations could use smart contracts to manage the disbursement of funds and recording automatically, which would decrease organizational burden. Organizations could also layer other mechanisms, like forecast-based financing processes, on top of these procedures to further enhance programmatic efficiency.[17]

Perhaps most significantly, DLTs could enable interoperability both within the operations of a single humanitarian organization and among several. Rather than duplicate data sets several times to integrate the efforts of several actors, DLTs could enable integrated, real-time access to data and program operations. Within a unique CTP, multiple actors could access encrypted data via a list distributed automatically and updated in real time. Although theoretically possible, any such system would likely have to contend with the low-connectivity and low-power environments \. Although some providers, like the IOTA Foundation, are building platforms and protocols optimized for low-connectivity circumstances, this challenge will certainly persist.

Across the humanitarian sector, DLTs could enhance interagency cooperation by making it possible for all relevant actors to trace the delivery of assistance to communities, or even individual beneficiaries. By making it possible for multiple humanitarian organizations to access encrypted data on programs across the sector, humanitarian organizations could coordinate their programs, decreasing redundancy and improving services for beneficiaries. Ledger-based identification systems, therefore, could enhance the security, auditability, and interoperability of cash transfer programs.

IDENTIFICATION FOR REFUGEES, STATELESS PERSONS, AND INTERNALLY DISPLACED PERSONS (IDPS)

For just over a century, international organizations have issued identity documents to refugees and stateless persons in the form of certificates of identity, travel documents, and/or passports.[18] For at least as long, documenting the identity of refugees and stateless persons has been highly contentious.[19]

Since the establishment of the League of Nations High Commission for Refugees and the appointment of Fridjhof Nansen to its highest office, the provision of documentary proof of identity

[17] Red Cross and Red Crescent Climate Centre, “Forecast-based financing.” https://www.climatecentre.org/programmes-engagement/forecast-based-financing

[18] UNHCR, “Nansen—a man of action and vision."

[19] Zetter, "Labelling Refugees: Forming and Transforming a Bureaucratic Identity."

has been an express mandate of intergovernmental agencies.[20] And, throughout the 20th century, the provision of identity documents to refugees and stateless persons remained a priority. Under Articles 27 and 28 of the 1951 Convention Relating to the Status of Refugees, all contracting states are required to issue documentary proof of identity to refugees lawfully residing in their territory, either in the form of identity papers or valid travel documents.[21] As the travaux préparatoires reveal, the articles were inserted to prevent refugees and stateless persons without proof of identity from becoming, as the representative of the International Refugee Organization to the Conference of the Plenipotentiaries put it, "pariah[s] subject to arrest for that reason alone."[22] The commitment to providing identity documentation to refugees that began with the League of Nations and was reinforced by the United Nations continues to be taken up by a host of private, public, and humanitarian organizations.

Although the relationship of refugees, stateless persons, internally displaced persons, and others to identification has changed little over the last century (identification remains capable of conferring both safety and risk on its bearer) the technologies and processes used by issuing agencies are shifting. As part of the gradual transition from analog to digital identification management systems, issuing agencies are piloting new technologies, including advanced biometrics and ledger-based identification management systems, to improve the provision of identification to beneficiaries.

Traditional approaches

Public, private, and humanitarian actors champion identity documentation for refugees, stateless individuals, and internally displaced persons as a path toward financial inclusion, national recognition, and—ultimately—resettlement and integration.[23]

For most, documenting identity occurs at birth. Civil registries provide legal identities to all individuals in a state's territory, often regardless of nationality. Refugees, stateless persons, and IDPs, however, represent a highly contentious group of individuals. Their arrival (or movement, in the case of IDPs) can factionalize nations for a variety of reasons.[24]

In many cases, national registries do not account for these groups. Instead, governments establish parallel registration regimes to monitor internal populations and outfit them with proof of identity. International agencies like the UN High Commissioner for Refugees (UNHCR) or the UN Relief and Works Agency (UNRWA) in the case of Palestine Refugees, support governments to set up refugee

[20] The Nobel Prize, "Nansen International Office for Refugees."

[21] UNHCR, "The 1951 Refugee Convention."

[22] As cited in Goodwin-Gill and McAdam, *The Refugee in International Law*.

[23] ID2020, "Why Digital Identity?"

[24] See, for example, Nawyn, "Refugees in the United States and the Politics of Crisis."

registration systems.[25] Historically, most of these systems have been analog: paper-based and founded on breeder documents like pre-existing birth certificates or ID cards.

Increasingly, however, UNHCR, UNRWA, and a host of other public, private, and humanitarian actors, are leveraging digital technologies to modernize verification, authorization, and authentication.[26]

Aid organizations seek to empower beneficiaries by providing identifications that enable access to jobs, incomes, remittances, online learning, and financial services providers. They also work to reinforce and enhance state capacity by leveraging identification management systems to buttress governance.

Although increasingly sophisticated, the identification management systems aid actors employ remain highly siloed. Efforts to verify, authorize, and authenticate individuals are often duplicated, creating redundancies and, consequently, systemic inefficiencies. Some organizations (see "Case Studies") are piloting distributed ledger-based identification management systems to better service these target populations.

Applications for DLT

Refugees are, by definition, vulnerable to persecution.[27] As noted above, potential danger to its bearer is embedded in every form of identification. Threats to the security of refugees, stateless persons, and IDPs, however, deserve special consideration because their vulnerability often occasions dangerous actions in order to remain invisible to institutions. Refugees' attempts to elude data collection include such extreme measures as the burning of fingertips to prevent biometric registration by the EURODAC system.[28] This is one form of what some term "systems avoidance": precautions taken by vulnerable individuals to escape data collection.[29] The prevalence of systems avoidance underscores the seriousness of the threat that data collection poses to refugees. New forms of identification management can enhance security protocols and mitigate some of these risks. However, many of the risks remain, at their core, a political issue.

Although measures can be taken to secure data, any recording can ultimately compromise individual security. The security afforded (or abrogated) by data management systems depends, ultimately, on what kind of data they record.[30] With increasingly sophisticated re-identification techniques, the line between identity data (information that can be used to verify directly) and programmatic data

---

[25] In the case of Palestine Refugees, see, Bocco, "UNRWA and the Palestinian Refugees: A History within History."

[26] ID2020, "Why Digital Identity?"

[27] (UNHCR), "The 1951 Refugee Convention."

[28] Latonero and Kift, "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control."; Ellerman,; "Undocumented Migrants and Resistance in the Liberal State."

[29] Brayne, "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment."

[30] See, for example, IBM Knowledge Center, "Creating an encrypted database."

(information pertaining to a specific service) has blurred beyond recognition. Re-identification techniques hinge on the ability to indirectly identify an individual by collating seemingly disparate data points. Most pertinent technology providers agree that storing personal data (though, interestingly, not all agree on a definition of the term) on-chain can bring about insurmountable security risks and is therefore inadvisable.[31] However, programmatic data pertaining to refugees, IDPs, and stateless persons can still be used to re-identify, albeit with greater effort. For this reason, any system that stores the data (identity or programmatic) of a vulnerable individual can inadvertently worsen security, even if it makes use of encryption techniques. Recognizing this fact, some technology providers, adhere to the principle of data minimization.

Advanced by the ICRC in its Handbook on Data Protection in Humanitarian Action, the principle of data minimization "seeks to ensure that only the minimum amount of Personal Data are processed to achieve the object and purposes of the Processing."[32] Biometrics startup iRespond, for instance, destroys the biodata it records once it has computed a digital identifier to protect against re-identification by malicious actors. It is possible, therefore, that the best policy for the identification of vulnerable individuals, like refugees, IDPs, and stateless persons, is the policy of minimization, rather than the deployment of further layers of identification.

Distributed ledger identification management systems can, however, offer the unique benefit of enhancing individual control over data. By shifting the locus of control over data from the institution to the individual, distributed ledger identification management systems can increase agency and, eventually, enable interoperability.

Certain distributed ledger-based identification management systems allow users to maintain their own repository of identity claims verified by trusted third parties.[33] An individual can hold those claims independently and only disclose necessary, anonymized information to institutions. This not only enhances individual control over data, it also enables greater interoperability. Rather than registering an individual several times within a single organization(or across several), humanitarian organizations could establish trust in third parties to independently verify identity claims. Once verified, beneficiaries could manage their own relationships with service providers. By so doing, aid organizations could optimize the delivery of services to refugees, stateless individuals, and IDPs while

---

[31] We follow the European Union by defining personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." However, we note that even though this definition does not give granular indication of what constitutes the term, we enlist it nonetheless as a working definition.

[32] International Committee of the Red Cross, "Handbook on Data Protection in Humanitarian Action."

The Handbook on Data Protection in Humanitarian Action advances an extremely wide definition of personal data: â€œany information relating to an identified or identifiable natural person.â€ While useful, given the sophistication of existing re-identification techniques, the definition may be too broad to carry meaning. Furthermore, with the profusion of big data analytics, which often makes use of a seemingly unrelated data points to draw generalizable conclusions, this understanding of the term may prove practically ineffectual.

[33] See, for example, Sovrin Foundation, "A Protocol and Token for Self-Sovereign Identity and Decentralized Trust."

preserving the security of their data. Furthermore, these systems could enable beneficiary control of data through disclosure techniques like zero knowledge proofs.[34]

This approach to interoperability could be scaled to the whole of the humanitarian sector. In turn DLT could enhance inter-agency cooperation by making it possible to trace the delivery of assistance to communities, or even individual beneficiaries, by all relevant actors. This would reduce redundancy while preserving the security of beneficiary data.

However, interoperability is often more a question of political will and legal structures than technical feasibility.[35] Ultimately, the question of interoperability will be answered at the interstices of regulatory frameworks, operational mandates, and technical possibilities.

LAND REGISTRATION AND TITLING

In May 2015 the government of Honduras announced that it would record a land title registry on a blockchain, inciting a frenzy of excitement in the international property rights sector. The hype only increased when, on a retreat at Richard Branson's private Necker Island, the Peruvian economist Hernando de Soto affirmed the game-changing potential of ledger-based identification management systems for land registration.[36]

The Honduran pilot, however, has since stalled due to unforeseen complications: disputes over land ownership on the ground and the lack of a strong public authority to adjudicate claims held technological solutions in abeyance. Despite the organizations piloting DLT-based identification systems for land titling, it is increasingly clear that, without the proper governance structures in place, such schemes face an uphill battle.

Although land titles are not typically understood as part of the humanitarian sector's portfolio, many in the space are beginning to reconceptualize land registration as foundational to the development of community based resilience to disaster.[37] They argue that disputes over land titles can engender violence against minority groups, which often only worsens during crises.[38]

---

[34] See, for example, Fiege, Flat, and Shamir, "Zero-Knowledge Proofs of Identity."

[35] Caribou Digital, "Identity at the margins: Identification systems for refugees."

[36] Shin, "Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury."

[37] In responding to natural disasters, humanitarian organizations have begun to view land titling and registration as an important part of their mandate.

International Federation of the Red Cross and Red Crescent Movements, "Land Rights and Secure Tenure Fundamental to Humanitarian Shelter Operations."

[38] Graglia, Mellon, and Robustelli, "The Nail Finds a Hammer: Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World."

Innovations teams within humanitarian organizations have begun to look to emerging technologies, like ledger-based identification management systems, to augment government and private sector capacities to secure land rights and, in turn, create pathways to economic growth, poverty reduction, food security, and disaster resiliency.

Traditional approaches

Land registration refers to the processes of providing evidence of titles, facilitating transactions, and preventing the unlawful disposal of land.[39] However, because land registration depends on national, and often local, law, it is difficult to generalize. Nonetheless, traditional land registration systems depend on the registration of transacting parties (land owner and land purchaser) at a public institution that possesses the authority to alter land titling and provides a path to recourse for disputes.[40] In many nations, however, systems of land registration are not globally enforced and no clear avenue for recourse exists.[41]

In many cases, therefore, disputes arise and can result in conflict among claimants. This is most severe in nations without strong public authorities to enforce land registration and resolve disputes, which often arise with regard to ownership. Several organizations in the government, private, and humanitarian sectors are attempting to reduce disputes by testing distributed ledger identification systems for the provision of an authoritative source of proof for land registration and titling.

Applications for DLT

Ledger-based identification management systems can complement the activities of public sector authorities to enforce processes of land registration and titling either by digitizing and recording a legal claim on a distributed ledger or by securing digital identities of claimants to a digital ledger.

In the former case, land titles are digitized and recorded on chain. A land owner can access a digital claim on a shared public ledger[42] with a private key. A shared, publicly accessible and verified registry records land titles, enabling individuals to prove ownership. In this case, no digital identity needs to be created for an owner. However, while ledger-based systems can facilitate proof of ownership, they cannot resolve underlying disputes; even if a digital title is secured on a blockchain, competing parties may still dispute ownership of the physical asset. In nations where the enforcement of land titling is weak, distributed ledger data management systems may be ineffective and might even compound foundational problems of governance by making it difficult to alter an incorrect record.

---

[39] Graglia, Mellon, and Robustelli, "The Nail Finds a Hammer: Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World."

[40] Payne, Durand-Lasserve, and Rakodi, "The limits of land titling and home ownership."

[41] Hanstad, “Designing Land Registration Systems for Developing Countries.”

[42] We follow Crosby, Nachiappan, Pattanayak, Verma and Kalyanaraman by defining “public ledger” as any list verified by consensus of a majority of the participants in the system (Pantas and Ting, “BlockChain Technology”).

Some authorities that have successfully applied distributed ledger identification systems to land titling have used an integrated approach. For instance, the Prosoft Alliance in Ukraine has integrated with a blockchain platform to authenticate the identities of transacting parties and provide authoritative timestamping.[43] These features integrate with traditional land titling systems. Another notable integrated approach is Georgia's National Agency of Public Registry, which integrated with the US startup Bitfury to provide identity authentication and security services for standard land titling records.[44]

Many pilots have found success in national landscapes, like Georgia (which ranks ninth in the World Bank's "Doing Business" report in terms of registering property,) where foundational problems of land titling have already been solved, and ledger-based identification management systems are simply layered on top of functional existing processes.[45] In nations where the governance of land titling is less stable, distributed ledger identification management systems may be less effective.

Humanitarian organizations can contribute to enhancing land titling and registration systems by layering privacy-protecting, user-centric distributed ledger identification management systems on top of functioning public sector registration, enforcement, and recourse mechanisms. By so doing, they can help create pathways to economic growth, poverty reduction, food security, and the general resilience of vulnerable communities to disaster.

HEALTH SERVICES

As Dr. Seth Berkley, CEO of GAVI has pointed out, the "child health card" is perhaps the most common form of identification worldwide—in 98% of all countries, children get one as proof of vaccination when they receive their first dose.[46] However, despite its widespread use, the child health card is strictly analog. Moreover, emerging efforts to provide digital identifications to children in vulnerable communities are closely intertwined with attempts to achieve global vaccination.[47]

Traditional approaches

Traditionally, medical records have been collected and maintained on standard databases. Current storage of medical records suffers from a lack of security, user-control, and interoperability. In recent years, several public, private, and humanitarian organizations have begun piloting distributed ledger identification management systems for healthcare to combat these issues.

---

[43] Cadasta Foundation, "Blockchain for Land Administration: Hype or Substance?"

[44] Bitfury, "Bitfury Group Presents Georgia Land-Titling Project at Harvard, United Nations."

[45] World Bank Group, "Doing Business 2018."

[46] Berkley, "Solving a Global Digital Identity Crisis."

[47] ID2020, "Immunization: an entry point for digital identity."

Typically, the collection and maintenance of data within healthcare systems makes use of spreadsheets and other simple data storage tools. While many of these tools feature security protocols, the data collected must often be shared with community based organizations in charge of administering healthcare on the ground, and many of these organizations lack the functionality to maintain security standards.[48]

Because of the complexity of data recording in healthcare systems, many beneficiaries are not granted control of their data, including, for example, the ability to withdraw consent once given.

In recent years, startups have begun piloting mechanisms that enable user-control of data. Some of these, including that of iRespond and Johns Hopkins University in Thailand, make use of distributed ledger identification management systems. Additionally, iRespond, does not store personally identifiable information on chain;, instead it stores a unique number that serves as a pointer to data stored off chain.

Although several actors use the same data collection software, many still collect their own data according to proprietary standards and practices. As a result,, humanitarian organizations and community based organizations focused on healthcare are often forced to duplicate data or perform cumbersome data transfers to coordinate assistance efforts and collaborate. A lack of interoperability plagues the humanitarian health services sector.

Applications for DLT

Some organizations are developing identification management systems for humanitarian healthcare programs that leverage cryptography (i.e., secret code) to secure data. Cryptographic protocols can be used to build security measures into identification management systems by design. Although not unique to distributed ledger-based identification systems, cryptographic techniques add an extra layer of security.

Several public initiatives are experimenting with ledger-based identification management systems for medical research and healthcare. In 2016, Estonia adopted e-governance technologies for digital registries and digital government services. The program included securing over one million public health records on a traditional database.[49] The status of the database, however, was recorded instantaneously on a permissioned blockchain that recorded whenever changes to the databases were logged.

Ledger-based identification systems could enable increased user control, and some actors have called for increased user control over the recording, maintenance, and use of patient records. Startups

[48] Collins, Sadler, Dent, Khara, Guerrero, Myatt, Saboya, and Walsh, "Key Issues in the success of community-based management of severe malnutrition."

[49] e-estonia, "Blockchain and healthcare: the Estonian experience."

like Seattle-based iRespond are developing ledger-based identification management systems leveraging blockchain technology to secure patient records. By building digital identities for beneficiaries, iRespond supports continuity of care; rather than creating a new record for each patient visit, healthcare providers can track patient status without accessing their personal data. By hashing biodata into a 12-digit code, iRespond can store links to patient health records on a blockchain.[50] Personal health data is then stored off chain in secure databases.

Attempts to make healthcare data systems interoperable are not unique to the humanitarian sector. In recent years, a number of healthcare and services providers have formed HL7, a consortium seeking to devise data standards and protocols to enable interoperability among currently disparate healthcare data management and collection tools.[51]

DLTs can also power interoperability among various humanitarian agencies contributing to healthcare efforts. Actors could coordinate efforts without compromising the privacy of beneficiaries by compiling a shared ledger, updated in real time with cryptographic hash functions, whereby a mathematical transformation secures or “encrypts” information, linked to patient records stored and secured off chain.

[50] iRespond, "Projects."

[51] Health Level Seven International, "About HL7."

Case studies

IFRC-KRCS BLOCKCHAIN OPEN LOOP CASH TRANSFER PILOT PROJECT

Overview

In May 2018 the International Federation of the Red Cross and Red Crescent Societies (IFRC) and the Kenya Red Cross Society (KRCS) piloted blockchain technology for cash transfer programming in Isiolo County, Kenya. An answer to calls for drought relief, the pilot disbursed cash through Safaricom M-Pesa, a mobile money network, to over 2,000 households in the Oldinyiro and Sericho wards. The disbursement was recorded in a proprietary data management system and on a permissioned blockchain, that is, a blockchain wherein only select parties have access, configured on MultiChain by third-party technology provider Red Rose.[52]

Roles

The pilot leveraged the Kenyan government as a trust anchor, using its national ID card as first-order proof of identity. Every Kenya national ID features a numeric code unique to the citizen it identifies. Both Safaricom M-Pesa, the financial services provider, and Red Rose, the third-party technology provider, used the code as a digital identifier (i.e., bits and bytes of data describing an individual, institution, or thing). The code served to identify beneficiaries during program registration. Once registered, Red Rose assigned beneficiaries another unique number for identification on the data management system. A hash of the unique beneficiary ID was used to generate a public key, or address, on the blockchain.

IFRC-KRCS disbursed funds to beneficiaries through an electronic funds transfer (EFT) system which integrated the data management platform with Safaricom M-Pesa and, in turn, deposited the funds in the beneficiaries' accounts. A record of disbursement was logged instantaneously on the permissioned blockchain. Red Rose controlled and operated the data on the data management platform. Red Rose also developed and maintained the blockchain. IFRC and KRCS had read access, both having nodes (i.e., computer systems that maintain the blockchain). In total the blockchain had four nodes. The blockchain was developed on MultiChain, a Coin Sciences product developed in 2014 to enable organizations to build their own chains using an off-the-shelf platform.

The data management system contained beneficiary ID number, national ID number, name, location, mobile number, and transaction data. Transaction data included time, amount, and two addresses, that of the sender and that of the beneficiary. The blockchain contained a hash of the beneficiary ID number and transaction data. Data was collected and recorded in accordance with Kenya's minimal requirements for mobile money transfers and the principles contained in the ICRC "Handbook on Data

[52] International Federation of the Red Cross and Red Crescent Societies, "Blockchain Open Loop Cash Transfer Pilot Project."

Protection in Humanitarian Action." IFRC-KRCS also looked to GDPR as an aspirational gold standard for data collection and management.[53]

Technologies

The pilot used biometrics, mobile, data management, application programming interface, and blockchain technologies. IFRC-KRCS indirectly leveraged biometrics through the Kenya National ID Card, which uses fingerprint recognition to verify identity. The pilot used a mobile app provided by the third-party firm to register beneficiaries with their Kenya national ID cards, authorizing them for participation in the program. Beneficiaries used native mobile devices to receive funds via Safaricom M-Pesa. Then a proprietary data management system, configured and maintained by Red Rose, recorded identification and transaction data. An application programming interface provided by Safaricom M-Pesa integrated with the data management platform via an EFT system to enable instantaneous disbursement of funds through the financial services provider (FSP). A blockchain recorded transaction data while an interface built by the third party displayed transactions recorded on the blockchain in real time.

Archetype[54]

The pilot leveraged the Kenyan government as a trust anchor—an authoritative entity for which trust is assumed and not derived,[55]—and one standalone system to facilitate the CTP. Using the Kenya National ID Card as a means of identity proofing, IFRC-KRCS registered beneficiaries. In turn, the third-party technology provider spawned unique digital identifiers to create a standalone identification system. Once registered and authorized for the program on the proprietary identification system, IFRC-KRCS could disburse funds to beneficiaries through Safaricom M-Pesa, which had already verified and authorized users through the Kenya National ID Card.

Business

Red Rose leveraged a data management system to handle registration, disbursement, and recording. It developed a blockchain for the pilot project, indicating an expansion into ledger-based identification systems.

Analysis

IFRC-KRCS used a ledger-based identification system to record transactions for a cash transfer program. Prior to the pilot, IFRC-KRCS had used data management systems provided by Red Rose to manage identification data and transaction data. Data management systems previously used by IFRC-KRCS lacked security, auditability, and interoperability.

---

[53] For more detail on the pilot, see IFRC, "Blockchain Open Loop Cash Transfer Pilot Project."

[54] For more detail on identification archetypes, see World Economic Forum, "A Blueprint for Digital Identity."

[55] FinMark Trust Africa, "Landscaping a digital financial identity for SADC."

Many cash transfer programs use spreadsheets or other logs to collect and manage data. However, spreadsheets lack security layers, making them vulnerable to theft and corruption. The use of spreadsheets for identification management also makes integration with third party systems redundant. Data records often have to be duplicated and shared with third parties to initiate the disbursement and recording of funds. The lack of a single, integrated, authoritative list of transactions also makes auditing a complicated, multi-step process. Thus, a reliance on spreadsheets or other logs can lead to problems of interoperability.

The ledger-based identification system used in the pilot improved the auditability of the pilot project. Encryption measures native to MultiChain secured identification data on a blockchain while a write-only timestamped list of transactions enabled greater ease of audit for IFRC-KRCS.

Although the ledger-based identification system improved the cash transfer program, similar functionality could have been achieved with an encrypted database for security purposes or a partially persistent data structure for the creation of a write-only timestamped list. In the future, however, IFRC-KRCS could achieve greater interoperability through the use of a distributed ledger. By up-scaling relying parties into operators with fully functioning maintenance nodes on a permissioned blockchain, IFRC-KRCS could achieve greater interoperability within the Red Cross Red Crescent Movement. Encrypted data could then be shared among nodes on a distributed ledger, enabling greater integration of programming. Eventually, through a utility for digital identity management, humanitarian organizations could improve interoperability across organizations, reducing redundant programming and improving the distribution of aid.

WFP BUILDING BLOCKS

Overview

In December 2017, the World Food Programme began piloting blockchain technology for cash transfer programming in the Za'atari and Azraq refugee camps in Jordan. A collaboration between WFP, UNHCR, and private sector firms including IrisGuard, Parity Technologies, and Baltic Data Science, the pilot project initially registered 10,000 Syrian refugees with unique digital identifications that allowed them to purchase goods from local merchants by scanning their irises. A permissioned blockchain built by private-sector partners on an Ethereum fork recorded transactions, facilitating remuneration, recording, and audit. The pilot aimed to reach 500,000 refugees in Jordan by end of 2018.[56]

[56] For more information on Building Blocks, see World Food Programme, "Building Blocks."

WFP also participated in a meet-up which detailed some aspects of the pilot: https://www.meetup.com/munichblockchain/events/237345574/

Roles

Building Blocks leveraged a proprietary UNHCR identification management database as a trust anchor. The UNHCR database holds the personal data of refugees, including name, location, transaction data, and a unique ID number corresponding to an iris scan held in the IrisGuard EyeBank. The EyeBank is a repository of biometric data operated by IrisGuard but controlled by the UNHCR, which has read and write access. It was established in 2016 under the Common Cash Facility (CCF), a public-private partnership between UNHCR; the Cairo Amman Bank, a financial services provider; and IrisGuard, a biometrics technology firm. Under the CCF, IrisGuard installed iris scanners in registration centers throughout Jordan to enhance verification processes for refugees.[57] Now, upon entering Jordan, refugees have their identity proofed and verified by UNHCR with iris scanners at registration centers.

Subsequent programs have used the iris scans to authenticate and authorize refugees for access to services. In the case of Building Blocks, refugees access cash assistance in the form of food vouchers at participating supermarkets by scanning their irises at devices installed at point of sale. When a beneficiary transacts, the iris scanner connects via a virtual private network to the EyeBank and, in turn, the UNHCR identification management database to authenticate identity and authorize the transaction. While UNHCR functions as the trust anchor, operating the foundational identification management system, IrisGuard maintains the identity authorization database, or EyeBank.[58] The UNHCR identification management database was constructed in-house by the Division of Information Systems and Telecommunications to cohere with proprietary Standard Operating Procedures (SOPs).

WFP leverages the UNHCR identification management database and IrisGuard EyeBank to facilitate the cash transfer program. Because beneficiaries scan their irises and purchase an item using digital food vouchers deposited into their account by WFP, the transaction is recorded instantaneously on a permissioned blockchain. All beneficiary transactions are recorded on a permissioned blockchain built and maintained by private sector partners including Parity Technologies and Baltic Data Science. WFP, Parity Technologies, and Baltic Data Science function as relying parties, making use of the underlying identity management database of the UNHCR and authentication services of IrisGuard. The permissioned blockchain was built in accordance with the principle of data minimization, whereby WFP and its technology providers gathered the minimal necessary data on beneficiaries.

Technologies

Building Blocks uses data management platform, iris biometrics, local and virtual private networks, blockchain, and electronic funds transfer technology. A UNHCR data management platform records the personally identifiable information of refugees including name, location, transaction data, and a unique case ID number corresponding to an iris scan held in the IrisGuard eyebank. Building Blocks

[57] UNHCR, "Common Cash Facility."

[58] Ethereum Foundation, "Devcon3 Day 4 Stream—Morning."

makes use of iris recognition to verify identity, using IrisGuard scanners to authorize transactions at point of sale. TheEyeBank database, hosted on a local area network and maintained by IrisGuard, holds the iris scans of beneficiaries. The EyeCloud host is connected by a virtual private network to a remote database that the UNHCR database calls to match a given ID number with a unique iris scan to authenticate the identity of a refugee. Once authenticated, refugees can access a variety of services, including digital food vouchers that allow beneficiaries to purchase food from certain merchants. Such transactions are recorded using the unique beneficiary identifier and a unique merchant identifier. A blockchain records the sale as a withdrawal from the beneficiary's account and a deposit to the merchant. Using the blockchain as a record of transactions, the WFP reimburses merchants at end of month via an EFT system that obviates the need for local financial services provision.

Private sector partners, including Parity Technologies and Baltic Data Science, an affiliate of Datarella, built the blockchain on top of an ethereum fork in five months. Building Blocks runs on a private permissioned blockchain using the Parity Ethereum client. It makes use of a proof-of-authority consensus algorithm. The blockchain runs on a single node, operated by the technology providers but controlled by WFP. To pilot test interoperability, WFP ran four redundant nodes in the hope that, in future, the Building Blocks blockchain could scale into an interoperable identification management system.[59]

Archetype

Building Blocks constitutes a federated trust network wherein a number of domains have established trust among themselves. The UNHCR identification management database and the IrisGuard EyeBank both held digital identifiers for program beneficiaries. By establishing trust and technical correspondence between two identification systems through the unique case ID number, Building Blocks integrated multiple trust networks into a single cash transfer program and recorded their activities on a permissioned blockchain.

Business

IrisGuard was incorporated in 2001 to provide biometric authorization and verification services for the public, private, and humanitarian sectors. Building Blocks represents its first integration with a ledger-based identification system. The pilot is also the first use of ledger-based identification systems by WFP for identification management, indicating an expansion by both WFP and IrisGuard into distributed ledger identification management systems.

The private sector partners Parity Technologies and Baltic Data Science leveraged their experience in providing services to allow Building Blocks to expand into the use of ledger-based identification management systems for the transfer of cash. Baltic Data Science continues to service Building

[59] Gerard, "The World Food Programme's much-publicised 'blockchain' has one participant—"i.e., it's a database."

Blocks, maintaining the blockchain and assisting with its expansion.[60] For its part, Baltic Data Science's affiliate, Datarella, is developing RAAY, an operating system for banking "inspired by designing, building and deploying the blockchain-based accounting and payment system Building Blocks."[61]

Analysis

Building Blocks uses a ledger-based identification management system to record transactions for a cash transfer program. Prior to Building Blocks, WFP used a beneficiary data management platform to manage cash transfer programs. Previous data management systems used by WFP suffered from high transaction costs as well as a lack of security and interoperability.

Building Blocks lowered transaction costs and heightened security. However, these ends could have both been achieved through traditional technologies. A ledger-based identification management system enabled Building Blocks to lower transaction costs. A write-only timestamped list of transactions recorded on the blockchain enabled an easier, direct remuneration process for WFP. Rather than reimburse merchants through local financial service providers, WFP used international wire transfer via an electronic funds transfer system from global bank accounts to remunerate merchants directly. This reportedly reduced transaction costs by over 98%.[62] Datarella, an affiliate of private sector technology provider Baltic Data Science, pegs saving costs for WFP at $3.5 million annually.[63]

Although the ledger-based identification systems improved the cash transfer program, similar functionality could have been achieved with enterprise technologies. Indeed, as initial WFP program manager Houman Haddad has noted, "what we are doing now could be done on a traditional IT system."[64]

The cost savings achieved through disintermediating local financial services providers via blockchain technology could have been achieved through the use of a partially persistent data structure.[65] Such a database can store transaction data in real time as an append-only list, allowing WFP to reimburse merchants directly just as the blockchain did. Similarly, the enhanced security yielded by WFP's deployment of blockchain technology could have been accomplished through a database with an encryption layer.

---

[60] Baltic Data Science, "Data Science and Blockchain as a Service."

[61] Datarella, "Building the Industrial Blockchain."

[62] World Food Programme, "Building Blocks: The Future of Cash Disbursements at the World Food Program."

[63] Datarella, "Building the Industrial Blockchain."

[64] See the comments section in Gerard, "The World Food Programme's much-publicised 'blockchain' has one participant—i.e., it's a database."

[65] See, for example, Driscoll, Sarnak, Sleator, and Tarjan, "Making Data Structures Persistent."

Still, the use of DLT could benefit Building Blocks by enabling interoperability. By up-scaling relying parties into operators with fully functioning maintenance nodes, and adding further nodes to incorporate more partners, Building Blocks could broaden its reach. Indeed, it could eventually serve as the identification management backbone across the UN and other humanitarian organizations. The aforementioned pilot of four redundant nodes evinces an interest in building an interoperable identification management system.

Conclusions

This report has offered an analysis of distributed ledger-based identification management systems. The summary of use cases presents several of the most talked-about potential applications including cash transfer programming, land registration and titling, health services, and identification provision for refugees, stateless individuals, and internally displaced persons. Two case studies explore identification management systems in action. A landscape of technology providers (see Appendix) details several of the firms offering products and services in the field. This conclusion attempts to summarize some of the opportunities and challenges presented by distributed ledger-based identification management systems.

Our research revealed that while many commentators focus on outcomes such as security, auditability, and cost-effectiveness (none of which are necessarily unique to ledger-based identification management systems) ledger-based identification management systems can provide distinct benefits in the humanitarian sector.

The potential for distributed ledger-based identification management systems to alter information management begins with the individual. Some distributed ledger-based identification management systems allow users to maintain control of their identity data: an individual stores claims about their identity in a "hardware wallet" (a digital repository) which can then be verified by trusted third parties and used to facilitate authentication.[66] Rather than repeatedly re-verify individuals, these processes enable individuals to hold verified claims and release them on their own terms. This shift of the locus of control raises a number of benefits and risks at the individual and institutional levels.

At the individual level, ledger-based identification management systems have the potential to enable users to control their information at a granular level on an ongoing basis. However, this also raises a number of risks. By attempting to shift the locus of control from institutions to individuals, DLTs could also shift liability. Regulators have only just begun to reckon with questions of liability in systems that use DLT. The transfer of control, whether de jure or de facto, could abdicate institutional responsibility to a certain extent. Accordingly, such systems burden individuals with the responsibility of control—not every individual, for example, will be able to make informed decisions about the implications of sharing their data with different types of organizations. DLT-based identification management systems also presume a base level of digital, linguistic, and numerical literacy that may not be widespread in humanitarian and development contexts.

By shifting the locus of control of data away from the institution and towards the individual, distributed ledger identification management systems also create benefits and risks at the institutional level. Ledger-based identification management systems could enable greater interoperability and, perhaps just as important to the humanitarian sector, intra-operability, within

[66] Gisolfi, "Self-sovereign identity: Unraveling the terminology."

Though not common to all distributed ledger identification management systems, this mechanism is evident in protocols like that reviewed in Sovrin Foundation, "A Protocol and Token for Self-Sovereign Identity and Decentralized Trust."

the organization. Rather than registering an individual several times within a single organization, or across several different organizations, humanitarian organizations could rely on the credentials and data that each beneficiary carries in their digital wallet. By so doing, aid organizations could optimize the delivery of services to individuals while preserving user-control of data. Similarly, rather than duplicate data sets to integrate the efforts of several actors, DLTs could enable integrated, real-time access to data and program operations. Actors could even draw general insights from aggregate data.

This approach to inter- and intra-operability could be scaled to the whole of the humanitarian sector. DLT could enhance inter-agency cooperation by making it possible for individuals to manage their own relationship with each humanitarian organization through a common exchange format. This would obviate the need for repeated registration by different organizations in different formats and thus reduce both overhead and redundancy while preserving user-control of data.

However, interoperability is often more a question of political will than technical possibility. Humanitarian and development organizations have a vested interest in preserving unique control over their programmatic data. The same can be said for the identity data of beneficiaries. Ultimately, for interoperability to be realized, humanitarian organizations will have to gather political will and align with regulatory frameworks. Only then can technology become effectual.

Likewise, though hypothetically possible, intra-operability poses both political and technical challenges: community-based organizations are often run independent of the iNGOs and NGOs that contracted them. Changing data recording practices at the CBO-level poses significant organizational problems. Technical capability varies widely across iNGOs, NGOs, and CBOs. Efforts to establish any shared data management practices must surmount a technically uneven landscape of providers.

Furthermore, legal limitations impede the implementation of any sort of technological change in the humanitarian sector. The dearth of developers and architects within humanitarian organizations necessitates an engagement with private sector technology firms to build DLT-based identification management systems. Early pilots have revealed divergent understandings of intellectual property agreements between the humanitarian and technology sectors. Establishing shared-value agreements will be challenging in a competitive, monied field as will, developing point-to-point trust agreements within the sector.

While technical architectures differ, many distributed ledger based identification management systems share a goal: to shift the locus of information control from the institution to the individual. These systems, by virtue of their technologies and procedures, have the potential to fundamentally alter the way that individuals interact with institutions and, ultimately, with each other. It is as yet unclear, however, exactly how (or if) this aim might be realized. Individuals could, for instance, maintain control over data themselves or through service providers. Regardless of the architecture chosen, distributed ledger-based identification management systems could occassion significant change in the humanitarian sector and beyond.

A lack of understanding of DLT systems is not unique to the humanitarian sector. Fit-for-purpose regulations addressing issues of data privacy and digital rights are only just emerging, and it remains unclear how much of it will apply to DLT-based systems. Adequate standards for identification management do not yet exist, and functional norms addressing topics like informed consent, data minimization, and the like, have yet to permeate the sector.

Questions of data security resonate universally, but the information of communities at the height of their vulnerability deserves special attention. Recently, vulnerable individuals have taken extreme measures to avoid identification and minimize the risk of leakage, what some have termed systems avoidance.[67] Its prevalence suggests the seriousness of the threat posed to refugees by the recording of data. New forms of identification management can enhance security protocols to mitigate some of these risks, but many of them remain political issues. In the case of vulnerable communities, enhanced security of data and digital rights are imperative, but without careful consideration and appropriate action, DLT-based identification management systems could create more problems than they solve.[68]

[67] Brayne, “Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment.”

[68] UNHCR, "What is a refugee?"

Appendix A: Distributed Ledger-Based Identification Systems Providers Landscape[69]

Name: AID: Tech
Proprietary/Open: Proprietary
Standards:
Year Founded: 2016
HQ: Ireland
Description: AID:Tech attempts to deliver digital entitlements using a blockchain backend to power its "Transparency Engine" and "TraceDonate." Using the "Transparency Engine," aid organizations can disburse remittances, welfare, aid, healthcare entitlements, and donations to beneficiaries while tracking them in real time via mobile notifications. AID: Tech enables organizations to record the development of programs in real time by providing beneficiaries with a digital identity and recording disbursement of entitlements on a permissioned blockchain,. "TraceDonate" powers peer-to-peer donations recorded on a permissioned blockchain. Its use cases thus far include international remittance, aid, and healthcare entitlements. [70]

Name: Baltic Data Science
Proprietary/Open: Proprietary
Standards:
Year Founded: 2016
HQ: Poland
Description: An affiliate of Datarella, Baltic Data Science offers blockchain as a service for a wide variety of use cases. Baltic Data Science offered technical support for Datarella and the World Food Programme's Building Blocks pilot.[71]

Name: BanQu
Proprietary/Open: Proprietary
Standards:
Year Founded: 2015
HQ: US
Description: BanQu offers blockchain as a service for the humanitarian and development sectors. BanQu focuses on supply chain traceability and transparency. It tracks the movement of goods with geolocation tags from producer to buyer to retailer and on to consumers. BanQu records the movement of goods on an immutable, decentralized ledger. In the process, BanQu provides digital identity to users on a custom app. Over time, user profiles accrue transaction histories along with connections to families, friends, small businesses, and NGOs, enabling them to build a credit history and eventually gain access to financial services providers.[72]

---

[69] This information was gathered through a desk study and records readily available covering key data points. Where no information could be readily found none is provided.

[70] AID: Tech, "What we do."

[71] Baltic Data Science, "Data Science and Blockchain As A Service."

[72] BanQu, "Our Platform."

Name: Cambridge Blockchain
Proprietary/Open: Proprietary
Standards:
Year Founded: 2015
HQ: US
Description: Cambridge Blockchain maintains an identity ecosystem that links service providers, regulators, and trusted parties to identity owners via attestations, or identity claims. Identity credentials are issued by trusted parties and enable identity owners to engage in transactions with service providers. Credentials are held in a private, permissioned blockchain maintained by Cambridge Blockchain. Regulators have read-only access.[73]

Name: Civic
Proprietary/Open: Proprietary
Standards:
Year Founded: 2016
HQ: US
Description: Civic offers a decentralized architecture for digital identity. Using the Civic app, identity owners are encouraged to upload their credentials via a private sign-up and secure private login. These credentials are created by the identity owner, encrypted, and stored on a wallet on their mobile device maintained by a third-party provider. On a public blockchain, Civic displays identifiers for authenticating authorities, hashed identity data. Using a flag or kitemark, Civic indicates that user identity credentials are still valid. By using a third party to store, maintain, and authenticate identity owner data, Civic abrogates liability.[74]

Name: Datarella
Proprietary/Open: Proprietary
Standards: OAuth
Year Founded: 2011
HQ: Germany
Description: Datarella offers enterprise blockchain platforms for the public, private, and humanitarian sectors. Its blockchain-based accounting system was used for the World Food Programme's Building Blocks pilot (discussed in case studies). Its current work includes RAAY, an enterprise blockchain for the financial industry.[75]

[73] Jacobovitz, "Blockchain for Identity Management."

[74] Civic, "Whitepaper."

[75] Datarella, "Building the Industrial Blockchain."

Name: EverID/ Everest
Proprietary/Open: Proprietary
Standards:
Year Founded: 2012
HQ: US
Description: EverID seeks to increase financial inclusions with a three-pronged offering. EverID is a digital identity platform that leverages biometrics to verify identity. It integrates with EverWallet, a multi-currency digital wallet capable of storing documents. Leveraging EverID and EverWallet, users can engage in peer to peer and external transactions on EverChain, a blockchain-based transfer system. With EverID, users upload legacy identity documents and third parties attest to their veracity via electronic signatures.[76]

Name: Evernym
Proprietary/Open: Open
Standards: Sovrin
Year Founded: 2013
HQ: US
Description: An enterprise partner for the Sovrin identity ecosystem, Evernym offers several apps that layer on top of the Sovrin framework. Evernym serves as a trust anchor within the Sovrin framework, creating identities for individuals and organizations. With Evernym, issuers—trusted, appointed institutions—can host and manage Sovrin nodes. Identity owners can exchange data with issuers and peer to peer using the Evernym messaging stack while preserving privacy and security. Evernym also integrates an API suite and GUI tools for the issuance and verification of digital identity credentials. Evernym also makes integration possible, powering interoperability with a variety of distributed ledgers.[77]

Name: hu-manity.co
Proprietary/Open: Open
Standards: OAuth
Year Founded: 2018
HQ: US
Description: hu-manity.co proposes an addition to the classic thirty human rights enshrined in the Universal Declaration of Human Rights and its addenda: the right to "legal ownership of [...] human data as property." With its proprietary smart contract infrastructure, hu-manity.co enables users to control their identity data as if it were their private property. Hu-manity.co products are built on an ethereum fork but can integrate with other chains. They are accessible via the #My31 app, which powers user-control over identity data.[78]

[76] Everest, "Whitepaper."

[77] Sovrin Board of Trustees, "Sovrin Provisional Trust Framework."

[78] Hu-manity.co, "About."

Name: iRespond
Proprietary/Open:
Standards: BOPS
Year Founded: 2011
HQ: US
Description: iRespond is a biometrics provider that integrates with the Sovrin Foundation to offer digital identity to users. iRespond makes use of a blockchain to store links to iris scan biometric data, housed in proprietary servers. iRespond does not store personally identifiable information but instead a 12-digit string of randomly generated numbers which correspond to a unique template and becomes a private key recorded on the iRespond blockchain. It is GDPR-compliant by design.[79]

Name: ObjectTech
Proprietary/Open: Proprietary
Standards: ISO
Year Founded: 2016
HQ: UK
Description: A product of the Dubai Future Accelerators program, ObjectTech forms part of the emirate's commitment to stay 10 years ahead of global public services offerings. ObjectTech makes use of LIDAR-backed facial recognition biometrics to record a three dimensional scan of a face, which is verified against an image on their digital passport. The biometric border system records a digital passport for travelers that is then used to authenticate against the biometrics recorded at the gate. ObjectTech records the identity data contained on the digitized passport on a blockchain. The blockchain, ObjectTech claims, enables full user control, or self-sovereignty, over identity data.[80]

Name: Red Rose
Proprietary/Open: Proprietary
Standards:
Year Founded:
HQ: Ireland
Description: Red Rose integrates software and hardware to facilitate humanitarian assistance. With ONEplatform humanitarian organizations can perform enrollment, disbursement, monitoring, post-distribution monitoring, and evaluation on a single interface. With ONEapp volunteers can register beneficiaries using Android devices, and ONEcard enables beneficiary transactions. A suite of hardware—including bluetooth printers, barcode scanners, ONEcard printers, ID scanners, fingerprint and iris scanners—optimize humanitarian assistance programs.[81]

[79] iRespond, "Our Solution."

[80] ObjectTech, "Identity Reimagined."

[81] Red Rose, "About."

Name: ShoCard
Proprietary/Open: Proprietary
Standards: OAuth
Year Founded: 2015
HQ: US
Description: ShoCard enables individuals and organizations to establish digital identities either through its proprietary app or via existing apps using the ShoCard software development kit. Users create a ShoCard ID by downloading the app, uploading a picture of a valid breeder document (government ID), and confirming the details that the app reads from the document. Once uploaded, the user creates a passcode. ShoCard then encrypts the data and saves it on the identity owner's phone. The ShoCard app then hashes the identity data and records it on a blockchain. The identity owner controls what identity data they release to third parties. They can initiate a transaction by verifying their identity through ShoCard. All transactions are recorded on the ShoCard blockchain.[82]

Name: Sovrin Foundation
Proprietary/Open: Open
Standards: Sovrin Foundation
Year Founded: 2016
HQ: US
Description: A private-sector not-for-profit organization, Sovrin aims to be the world's first global utility for self-sovereign identity. The Sovrin stack is composed of a ledger, agents, and clients. The Sovrin distributed ledger, which holds identity records, is maintained by trust anchors and governed by the Sovrin Foundation. Sovrin agents are network services that enable users to engage in identity and data management transactions while preserving user-privacy and control. With Sovrin clients, identity owners can communicate via local devices including smartphones and laptops with Sovrin agents and the Sovrin ledger. Using a Sovrin app, an identity owner can present a claim that has been conferred on them by an issuer to an inspector for authentication. The identifier registry records both the allocation and presentation of claims. Using a variety of encryption measures, Sovrin enables identity owners to perform transactions involving identity data while maintaining privacy.[83]

[82] ShoCard, "Travel Identity of the Future."

[83] Sovrin Foundation, "A Protocol and Token for Self-Sovereign Identity and Decentralized Trust."

Name: Tierion
Proprietary/Open: Open
Standards:
Year Founded: 2015
HQ: US
Description: A "proof engine," Tierion offers blockchain as a service for businesses interested in a variety of use cases. Using permissioned blockchains, businesses can integrate Tierion to maintain a timestamped history of business data including processes and documents. Tierion also enables users to verify credentials, such as education and awards, through a distributed ledger. By recording anonymized credentials on a shared log, Tierion allows users to attest and verify certain identity attributes.[84]

Name: TYKN
Proprietary/Open: Open
Standards:
Year Founded: 2014
HQ: Netherlands
Description: TYKN will offer a distributed identification system for humanitarian aid built on the Sovrin stack. The service will be open source and integrate with a blockchain as a service platform to bring tailor-made tools to NGOs and governments seeking to expand or inaugurate digital identity programs.[85]

Name: uPort
Proprietary/Open: Open
Standards:
Year Founded: 2016
HQ: US
Description: A ConsenSys Formation, uPort is building an open identity system for the decentralized web that integrates a digital wallet, authentication protocols, a mobile software development kit, and a platform for identity data, or credentials. uPort seeks to give ownership of identity to users by enabling them to register their own identity on an ethereum fork and send and request credentials from identity data issuers which are in turn authenticated via a digital signature. uPort's mobile app enables users to manage their own private keys and identity data and connect with platforms to issue relevant identity facts via a zero knowledge proof.[86]

[84] Vaughan, Bukowski, and Rempe, "A Global Platform for Verifiable Data."

[85] Tykn, "About."

[86] Lundkvist, Heck, Torstensson, Mitton, and Sena, "UPORT: A Platform for Self-Sovereign Identity."

Bibliography

AID: Tech. "What we do," https://aid.technology/what-we-do/

Accenture. "UNHCR: Identity Management System Uses Biometrics to Better Serve Refugees." https://www.accenture.com/us-en/success-unhcr-innovative-identity-management-system

Baltic Data Science. "Data Science and Blockchain As A Service." http://balticdatascience.com/

BanQu. "Our Platform.," https://banqu.co/the-tech/

Berkley, Seth. "Solving a Global Digital Identity Crisis." MIT Technology Review, 2017. https://www.technologyreview.com/s/604294/solving-a-global-digital-identity-crisis/

Bitfury. "Bitfury Group Presents Georgia Land-Titling Project at Harvard, United Nations," https://bitfury.com/content/downloads/11_9_17_bitfury_presents_united_nationas_harvard.pdf

Bjelica, Jelena and Martine van Bijlert, Afghanistan Analysts Network. "The Troubled History of the E-tazkera (Part 2): Technical stumbling Blocks.," Afghanistan Analysts Network, Januay 2016 https://www.afghanistan-analysts.org/the-troubled-history-of-the-e-tazkera-part-2-technical-stumbling-blocks/

Bocco, Riccardo. "UNRWA and the Palestinian Refugees: A History within History." Refugee Survey Quarterly 28.2-3 (2009): 229-52. https://doi.org/10.1093/rsq/hdq001

Brayne, Sarah. Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment. American Sociological Review 79.3 (2014): 367-91. https://doi.org/10.1177/0003122414530398

Brown, Marshall. “Humanitarian Blockchain: Coding For A Humane, Sustainable World.” Forbes, February 2018. https://www.forbes.com/sites/marshallbrown/2018/02/15/humanitarian-blockchain-can-we-code-for-a-humane-sustainable-world/#32264426f3d4

Cadasta Foundation. "Blockchain for Land Administration: Hype or Substance?" https://cadasta.org/blockchain-for-land-administration-hype-or-substance/

Caplan, Jane and John Torpey. Documenting Individual Identity: The Development of State Practices in the Modern World. Princeton University Press, 2002.

The Cash Learning Partnership. "About Us." http://www.cashlearning.org/about-us/overview

Castells, Manuel. Power of Identity: The Information Age; Economy, Society, and Culture., Blackwell Publishers, 1997.

Civic. "Whitepaper," 2017. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf

Collins, Steve, Kate Sadler, Nicky Dent, Tanya Khara, Saul Guerrero, Mark Myatt, Montse Saboya, and Anne Walsh. "Key Issues in the success of community-based management of severe malnutrition." WHO, November 2005. http://www.who.int/nutrition/publications/severemalnutrition/FNB_0379-5721_Key_issues.pdf

Currion, Paul. "The Refugee Identity.," Caribou Digital, March 2018. https://medium.com/caribou-digital/the-refugee-identity-bfc60654229a

Datarella. "Building the Industrial Blockchain." https://datarella.com/

Driscoll, James R., Neil Sarnak, Daniel D. Sleator, and Robert E. Tarjan., "Making Data Structures Persistent." (Journal of Computer and System Sciences, 38.1 (1989): 86-124., https://www.cs.cmu.edu/~sleator/papers/making-data-structures-persistent.pdf

Duffield, Mark. "Challenging environments: Danger, resilience and the aid industry," Security Dialogue 43.5, (October 19, 2012): 475-92. http://journals.sagepub.com/doi/10.1177/0967010612457975

Einaste, Taavi. "Blockchain and healthcare: the Estonian experience." e-estonia, February 2018. https://e-estonia.com/blockchain-healthcare-estonian-experience/

Element, "About Us," https://www.discoverelement.com/#5

Ellerman, Antje. "Undocumented Migrants and Resistance in the Liberal State." Politics & Society 38.3 (August 2010). https://doi.org/10.1177/0032329210373072

Ethereum Foundation, "Devcon3 Day 4 Stream—Morning," November 2017. https://www.youtube.com/watch?v=vXVcuWvR5Z0&app=desktop#t=1h30m48s

Everest, "Fintech Elevating Humanity," https://everest.org/wp-content/uploads/2018/09/Everest_Whitepaper_01Sept2018-v2.pdf

Fraud Prevention Unit. "A Guide to Afghan Documents." U.S. Embassy Kabul, Afghanistan, 2011. https://wikileaks.org/gifiles/attach/10/10776_US%20Embassy%20Kab.pdf

Fiege, Uriel, Amos Flat, and Adi Shamir. "Zero-Knowledge Proofs of Identity." Journal of Cryptography (1988): 77-94. http://crypto.cs.mcgill.ca/~crepeau/COMP647/2010/TOPIC03/FFS88.pdf

FHIR. "About." http://www.hl7.org/about/index.cfm?ref=nav

Gelb, Alan and Anna Diofasi Metz. "Identification Revolution: Can Digital ID Be Harnessed for Development?" Center for Global Development, 2018. https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf

Gerard, David. "The World Food Programme's much-publicised 'blockchain' has one participant—i.e., it's a database," November 2017. https://davidgerard.co.uk/blockchain/2017/11/26/the-world-food-programmes-much-publicised-blockchain-has-one-participant-i-e-its-a-database/

Gisolfi, Dan. "Self-sovereign identity: Unraveling the terminology.," IBM, June 2018. https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-unraveling-the-terminology/

Goodwin-Gill, Guy and Jane McAdam. The Refugee in International Law. Oxford University Press, 2007.https://global.oup.com/academic/product/the-refugee-in-international-law-9780199207633?cc=us&lang=en&

go.eID.AS. "About." https://go.eid.as/#about

Graglia, Michael, Christopher Mellon, and Tim Robustelli. "The Nail Finds a Hammer: Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World." New America, October, 2018. https://www.newamerica.org/future-property-rights/reports/nail-finds-hammer/

Grossman, Wendy M. "Trust Who You Are Online With.," infosecurity, April 2016. https://www.infosecurity-magazine.com/magazine-features/trust-who-you-are-online-with/

Hague, Barry and Brian Loader, eds. Digital Democracy: Discourse and Decision Making in the Information Age, Routledge, 1999.

Hanstad, Tim. "Designing Land Registration Systems for Developing Countries." American University International Law Review 13.3 (1998): 647-703. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1358&context=auilr

Health Level Seven International. "About HL7." http://www.hl7.org/about/index.cfm?ref=nav

Hu-manity.co. "About." https://hu-manity.co/my31app/

IBM Knowledge Center. "Creating an encrypted database." https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.admin.sec.doc/doc/t0062035.html

IFRC. "Blockchain Open Loop Cash Transfer Pilot Project," October 2018. https://www.preparecenter.org/resources/blockchain-open-loop-cash-transfer-pilot-project

International Committee of the Red Cross. "Handbook on Data Protection in Humanitarian Action." Eds. Christopher Kuner and Massimo Marelli, July 2017. https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

International Federation of the Red Cross and Red Crescent Societies. "Land Rights and Secure Tenure Fundamental to Humanitarian Shelter Operations," July 2013. http://www.ifrc.org/fr/nouvelles/nouvelles/common/land-rights-and-secure-tenure-fundamental-to-humanitarian-shelter-operations-62681

———. “Blockchain Open Loop Cash Transfer Pilot Project,” September 2018. https://www.preparecenter.org/resources/blockchain-open-loop-cash-transfer-pilot-project

Irisguard. "What we do.," http://www.irisguard.com/

Ishai, Yuval, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. "Cryptography from Anonymity." Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science, 2006. http://web.cs.ucla.edu/~sahai/work/web/2006%20Publications/IKOS06.pdf

Jacobovitz, Ori. "Blockchain for Identity Management," December 2016. https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf

Ko, Vanessa and Andrej Verity. "Blockchain for the Humanitarian Sector: Future Opportunities." UN Office for the Coordination of Humanitarian Affairs, Digital Humanitarian Network, December 2016 https://reliefweb.int/report/world/blockchain-humanitarian-sector-future-opportunities

Latonero, Mark and Paula Kift. “On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control.” Social Media and Society, 2018. https://doi.org/10.1177/2056305118764432

Lundkvist, Christian, Rouven Heck, Joel Torstensson, Zac Mitton, and Michael Sena. "UPORT: A Platform for Self-Sovereign Identity," October, 2016. http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

Mercy Corps. “Cash Transfer Programming: toolkit.” https://www.mercycorps.org/sites/default/files/CTP1MethodologyGuide.pdf

Nawyn, Stephanie J. "Refugees in the United States and the Politics of Crisis." Oxford Handbook of Migration Crises, Eds. Cecilia Menjívar, Marie Ruiz, and Immanuel Ness. Oxford University Press, 2018. http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190856908.001.0001/oxfordhb-9780190856908-e-23

Norwegian Refugee Council. "Access to Tazkera and other Civil Documentation in Afghanistan," November 2016. https://www.nrc.no/resources/reports/access-to-tazkera-and-other-civil-documentation-in-afghanistan/

———. "Country Programme in Afghanistan," April 2017. https://www.nrc.no/globalassets/pdf/fact-sheets/2017/afghanistan/170515-nrc-afg-t1-2017-fact-sheet-with-map.pdf

The Nobel Prize. "Nansen International Office for Refugees." https://www.nobelprize.org/prizes/peace/1938/nansen/history/

ObjectTech. "Identity Reimagined." https://www.objecttechgroup.com/

Oxfam International. "Cash Learning Partnership (CaLP)." https://policy-practice.oxfam.org.uk/our-work/humanitarian/cash-learning-partnership

Payne, Geoffrey, Alain Durand-Lasserve, and Carole Rakodi. "The limits of land titling and home ownership." Environment and Urbanization 21.2, (2009): 443-62. http://journals.sagepub.com/doi/10.1177/0956247809344364

Red Cross and Red Crescent Climate Centre. "Forecast-based financing." https://www.climatecentre.org/programmes-engagement/forecast-based-financing

Red Rose. "About." http://www.redrosecps.com/about

Roberts, Jeff John. "How Biometrics are Worse than Passwords." Fortune, May 2016. http://fortune.com/2016/05/12/biometrics-passwords/

Schoemaker, Emrys, Paul Currion, and Bryan Pon, "Identity at the Margins: Identification Systems for Refugees." Caribou Digital, 2018. http://docs.caribouprojects.net/identity/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf

Scott, James C. Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed., Yale University Press,: 1998.

Shalizi, Hamid. "Who is an Afghan? Row over ID cards fuels ethnic tension." Reuters, February 2018. https://www.reuters.com/article/us-afghanistan-politics/who-is-an-afghan-row-over-id-cards-fuels-ethnic-tension-idUSKBN1FS1Y0

Shin, Laura. "Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury," Forbes, April 2016. https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#56fe17d244da

ShoCard. "Travel Identity of the Future," 2016. https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf

Sovrin Board of Trustees. "Sovrin Provisional Trust Framework," March 2017. https://www.evernym.com/wp-content/uploads/2017/07/SovrinProvisionalTrustFramework2017-03-22.pdf

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

Turner, Dawn M. "Understanding eIDAS." Cryptomathic, January 2016. https://www.cryptomathic.com/news-events/blog/understanding-eidas

Tykn. "About." https://tykn.tech/about/

UNHCR. "The 1951 Refugee Convention." http://www.unhcr.org/en-us/1951-refugee-convention.html

———. "Common Cash Facility," March 2017. https://www.unhcr.org/596331dd7.pdf

———. "Nansen—a man of action and vision," September 2009. http://www.unhcr.org/en-us/events/nansen/4aae50086/nansen-man-action-vision.html

———. "What is a refugee?" http://www.unhcr.org/what-is-a-refugee.html

UN OCHA. "2017 Afghanistan Humanitarian Response Plan Mid-Year Review," 2017. https://reliefweb.int/sites/reliefweb.int/files/resources/afg.pdf

USAID. "Identity in A Digital Age: Infrastructure for Inclusive Development," 2017. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

Vaughan, Wayne, Jason Bukowski, and Glenn RempeTierion Network. "A Global Platform for Verifiable Data." Tierion Network, June 2017. https://tokensale.tierion.com/TierionTokenSaleWhitePaper.pdf

Veridium, "Unlocking the World's Environment Asset Markets." https://www.veridium.io/static/whitepaper.pdf

World Bank Group. "Doing Business 2018: Reforming to Create Jobs," 2018. http://www.doingbusiness.org/content/dam/doingBusiness/media/Annual-Reports/English/DB2018-Full-Report.pdf

World Economic Forum. "A Blueprint for Digital Identity," August 2016. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

World Food Programme. "Building Blocks: The Future of Cash Disbursements at the World Food Program," 2017. https://unite.un.org/sites/unite.un.org/files/session_2_wfp_building_blocks_20170816_final.pdf

———. "Building Blocks." https://innovation.wfp.org/project/building-blocks

Zetter, Roger. "Labelling Refugees: Forming and Transforming a Bureaucratic Identity." Journal of Refugee Studies 4.1 (1991): 39-62. https://www.researchgate.net/publication/31258425_Labelling_Refugees_Forming_and_Transforming_a_Bureaucratic_Identity