Self-Sovereign Identity Systems for Humanitarian Interventions

A Case Study on Protective Cash Transfer Programs

L. Stevens
Delft University of Technology
The Netherlands

Situation: Information management enables humanitarian organizations to make adequate interventions based on timely, appropriate and trustworthy information. A crucial type of information are identities, because they can be used to assess vulnerability and efficiently manage aid distribution. Vulnerability determines who receives aid first because resources are always limited. This information is increasingly being stored and processed in identity systems.
Complication: Most identity systems are centralized and produce analogue proofs of identity such as passports or ID cards. These systems are susceptible to privacy and data breaches. Centralization leads to single-points-of-failure and could lead to fraudulent behavior resulting in people lacking formal proofs of identity. In general there is limited interoperability between identity systems and limited collaboration between the owners of these systems.
Approach: To create an interoperable and shared digital identity system using a Design Science Research strategy and systems engineering approach. This system must be distributed, protect privacy and put the identity owner in control of his or her data. The foundation of the system consists of Humanitarian Information Management principles, Privacy-by-Design principles and Self-Sovereign Identity principles. This research creates a functional blockchain based system, that enables identities for the use-case of Cash Transfer Programs.
Results: We present a validated set of ten design decisions that represent the trade-offs that have been made and prescribe a blueprint for a technical design.
Next steps: Future research should be done on how such a system could be implemented and used. This would require a process design approach that has to be developed, Also, elaborate research into user experience and user interfaces should be conducted.

Keywords: Cash Transfer Programs, Self-Sovereign Identities, Blockchain, Design Science Research, Decentralized Identifiers

1. IDENTITY AND DATA SHARING WITHIN THE HUMANITARIAN SECTOR

Climate related disasters, geophysical catastrophes, armed conflicts and man-made environmental emergencies are becoming more frequent (Development Initiatives, 2017). The effects are often mutually reinforcing, severe, immediate and have a ripple effect (Pega et al., 2014). In 2010, approximately 500 million people lived in an uncertain and destructive environment (Guha-Sapir & D'Aoust, 2010). This was even before the Syrian conflict and Ebola crisis struck. In the Global Humanitarian Overview 2017, published by UN OCHA[1], an estimated 128.6 million people were in humanitarian need for which $22.2 billion is required for relief. Almost a 10-fold increase of what was needed in 1992 when the appeal for funding humanitarian needs was started (UN OCHA, 2016, p.5). All the while, the necessary resources to overcome or prevent the devastating outcomes of these disasters, remain limited. Therefore, NGOs, governments and humanitarian organizations are in search of more efficient and effective methods for intervention (Brien et al., 2017) and in the meantime, direct their resources to those who are most vulnerable.

Adequate interventions are enabled by timely, appropriate and trustworthy information. This makes information management (IM) a crucial activity. IM is empowered by using information technology (Van De Walle, Van Den Eede, & Muhren, 2009). *Information systems* (IS) merge information technology with work processes, and constitutes of six activities: "information capturing, transmitting, storing, retrieving, manipulating and displaying" (Van De Walle et al., 2009, p.13). Information systems gather data which "facilitate various institutional process improvements, such as data-driven decision making, increased efficiency, or greater transparency and accountability. These process improvements, in turn, enable the system to contribute to functional goals"(USAID, 2017, p.19). Humanitarian organizations are increasingly using information systems to increase efficiency and have joined the data revolution (Gonzalez Morales, Hsu,

[1]United Nations Office for the Coordination of Humanitarian Affairs

Poole, Rae, & Rutherford, 2014). Information systems are also used to optimize the designation of resources to vulnerable people. For example, to establish whether someone satisfies the vulnerability criteria, *identity systems* are consulted. Identity systems help in identifying and registering people, consisting of software, hardware and procedures (The World Bank Group, 2017b). In many nation states, providing identities is institutionalized by the government, in which identity attributes (e.g. biometrics, birth certificates, land-titles) are registered and issued as an analogue legal identity in the form of a passport or ID-card. These legal identities are considered a very strong proxy for trust and can be used to identify oneself at government departments, banks, telecommunication operators, insurance companies and the like (Gelb & Decker, 2012). Identities are a crucial part of information in many humanitarian operations, but the existing identity systems turn out flawed in such contexts:

- Information management by humanitarian organizations often takes place in dynamic, complex and chaotic environments, this frustrates coordination and collaboration in identity IM (Van De Walle & Comes, 2015);
- Investments in identity systems result in sector silos, which reduces interoperability and limited scalability (The World Bank Group, 2017b);
- 1.1 billion people have no official means to prove their identity, with the majority living in Africa and Asia (The World Bank Group, 2017a). Either because their existence is not acknowledged by the central institutions providing non-digital identities or because they are otherwise incapable of acquiring one, for example due to high costs, long travel distances or the lack of birth certificates.
- Most identity systems are centralized or federated (Smedinghoff, 2012; Wolfond, 2017; Dunphy & Petitcolas, 2018) this makes them susceptible to mass surveillance, individual surveillance and data breaches due to a single-point-of-failure (Nyst, Makin, Pannifer, & Whitely, 2016)

These obstacles should be mitigated to ensure secure, private and usable identity systems (Jacobovitz, 2016). A humanitarian identity system that tackles these challenges is yet to be designed. The final form of a system is a result of a process design in which participants interact and implement the system according to their (changing) preferences, which requires a technical and institutional design to be flexible. According to systems engineering practices, this design should not only constitute a technical perspective but also an institutional viewpoint and a process design to be successful.

2. DESIGN PRINCIPLES AND BLOCKCHAIN TECHNOLOGY

In this research we will present a technical and institutional design that is flexible as to best accommodate this future process design, but the actually design this process is left out of scope. The technical and institutional design shall be presented as a set of design decisions because they simulate trade-offs based on several collections of design principles or guidelines. First, we resort to Humanitarian Information Management Principles (HIMP), which aim for collaboration, inclusiveness and interoperability OCHA. Although HIMP are not always complied with in reality as a result of the turbulent humanitarian context Van De Walle and Comes, they can be used to embed sector-wide coordination in a design and potentially break up information silos. HIMP focuses on the data controllers and data processors, thus it can be complemented with a data subject perspective that is provided by the Privacy-by-Design (PbD) principles written down by Cavoukian (2009). PbD embeds data protection for the data subject into a design. Unfortunately, both HIMP and PbD do not deal with the issue of centralization. There is a good reason for that: there was no fruitful way to do it when they were developed. Centralization was necessary to grant the trustworthy value that official identities hold, but this has its downsides. With the conception of blockchain technology this could be the past. To grasp this, one first needs to understand what a blockchain is.

A blockchain is a digitally distributed ledger, which is almost immutable, append-only and borderless. In essence, blockchain is simply a way to structure data. All data on a blockchain is digitized which eliminates the need for paper and manual documentation (Deloitte, 2017). So instead of relying on an analogue, hard-copy identity like a passport, one can rely on a digital identity. Specific information is stored in a block of data which is cryptographically sealed, chronologically stored with a permanent time-stamp and thus providing a trace of data transactions (Deloitte, 2017). These blocks should not contain any personal details but could contain references to securely and locally stored private information. Each node in the network holds a copy of the ledger, hence the term "distributed", of the data which is automatically updated when everyone in the network agrees on an updated version of the ledger (Deloitte, 2017). Blockchain facilitates the formation of self-sovereign identities. Self-sovereignty is about data subjects owning and controlling their own identity, this is possible in a distributed system with no single authority (Baars, 2016). Since this technology does not require one or multiple central authorities to provide a trustworthy data record but rather relies on consensus and strong cryptographic properties, it could tackle challenges concerning the power of central institution, security and privacy. Allen (2016), in a seminal blogpost, proposes a set of Self-Sovereign Identity (SSI) principles.

Table 1
Overview of Principles based on Allen (2016), Cavoukian (2009) and OCHA (2002)

Principles	Source	Rationale
Existence	SSI	Users must have an independent existence
Control	SSI, PbD	Users must control their identities
Access	SSI	Users must have access to their own data
Transparency	SSI, PbD	Systems and algorithms must be transparent
Persistence	SSI, HIMP	Identities must be long-lived
Portability	SSI	Information and services about identity must be transportable
Interoperability	SSI, HIMP	Identities should be as widely usable as possible
Consent	SSI	Users must agree to the use of their identity
Minimalization	SSI, HIMP	Disclosure of claims must be minimized
Minimization	SSI, HIMP	Only relevant data is collected
Protection	SSI, PbD	The rights of users must be protected
Proactive; Preventative	PbD	Design for it in advance, prevent incidents from happening
Privacy by Default	PbD	Privacy must be embedded in the design as the default
Humanity	HIMP, PbD	System must do no harm
Accessibility	HIMP	Each humanitarian actor must have access
Inclusiveness	HIMP	System must stimulate collaboration and partnership
Accountability	HIMP	System must evaluate the reliability and credibility of the data
Objectivity	HIMP	A variety of data sources must be used
Timeliness	HIMP	Data must be collected, analyzed and disseminated efficiently

The three sets of principles, can be combined into one comprehensive list, as can be seen in table 2. To use this trio as a guideline is new. Consequently, we do not know what such a system would look like. Therefore a case study on a specific type of humanitarian assistance, Cash Transfer Programs (CTPs), is conducted. The remainder of this article is build up as follows. In the next paragraph this case study is introduced and the research design is discussed. In paragraph 4, the role identity plays in CTPs and the results are presented. In paragraph 5 we will discuss these results and conclude this study.

3. DESIGN SCIENCE RESEARCH FOR CASH TRANSFER PROGRAMS

Cash Transfer Programs (CTPs) are humanitarian interventions that can be implemented as an alternative or in parallel to in-kind assistance. CTPs are increasingly popular (Barder et al., 2015) and can be defined as: "..programs that provide non-contributory cash grants to selected beneficiaries to satisfy minimum consumption needs" (Garcia & Moore, 2012, p. 18). A CTP can have a *protective* aim, where they assure that people continue to live on a basic level of welfare and do not endure permanent losses as the result of a disaster. A CTP can also *prevent* people from falling into poverty in the first place or *promote* people out of poverty (Garcia & Moore, 2012). All three types of CTPs should, when conducted, be organized by national or local governments, yet usually only the latter two are. During disasters CTPs are carried out with permission of the authorities, but they are themselves incapable or unwilling to do so (Pega et al., 2014; Arnold, Conway, & Greenslade, 2011; Garcia & Moore, 2012). This gives the humanitarian organizations a mandate to use digital identity systems in protective CTPs, which is why this research focuses on protective CTPs.

The set of design decisions is the final result of a Design Science Research (DSR) strategy and systems engineering approach. The strategy lays out the phases of this research, while the systems engineering defines the mind-set. The DSR strategy is often used in IS research and applied to wicked problems (Johannesson & Perjons, 2014). For a wicked problem there are no off-the-shelf solutions and requirements are unknown or unstable (Churchman, 1967). Hence, DSR strategy is a good fit. The same goes for systems engineering which is often used for complex socio-technical issues. Balancing the difficult to understand blockchain technology with the tangled humanitarian governance structures and challenging environments, requires a systems engineering perspective that meticulously demarcates the solution space. In line with DSR theory by Johannesson and Perjons (2014) a research design was set-up. The first step was a system analysis consisting of a technical, institutional and stakeholder viewpoints. Desk research and a literature review provided the input for this analysis and the results were validated using semi-structured interviews. A decision was made to focus on three sets of principles. The second step was to develop a program of requirements based on these principles. In the third step a comparative analysis of four blockchain based identity systems was conducted and mapped against the program of requirements. This generated alternatives for the design and made clear where trade-offs had to be made, resulting in ten design decisions. In figure 1 it is visualized how the principles are embedded in the design decisions. In

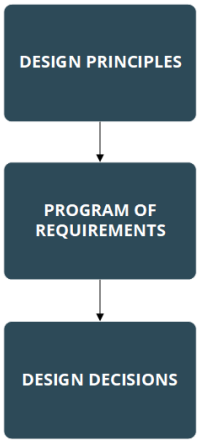

Figure 1. From principles to design decisions

the appendix the full traceability is provided. Step 4 demonstrated the potential use of these design decisions and discusses an expert validation, upon which a second version of the design decisions was generated.

4. DESIGN CHOICES

Before going in to the results of the research, it is of importance to better understand how protective CTPs work and how identity is an integral part of it.

4.1. The case of Protective Cash Transfer Programs

At the start of every CTP lies a geographical demarcation and a market survey to establish whether a local market is responsive or bound to be responsive at the time of cash disbursement. If not, an in-kind assistance program would be preferred. The design and development of a protective CTP is done by using guidelines of which many exist and which are often organization specific. Two general toolkits are provided by the ICRC[2] and the Cash Learning Partnership[3] (CalP). Synthesizing the steps and phases provided in these toolkits results in a generic flow diagram that is presented in figure 2. First a CTP is initiated, which can be done by a humanitarian organization or a government, but in all cases the local or national government must approve the initiative. Then a CTP is planned and designed. One can distinguish six design components: Objectives, Monitoring & Evaluation, Transfer Amounts, Targeting & Registration Method, Time Frames and Transfer Mechanism (Best Use of Resources Initiative, 2015; Harvey & Bailey, 2011). In the second step, the operational program is created which entails what distribution channels are used, who is involved and other practical details. Then the potential beneficiaries are targeted, done based on the vulnerability criteria that are defined in the planning phase. Criteria can be related to the disaster, have to do with socio-economic and demographic variables or focus on specific vulnerable groups (Red Cross Movement, 2017). The people that meet the criteria are then registered and identified. The cash can be distributed either as a conditional (specific rules for spending apply) or unconditional cash grant. Lastly the humanitarian organizations monitor the spending by doing follow-up interviews, focus groups and market surveys. This structure of events demonstrates the importance of identities for targeting, of assuring the right people receive assistance for a pre-specified number of times and for monitoring. Identity here has a functional purpose and is instrumentally used, or, in other words, it has a single purpose for humanitarian (cash based) assistance with an organization (USAID, 2017). In areas where multiple humanitarian organizations operate, this means people receive several functional identities and in some cases lead to people being "NGO fatigued" due to the many inquiries and data collections (Fabres, 2011).

There are several methods for targeting of which community based targeting and categorical selection are frequently used. Categorical selection is based on the selection criteria and people are either in or out the category, while community based targeting invites local representatives to have a say in who is included or not. Both of these methods are suboptimal, as including local representatives introduces local bias (Kelaher & Dollery, 2008) and categorical selection is highly dependent on the available data which is often scarce (Brooy, 2007). Once a list of people is set up, they should be registered and identified. Identification can also be seen as authentication, are the people listed as who they say they are and do they really meet the criteria.

Identities in CTPs are registered, validated and stored by the use of several information and identity systems. Sometimes comprehensive software is used, such as PIRS from the International Organisation for Migration (IOM) or BIMS from the UNHCR. But the turmoil in disaster environments does not always allow for state-of-the-art options to be used, so excel-sheets stored on local laptops and paper-based lists are still frequently used. We can see that these systems, combined with manual targeting, are prone to targeting errors, fraud and selection biases. Kebede (2006) finds that targeting errors might make the most vulnerable even worse off, because the scarce amount of resources can be bought by even fewer people. Within these systems there is a high degree of centralization and information siloes, i.e. there is little collaboration or interoperability. People that are selected for CTPs are unable to control their identities and have to trust humanitarian organizations will handle their data securely and respect their privacy. One could wonder about the emphasis on privacy in these crisis situations. However, recalling any ethnic cleansing or genocide, one can understand the importance of protecting personally and demographically

[2] http://rcmcash.org/

[3] http://www.cashlearning.org/toolkits/cash-toolbox

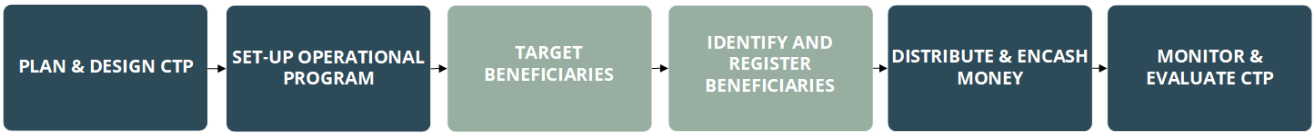

Figure 2. Flowdiagram of a Cash Transfer Program

identifiable information.

To summarize, identities play an integral part in CTPs. They allow for registration, monitoring and targeting of people that are in dire need of cash-based assistance. The identity systems used for CTPs come across similar and more context specific challenges that identity systems deal with. These realizations legitimize the application of a blockchain based self-sovereign identity system which can be designed for the purpose of collaboratively managing identities in an interoperable system.

4.2. Ten Design Decisions

So how would such a system look? In this article we propose a set of design decisions to convey this system design as it illustrates making trade-offs. These design decisions have been validated by translating them into BPMN and UML Class diagrams, furthermore the set has been validated by five experts. The experts had backgrounds in blockchain development, blockchain identities, generic identity management and humanitarian IT systems. In the following paragraphs the final version of the design decisions stemming from this research are discussed. To be clear, the first decision is to use blockchain as we must acknowledge that blockchain is no holy grail and other alternatives are out there.

Design Decision #1: Use Blockchain Technology. The decision for blockchain is made because it enables self-sovereignty, uses very strong encryption and because it encodes trust partly into the system. The openness of blockchain technology stimulates organizations to behave correctly which might improve collaboration between humanitarian organizations. Yet, blockchain is a nascent technology which comes with uncertainties. Also, there are multiple blockchains being developed for similar use-cases (not necessarily humanitarian) that could increases the overall inefficiencies of blockchains. One could question whether the humanitarian sector has the mandate to participate in this rat race, but at least the sector has a good use case. In case multiple blockchains are developed than at least these systems should be extremely interoperable.

Design Decision #2: Use a Public Permissioned chain. A public permissioned chain is open to all for registration of their identities, which people could do themselves if they own a device or could otherwise do at a registration terminal. To create and update blocks, nodes in the network should have certain authorities. This does interfere with the concept of at truly self-sovereign system, but it resembles the current governance system more which could favour implementation. A public permissioned chain does not fully encapsulate trust in a system, so there is a need for a trust-framework outside the technical system. This might create a barrier, because a group of individuals or organizations either allows or disallows organizations to join, in the meanwhile it also creates a buy-in and could yield a larger effort to make it successful. Lastly, permissioned chains are much more scalable than permissionless chains and its growth can be controlled (Hileman & Rauchs, 2017). This control can be an attractive feature for participants that might be weary of this new technology.

Design Decision #3: Use Decentralized Identifiers and a fully User-centred System. Each identity system needs an identifier that uniquely identifies an entity in the system. To make sure no double identifiers exist central authorities are often in charge of handing them out. However, blockchain and in specific decentralized identifiers (DIDs) require no central authorities to ensure uniqueness. On top, DIDs are a W3C standard which ensures interoperability and flexibility as they can be used on any blockchain. DIDs are pairwise pseudonymous, which means that they are only used between one identity owner and one other party (W3C, 2018). DIDs enable a fully user-centred design, which allows the identity owner to take full control of his or her identity and initiate all contact with other participants in the network (Sporny & Longley, 2016). An identity owner can have several hundred DIDs, for each digital relationship there is one. Only the DIDs are stored on the blockchain, which upon initiation of the owner can reveal a means of contact without storing any private information on the blockchain. The connection can be revoked when the owner wishes to. In figure 3 the workings of this user-centred design and DIDs is presented. In this scenario the identity owner has already acquired a basic digital identity. So the identity owner request a validated credential, for example a date of birth. The attribute provider has its own registry of information and provides a credential based on the information in that registry, signs the credential of which a public part is stored on the blockchain so it becomes clear for everyone in network that this particular attribute provider has signed it. The attribute provider then issues the credential, upon which the identity owner countersigns. To request a service with a service provider, or in this case a humanitarian organization that executes a CTP, the identity owner connects with the service provider. The service provider then sends an inclusion algorithm, that

the identity owner can fill in with credentials. It sends back whether the criteria are met and who has signed the credentials, the service provider can then check if it trusts the attribute providers.

Design Decision #4: Use Hyperledger Indy as a Blockchain. There are several permissioned blockchains that can be used. We chose Hyperledger Indy as it is developed specifically for self-sovereign identities, embeds privacy-by-design principles, is public permissioned and has a wide support of powerful international organizations Sovrin and TYKN. Using the roles provided by Hyperledger, only humanitarian organizations can be made service providers. This enables a functional purpose for CTPs.

Design Decision #5: Use a GPLv3 license. If the whole humanitarian sector should be able to use the system, it should not be made proprietary. This could make the system less attractive for others to join. There are several open source licenses, the GPLv3 is strongly protective and requires other users or developers to instantly open up their versions of the system (Hess, 2014). It does allow for commercial use, which might be frowned upon since it is realized with non-profit funds. This way of licensing the system, creates transparency for all stakeholders involved. The level-playing field is equal, which could bring more organizations to the table. A potential drawback is that it could result in free-rider behavior.

Design Decision #6: Use Hyperledger Indy Roles and matching Interfaces. Within Hyperledger Indy there are several roles. The highest in rank are the Trustees, which can be seen as a board of directors for the system. They appoint Stewards who run two types of nodes (Hyperledger, 2018). Validator nodes that can write and update the blockchain, and observer nodes that give reading access to the blockchain. Stewards appoint Trust Anchors, which can be identity providers, attribute providers or service providers. The users in the system are called identity owners or Custodians. The former control their own identity while the latter control the identity for somebody else. All communication between Trust Anchors, identity owners and Custodians is done outside of the blockchain via software agents. For this a Decentralized Public Key Infrastructure (DPKI) is used, that "is a collection of internet technologies that provides secure communications in a network" (Hyperledger, 2017) which requires no central authority.

Design Decision #7: Offchain storage is to be determined by context. For privacy purposes, only the DIDs and public-faced credentials are stored on the blockchain. All other information has to be stored offchain. Most notably the private key that gives access to an Identity Wallet holding all the DIDs for one person is stored offchain. This can be done on a personal device, if available, or on paper. The raw identity attributes or self-attested claims, e.g. identity attributes that have not been validated yet, can also be stored on the device or on paper. Each identity owner should have a backup available, which can be made via the software agents. This backup holds some centrality since it is stored via the software agents which can have multiple options available such as secure cloud storage's (positive for scaling purposes), Highly Secure Modules or Smartcards. The same applies here: it depends on the context which software agent is used. Several options exist and each option should be as safe and secure as possible.

Design Decision #8: Social and offline key recovery, two-factor authentication and centralized account protection. Self-sovereignty implies that key loss should also be arranged in a decentralized fashion, yet there are no solutions out there to prevent a permanent key loss. Additionally, a key loss might result in someone else taking over the account and misusing an identity. In this humanitarian context it could make people even worse off, as vulnerable people would now be the ones without digital identities. This must be prevented and therefore some of the centrality that is already included in the system by the permissioned architecture, is utilized as a means to retrieve access. Several techniques such as multi-signature signing (BitGo, 2018) or hierarchical deterministic key pairs (Robles & Appelcline, 2016) can be exploited to achieve this feat. Alongside, social recovery which comprises of assigning trusted peers in the network to recover a key or using an offline back-up to restore access are also offered. Finally, two-factor authentication (biometrics plus passphrase) can be used to access the account at centralized computer terminals in case of private key loss.

Design Decision #9: Targeting is seen as a service not as a separate activity. The system is designed with a functional purpose: providing a tool for interoperable and collaboratively managing of identities to improve targeting, identification and registration in CTPs. In the current practice, targeting is initiated by humanitarian organizations based on a set of inclusion criteria. Via various targeting mechanisms people are selected, which can result in inclusion errors, fraud and is time consuming. If targeting is seen as a service, than people should only be informed about its existence, how and when they can apply for the service. Using an inclusion algorithm that is send to the identity owner which verifies the credentials and matches it to the inclusion criteria, little bias is included and an objective inclusion score is retrieved. One could imagine people subscribing to a newsfeed in which all participants of the network can publish their CTPs and inclusion criteria, the identity owner can then reach out him/herself.

Design Decision #10: Validation by attribute provider and appointed validator. Many self-sovereign systems provide peer-validation, but its value is difficult to establish. It could be transformed into a trust score of sorts, but then the peers that validate must provide some kind of public validation which can be related to each other. Within a human-

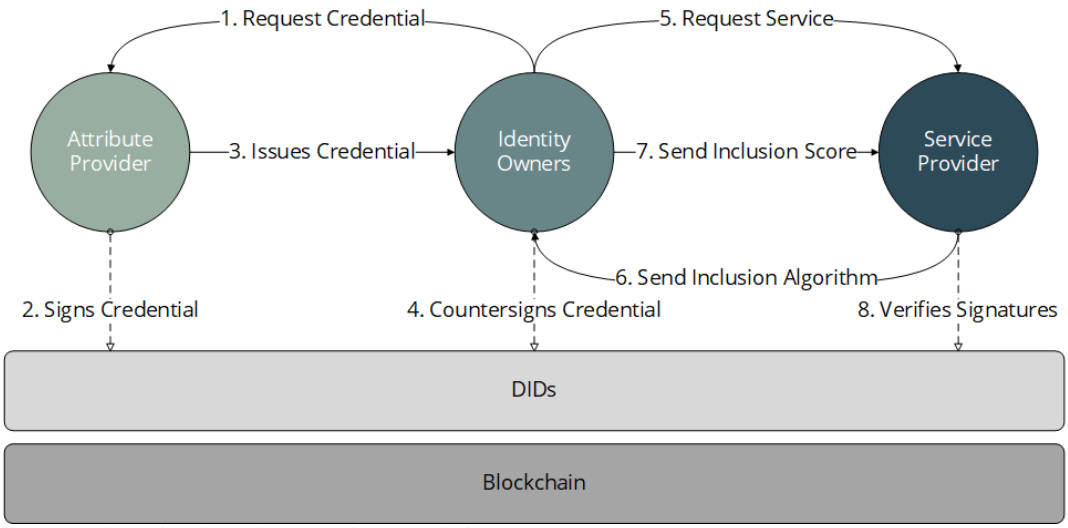

Figure 3. User-centred Design based on Sovrin Foundation (2018)

itarian context this is not preferable, since it could demographically classify groups of people. On the other hand, humanitarian organizations often collaborate with volunteers or community representatives that also sensitize the community for CTPs and have local knowledge. This creates the need for some peers to be able to validate in the field, but only if they are authorized by humanitarian organizations or other attribute providers. Validation is also possible by attribute providers that already hold some information on identity owners, for example schools, municipalities and tax offices. These can be approached by the identity owner to validate specific attributes.

5. DISCUSSION

The design decisions combined present a prescription upon which a digital identity system for CTPs could be developed. They serve a functional purpose. Yet, in the wider context of humanitarian assistance and identity in general, we can reflect on the opportunities for the design decisions to also serve a foundational purpose. A foundational purpose implies that there is a single system useful for multiple purposes. E.g. beneficiaries could also use their digital identities for taking out insurance or acquiring a mobile phone contract. (USAID, 2017). This would give identity owners, attribute providers and service providers a continuous incentive to keep information up-to-date. It might be desirable to first develop this system with a functional purpose since CTPs are a suitable use case to create an installed base of identity owners. Especially since humanitarian organizations have a limited mandate outside times of distress, the value of an already functioning system might persuade nation states to join and create a foundational system with a continuous value proposition. The current design decisions do not immediately allow for this as only humanitarian organizations are allowed to provide services. Nonetheless if Stewards and Trustees decide to open-up the role for service provider, other non-humanitarian organizations could take on this role. National and local governments, other authorities but also private organizations could provide these services. In that case the system would also be useful for CTPs that have the purpose of promotion or prevention. This would truly break-up information silos within and outside of the humanitarian sector while protecting the privacy of each identity owner. The added value for collaboration and interoperability lies mainly in the provision of a tool, which could bring together all involved organizations in a process management approach. If the right process design is created which has an acceptable entry-barrier but makes it difficult for participants to leave the negotiation table, the set of design decisions could be transformed into a final technical and institutional design. So although blockchain takes away a lack of trust in data sharing and breaks up silos, working with blockchain based systems is not trustless, even more so if a permissioned chain is used (Hileman & Rauchs, 2017). Organizations might still distrust credentials given to identity owners and this is a problem technology alone will not solve and might not be solvable at all. Finally, the decision to go with a permissioned system comes with some centrality. Nevertheless, the privacy of people is better protected and there are no single-point-of-failures due to the distributed architecture. The permissioned character also allows for controlled growth of the system, which can be particularly important as existing programs and aid workers must have time to adapt.

6. CONCLUSION & FUTURE RESEARCH

This study takes a DSR strategy and systems engineering approach. Within the case study of CTPs we focus on creating a self-sovereign digital identity system with a functional

purpose. The unique combination of Humanitarian Information Management Principles (HIMP), Privacy-by-Design (PbD) principles and Self-Sovereign Identity (SSI) principles lays at the foundation of the ten design decisions above. This contributes to the academic knowledgebase as it combines the ideological concept of self-sovereignty is combined with the practical measures to improve collaboration and better protect the privacy of data subjects. We found that the design decisions, if taken out of the context of CTPs, can serve a foundational purpose but this is dependent on the specific roles of participants. Significant added value of this study can be found in that the design decisions can bring together important stakeholders as it offers flexibility, transparency and interoperability. Without these design decisions it would be much more difficult to get the right organizations around the table. Nonetheless, the critical decisions and final agreements shall be made collaboratively and require trust regardless of what a technical system can offer. Future research should therefore focus on how this process design might look. This should take in the current humanitarian governance structures, formal and informal powers and financial arrangements. The result of this research could be a concise participation model, proposed leading actors and process rules. Throughout the process the representation of the design principles should be monitored. Other future research has to be done on the preferences and needs of identity owners. Cultural differences, illiteracy, digital immaturity and ownership of devices, all play a role in how identity owners might perceive the system. This requires field-research, co-design sessions and translating the results into interfaces. Lastly, when the system has a more foundational purpose the information should be kept up to date by the community and identity owners themselves. Several researchers have already touched upon the theories of Elinor Ostrom and self-governance in relation to blockchain based systems, it would be interesting to see if this theory or other theories could be of assistance in composing the right environments and incentives to keep information up-to-date. This would truly realize a global digital identity system where information is up-to-date and in control of the people that it belongs to. Not only the humanitarian sector would benefit, but humanity in general.

References

Allen, C. (2016). *The Path to Self-Sovereign Identity.* Retrieved from http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Arnold, C., Conway, T., & Greenslade, M. (2011). *Cash Transfers* (Tech. Rep.). Department for International Development.

Baars, D. (2016). *Towards Self-Sovereign Identity using Blockchain Technology* (Unpublished doctoral dissertation). Universtiy of Twente.

Barder, O., Blattman, C., Cameron, L., Egeland, J., Elmi, M., Faye, M., ... Woodman, L. (2015). *Doing cash differently: How cash transfers can transform humanitarian aid* (Tech. Rep. No. September). ODI. Retrieved from https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf doi: 2052-7209

Best Use of Resources Initiative. (2015). *Cost Efficiency Analysis: Unconditional Cash Transfer Programs* (Tech. Rep.). New York: IRC. Retrieved from https://www.rescue.org/sites/default/files/document/954/20151113cashcefficreportfinal.pdf

BitGo. (2018). *BitGo: Making Digital Currencies Usable for Business.* Retrieved from https://www.bitgo.com/info/solutions#custody

Brien, C. O., Scott, Z., Smith, G., Barca, V., Kardan, A., Holmes, R., & Watson, C. (2017). *Shock-Responsive Social Protection Systems Research Synthesis Report* (Tech. Rep. No. January). Oxford: Oxford Policy Management.

Brooy, J. L. (2007). A Weighted Welfare Analysis of Local Price Inflation. *Journal of Human Security*, *5*(2), 65–82.

Cavoukian, A. (2009). *Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices* (Tech. Rep.). Retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf%5Cnwww.privacybydesign.ca doi: 10.1007/s12394-010-0062-y

Churchman, C. (1967). Guest editorial: Wicked problems". *Management sciences*, *14*(4), 141–142.

Deloitte. (2017). *Key Characteristics of the Blockhcain.* Deloitte Touche Tohmatsu India LLP. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-key-characteristics-noexp.pdf

Development Initiatives. (2017). *Global Humanitarian Assistance Report 2017* (Tech. Rep.). Bristol: Development Initiatives. Retrieved from http://devinit.org/wp-content/uploads/2017/06/GHA-Report-2017-Full-report.pdf

Dunphy, P., & Petitcolas, F. (2018). A First Look at Identity Management Schemes. *IEEE Security and Privacy Magazine*.

Fabres, B. (2011). Think Global, Act Global in the Mekong Delta? Environmental Change, Civil Society and NGOs. *Advances in Global Change Research*, *45*(1), 7–34. doi: 10.1007/978-94-007-0934-8

Garcia, M., & Moore, C. M. T. (2012). *The Cash Dividend*. Washington D.C.: The World Bank. Retrieved from http://elibrary.worldbank.org/doi/book/10.1596/978-0-8213-8897-6 doi: 10.1596/978-0-8213-8897-6

Gelb, A., & Decker, C. (2012). Cash at Your Fingertips: Biometric Technology for Transfers in Developing Countries. *Review of Policy Research*, *29*(1), 91–117.

Gonzalez Morales, L., Hsu, Y., Poole, J., Rae, B., & Rutherford, I. (2014). *A World That Counts* (Tech. Rep.). IEAG. Retrieved from www.undatarevolution.org

Guha-Sapir, D., & D'Aoust, O. (2010). *Demographic and Health Consequences of Civil Conflict* (Tech. Rep.). Washington, D.C.: The World Bank. Retrieved from http://wdr2011.worldbank.org/sites/default/files/pdfs/WDRBackgroundPaper-SapirandD'Aoust.pdf?keepThis=true&TB_iframe=true&height=600&width=800

Harvey, P., & Bailey, S. (2011). *Cash transfer programming in emergencies* (Vol. 44; Tech. Rep. No. 11). London: ODI. doi: 0855985631

Hess, K. (2014). *Decisions, decisions. How do you choose an open source license?* Retrieved from https://www.zdnet.com/article/decisions-decisions-how-do-you-choose-an-open-source-license/

Hileman, G., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study* (Tech. Rep.). Cambridge, UK: Cambridge Centre for Alternative Finance. Retrieved from https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf

Hyperledger. (2017). *Introduction âĂŤ hyperledger-fabricdocs master documentation.* Retrieved from http://hyperledger-fabric.readthedocs.io/en/release-1.1/blockchain.html

Hyperledger. (2018). *Getting Started with Libindy.* Retrieved from https://github.com/hyperledger/indy-sdk/blob/master/doc/getting-started/getting-started.md

Jacobovitz, O. (2016). *Blockchain for Identity Management* (Tech. Rep. No. December). Beer Sheva: Ben-Gurion University. Retrieved from https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. Stockholm: Springer International Publishing. doi: 10.1007/978-3-319-10632-8

Kebede, E. (2006). Moving from emergency food aid to predictable cash transfers: Recent experience in Ethiopia. *Development Policy Review*, *24*(5), 579–599. doi: 10.1111/j.1467-7679.2006.00349.x

Kelaher, D., & Dollery, B. (2008). Cash and in-kind food aid transfers: The case of tsunami emergency aid in banda aceh. *International Review of Public Administration*, *13*(2), 117–128. doi: 10.1080/12294659.2008.10805125

Nyst, C., Makin, P., Pannifer, S., & Whitely, E. (2016). *Digital Identity : Issue Analysis Executive Summary* (Tech. Rep. No. June). Guildford, UK: Consult Hyperion.

OCHA. (2002). Best Practices in Humanitarian Information Management and Exchange. In *Symposium on best practices in humanitarian information exchange.* Geneva: United Nations Office for the Coordination of Humanitarian Affairs.

Pega, F., Walter, S., Liu, S., Pabayo, R., Lhachimi, S., & Saith, R. (2014). Unconditional cash transfers for reducing poverty and vulnerabilities: effect on use of health services and health outcomes in low- and middle-income countries. *Cochrane Database of Systematic Reviews 2014,*(6), 1–18. doi: 10.1002/14651858.CD011135.www.cochranelibrary.com

Red Cross Movement. (2017). *M3_3_2_1 Targeting criteria.* Geneva: International Red Cross and Red Crescent Movement. Retrieved from http://webviz.redcross.org/ctp/docs/en/1.toolkit/Module3ResponseAnalysis/M3_3Targeting/M3_3_2Identifytargetingcriteria&mechanisms/M3_3_2_1Targetingcriteria.docx

Robles, K., & Appelcline, S. (2016). *Hierarchical Deterministic Keys for Bootstrapping a Self-Sovereign Identity.* Retrieved from https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/draft-documents/hierarchical-deterministic-keys-for-bootstrapping-a-self-sovereign-identity.md

Smedinghoff, T. J. (2012). Solving the legal challenges of trustworthy online identity. *Computer Law and Security Review*, *28*(5), 532–541. Retrieved from http://dx.doi.org/10.1016/j.clsr.2012.07.001 doi: 10.1016/j.clsr.2012.07.001

Sovrin, & TYKN. (2018). *Paper Sovrin.*

Sovrin Foundation. (2018). *Sovrin âĎć : A Protocol and Token for Self- Sovereign Identity and Decentralized Trust* (No. January).

Sporny, M., & Longley, D. (2016). *A Web-based Ledger Data Model and Format.* Retrieved from https://www.w3.org/2016/04/blockchain-workshop/interest/sporny-longley.html

The World Bank Group. (2017a). *Identification for Development (ID4D).* Retrieved from http://www.worldbank.org/en/programs/id4d

The World Bank Group. (2017b). *Technical Standards for Digital Identity: Draft for Discussion* (Tech. Rep.). Washington, D.C.: International Bank For Reconstruction and Development/The World Bank.

UN OCHA. (2016). *Global Humanitarian Overview 2017* (Tech. Rep.). New York City: United Nations. Retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/GHO_2017_publication_corrections_digital.pdf

USAID. (2017). *Identity in a Digital Age: Infrastructure for Inclusive Development* (Tech. Rep.). Washington, D.C.: USAID. Retrieved from https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

Van De Walle, B., & Comes, T. (2015). On the Nature of Information Management in Complex and Natural Disasters. *Procedia Engineering*, *107*, 403–411. Retrieved from http://dx.doi.org/10.1016/j.proeng.2015.06.098 doi: 10.1016/j.proeng.2015.06.098

Van De Walle, B., Van Den Eede, G., & Muhren, W. (2009). Mobile Response. In J. Löffler & M. Klann (Eds.), *Lncs* (pp. 12–21). Springer-Verlag. Retrieved from http://link.springer.com/10.1007/978-3-642-00440-7 doi: 10.1007/978-3-642-00440-7

W3C. (2018). *Decentralized Identifiers (DIDs) v0.10.* Retrieved from https://w3c-ccg.github.io/did-spec/

Wolfond, G. (2017). A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review*, *7*(10), 35–40. doi: http://doi.org/10.22215/timreview/1112

APPENDIX

Table 2
Overview of Principles based on Allen (2016), Cavoukian (2009) and OCHA (2002) and mapped to requirements

Principles	**Source**	**Rationale**	**Satisfied by Requirement**
Existence	SSI	Users must have an independent existence	R.1
Control	SSI, PbD	Users must control their identities	R.2, U.3, U.4
Access	SSI	Users must have access to their own data	U.1, U.3, U.4
Transparency	SSI, PbD	Systems and algorithms must be transparent	C.3, C.13, C.15
Persistence	SSI, HIMP	Identities must be long-lived	U.3, U.4
Portability	SSI	Information and services about identity must be transportable	I.5
Interoperability	SSI, HIMP	Identities should be as widely usable as possible	C.14, R.10
Consent	SSI	Users must agree to the use of their identity	R.6, U.4
Minimalization	SSI, HIMP	Disclosure of claims must be minimized	U.4
Minimization	SSI, HIMP	Only relevant data is collected	R.4
Protection	SSI, PbD	The rights of users must be protected	C5, C.6, C.7
Proactive; Preventative	PbD	Design for it in advance, prevent incidents from happening	Integral to design
Privacy by Default	PbD	Privacy must be embedded in the design as the default	C.7
Humanity	HIMP, PbD	System must do no harm	C.5
Accessibility	HIMP	Each humanitarian actor must have access	C.10, C.11
Inclusiveness	HIMP	System must stimulate collaboration and partnership	C.11, C.14
Accountability	HIMP	System must evaluate the reliability and credibility of the data	T.3
Objectivity	HIMP	A variety of data sources must be used	R.7, R.8
Timeliness	HIMP	Data must be collected, analyzed and disseminated efficiently	T.7

Table 3
Design decisions and system mapped onto program of requirements

ID	Requirement	Satisfied?	Decision
R.1	Each Person Affected shall be able to register for one digital identity as an Identity Owner	**No**	**2,3**
R.2	Each Person Affected shall be able to self-register or register by delegate	**Yes**	**2**
R.3	Each Person Affected should add a geo-location when registering	**Yes**	**6**
R.4	System shall only request a maximum amount of identity attributes	**Yes**	**2**
R.5	System should check for double identities	**No**	**3**
R.6	Humanitarian Organizations shall ask Person Affected to provide consent for the use of data	**Yes**	**4**
R.7	Only humanitarian Organizations shall be able to register as an attribute provider, identity provider and service provider	**Yes**	**2,4**
R.8	Community Representatives and Authorities should be able to register as an attribute provider	**Yes**	**2,4**
R.9	Humanitarian Organizations, Community Representatives and Authorities must have an humanitarian registration interface	**Yes**	**6**
R.10	System must allow all humanitarian organizations to become part of it	**No**	**1,2**
I.1	A Person Affected shall be able to have identity attributes validated by several attribute providers	**Yes**	**3**
I.2	Attribute providers shall be able to validate identity attributes and geolocations	**Yes**	**3**
I.3	Attribute providers shall be able to issue verifying credentials	**Yes**	**3**
I.4	Attribute providers must have an easy to use validation interface	**Yes**	**6**
I.5	Person Affected must always be able to access his/her credentials in a private storage	**Yes**	**7**
U.1	Person Affected must have an easy to use user-interface	**Yes**	**6**
U.2	A Person Affected shall be able to request services throughout the system	**Yes**	**3**
U.3	Person Affected shall be able to safely access, update, disclose and revoke their identities	**Yes**	**1,3**
U.4	Person Affected shall be able to regain access to their identity after loss of control or loss of access	**Yes**	**8**
T.1	Humanitarian Organizations shall be able to match Person Affected with their inclusion criteria	**Yes**	**9**
T.2	Humanitarian Organizations must have a service interface for targeting	**Yes**	**6**
T.3	Humanitarian Organizations shall be able to verify identities based on issued credentials from other organizations	**Yes**	**1,3**
T.4	Humanitarian Organizations must only be able to set up inclusion criteria based on minimum amount of identity attributes	**Yes**	**9**
T.7	Humanitarian Organizations should delete all information that is no longer necessary for a CTP project	**Yes**	**9**
C.1	The system must have roles for Identity Owners, Attribute Providers, Service Providers and Identity Providers	**Yes**	**2,6**
C.2	A Person Affected should be able to provide feedback during use of the system	**Yes**	**5**
C.3	System should be able to provide open response to the feedback of people	**Yes**	**2**
C.4	Humanitarian Organizations shall be able to create sub-entities to pass down responsibilities	**Yes**	**2,4**
C.5	All participants and the system must safely store all information	**No**	**1,2,7**
C.6	System must provide secure end-to-end encryption for all communication and sharing of data	**Yes**	**3**
C.7	System must provide the highest form of privacy feasible	**Yes**	**1,4,7**
C.8	System should enable an overview of where people have been registered	**Yes**	**6**
C.9	System must demand high data standards for all humanitarian organizations	**Yes**	**2**
C.10	System must be inclusive and accessible for all humanitarian organizations	**No**	**1,2**
C.11	System must be accessible at all times	**Yes**	**1,2**
C.12	System must be flexible and able to scale up	**Yes**	**1,2,4**
C.13	System must be open-source	**Yes**	**5**
C.14	System must use interoperable standards for digital identification	**Yes**	**1**
C.15	System must open up the governance structure online	**Yes**	**2**
C.16	System must have a functional purpose and grow into a foundational purpose	**Yes**	**2**
C.17	System must be accompanied by a participation model and process approach	**Yes**	**2**
C.18	System must not have a single owner	**Yes**	**1**
C.19	System must have an incentive system to demonstrate good behavior	**Yes**	**2.4**
C.20	Actors in the system shall be able to communicate with each other if communication is initiated by the Identity Owner	**Yes**	**3,6**