THE GRADUATE INSTITUTE GENEVA

INSTITUT DE HAUTES
ÉTUDES INTERNATIONALES
ET DU DÉVELOPPEMENT
GRADUATE INSTITUTE
OF INTERNATIONAL AND
DEVELOPMENT STUDIES

Managing Registration on the Blockchain –

The Future of Identity Management in Humanitarian Cash Transfer Programmes?

DISSERTATION

Submitted in fulfilment of the requirement for the Master in International Affairs (MIA)

By

Tara Stähli

Geneva, June 2018

Acknowledgment

I would like to express my sincere gratitude to Arjen Crince, Simon Tembo, Wunderful, Aneel Ahmed, Ajayi Ayobamile, Joanna Burton, Paula Gil Baizan, Rebecca Visschedijk and those who wish to remain anonymous for taking the time to provide thoughts and valuable insights on their experience and knowledge in Cash Transfer Programming as well as Vincent Graf and Niall Dennehy for their share of time and knowledge on digital identity and blockchain technology.

Throughout the research and writing process, I benefited largely from the diligent support and encouragement of the Netherlands Red Cross 510 Data Science Team. In particular I would like to thank Jonath Lijftogt, Stefania Giodini and Maarten Van der Veen for their supervision and insightful feedback on draft versions of this thesis.

Special thanks go to my supervisor Michael Schiltz for his openness towards my choice of an uncharted thesis topic and his guidance throughout the process. I would like to thank Filipe Calvão equally for supporting and guiding me as the second reader.

A heartfelt "Thank you" is directed at my family and friends for their unconditional support throughout the writing process of this thesis and, moreover, the entire period of my master's degree. Without their support, this accomplishment and all related endeavours would not have been possible. A final candid "Thank you" goes to Oliver for his continuous encouragement, for probing me to explore topics outside of my comfort zone and think in new ways.

Glossary of Abbreviations

AHR	Advanced Human Recognition
CBA	Cash-Based Assistance
CEN	European Committee for Standardisation
	[Original: Comité Européen de Normalisation]
CTP	Cash Transfer Program
DID	Digital Identity
DLT	Distributed Ledger Technology
FCBA	Future cash based assistance
GDPR	General Data Protection Regulation
HCI	Human-Computer Interaction
H2H	Human-to-Human
ICRC	International Committee of the Red Cross
ID	Identification Card
ISO	International Organisation for Standardisation
IDT	Information Diffusion Theory
MSF	Médecins Sans Frontières [Doctors Without Borders]
NGO	Non-Governmental Organisation
P2P	Peer-to-Peer
POI	Proof-of-Individuality
PoS	Proof-of-Stake
PoW	Proof-of-Work
RC	Red Cross
SDG	Sustainable Development Goals
TAM	Technology Acceptance Model
UNDP	United Nations Development Programme
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations International Children's Emergency Fund
UNOCHA	United Nations Office for the Coordination of Humanitarian Affairs
USAID	United States Agency for International Development
WFP	World Food Programme

Abstract

Humanitarian cash transfers are seen as a means to help diminish the gap between needs and available funding and are expected to increase in scale in the near future. In order to overcome current challenges of cash transfer programs, to make humanitarian aid more transparent and the system more accountable to its beneficiaries in general, means of improving the targeting and registration process of cash transfer programs are being explored. Solutions to complementing or replacing current registration and identity management systems are sought after in the innovative yet largely unexplored blockchain technology. The complexity of blockchain technology itself, however, introduces new challenges not only in terms of technology deployment, but moreover its usability to stakeholders and end users. The objective of this thesis is to shed light on the interface between the theoretical construct of a blockchain-backed identity and the practical usability and end-user acceptance of beneficiaries of a cash transfer programme.

Table of Contents

1. Introduction

“Having a digital identity is a basic human right.”[1]

“Identity is far more than just a card with a name and a photograph. ID technologies sit at the interface between the power and prerogatives of institutions and the rights and needs of individuals.[2]*”*

The humanitarian aid system is under austere strain. In 2016 an estimated 164 million people across 47 countries were in need of international humanitarian aid due to new and on-going crises. Affected countries more often than not face multiple crisis types – ranging from armed conflict to hosting refugees and facing disasters caused by natural hazards – leaving their communities vulnerable and reliant on assistance. Consequently, international humanitarian response has amplified from a total cost of $16.1bn in 2012 to $27.3bn in 2016.[3] Inevitably, the gap between needs and available funding is flaring.[4]

A widespread notion of a means to help diminish this gap lies within humanitarian cash transfers. Traditionally, humanitarian organisations have supported crisis-affected communities with physical commodities – such as food, shelter materials, blankets and seeds – but are increasingly shifting their focus to the distribution of cash as an alternative, enabling affected people to decide upon what they need and then purchase that at local markets[5]. Distribution of cash in humanitarian response is beneficial in various ways: By choosing cash transfers over delivery of goods in appropriate circumstances, assistance is provided to affected people faster and in a more targeted way than by traditional means, recipients are able to prioritize their own needs and maintain their dignity, overhead costs are reduced and local economies are fostered.[6]

[1] Anna Irrera, “Accenture, Microsoft team up on blockchain-based digital ID network”, *Reuters*, 19 June 2017, accessed 14 April 2018, https://www.reuters.com/article/us-microsoft-accenture-digitalid/accenture-microsoft-team-up-on-blockchain-based-digital-id-network-idUSKBN19A22B

[2] USAID, “Digital identity“,11 September 2017, accessed 12 April 2018, https://www.usaid.gov/digital-development/digital-id/report, 2

[3] Development Initiatives, “Global humanitarian assistance report 2017, June 2017, accessed 14 April 2018, *Development Initiatives*, http://devinit.org/post/global-humanitarian-assistance-2017/, 2

[4] John Farrington et al. “Targeting approaches to cash transfers: comparisons across Cambodia, India and Ethiopia”, Overseas Development Institute, June 2007, accessed 15 April 2018, https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/3924.pdf, 7

[5] Paul Harvey and Sarah Bailey. “Cash transfer programming and the humanitarian system.” Background note for the High Level Panel on Humanitarian Cash Transfers, April 2015. London: Overseas Development Institute, Accessed 20 April 2018, https://www.odi.org/publications/9455-cash-transfer-programming-and-humanitarian-system

[6] “CBA: Cash based assistance the future”, 510.global, 26 January 2018. Accessed 15 April 2018. https://www.510.global/the-future-of-cash-based-assistance-2/

The delivery of cash to beneficiaries is conducted through a number of means, including 'cash in envelopes', pre-paid plastic cards or electronically through mobile phone transfers.[7] However, current cash transfer programs (CTP) face a number of challenges including security issues, costliness, corruption and time. Of all the challenges, targeting and registration, meaning the process of determining *who* is eligible to receive aid and *how* this person is registered into the CTP system remains the hardest one.[8] With CTPs being widely funded and employed by governments, international aid agencies (NGOs, UN, Red Cross and Red Crescent National Societies) and national civil society organizations, they are expected to multiply and increase in scale in the near future.[9] In order to overcome current challenges of CTP, to make humanitarian aid more transparent and the system more accountable to its beneficiaries in general, means of improving the targeting and registration process of CTPs are being explored. Solutions are being sought after in technology – one of them being blockchain technology, i.e. distributed ledger technology.

Initially linked to financial applications, attention is now beginning to shift toward the appropriation of this disruptive technology in a myriad of sectors, including development and humanitarian aid where resources are limited, budgets are low and documentation is scarce.[10] Blockchain is perceived as a potential means to improve current identity management systems for implementing humanitarian organisations as well as for beneficiaries of respective programs and projects. Robust identification is required for a number of reasons, i.e. for a project-implementing humanitarian organisation this includes streamlining of humanitarian services and managing recipients' eligibility of benefits.[11] Consequently, for individuals, identification often acts as a prerequisite access rights, entitlements, services and ensure political, economic and social inclusion for individuals.[12]

Blockchain technology is thus being taken into consideration in complementing or replacing databases used for registration and identity management in humanitarian operations.[13] As a type of distributed database hosted across a network of several participants,

[7] Paul Harvey and Sarah Bailey, "State of evidence on humanitarian cash transfers", Overseas Development Institute, March 2017, accessed 29 April 2018, https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9591.pdf, 7

[8] Ibid., 4

[9] Development Initiatives, "Humanitarian assistance report 2017, 7

[10] Ben Paynter, "How blockchain could transform the way international aid is distributed", Fastcompany, 18 September 2017, accessed 23 April 2018, https://www.fastcompany.com/40457354/how-blockchain-could-transform-the-way-international-aid-is-distributed

[11] USAID, "Identity in a digital age", 16

[12] Michael Pisa and Matt Juden, "Blockchain and economic development: hype vs. reality", CGD Policy Paper 105, July 2017, accessed 5 May 2018, https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality

[13] USAID, "Identity in a digital age", 58

blockchain technology allows for information to be stored and shared in a secure, trustworthy and immutable way.[14] Storing personal identifying data safely is fundamental to any form of identity management system. Hence, technology providers are becoming confident that the transparent and decentralized nature of blockchain technology is becoming "the key ingredient in providing an interoperable identity framework", [15] as it enables the development of a non-refutable and unbreakable record of data and gives individuals greater control as to who can access their personal information to which extent.

Some of blockchain's main attributes, including immutability, security, privacy, trust and portability, have moved this technology into the limelight. A number of start-ups including BanQu, Taqanu and Sovrin Foundation have acknowledged the potential of this disruptive technology in cracking the tough nut of beneficiary registration – and developed blockchain-based ID approaches aimed at providing functional digital IDs to some of the world's most vulnerable.[16] Furthermore, Accenture and Microsoft recently announced the development of a prototype for a digital ID network based on blockchain technology for the UNHCR identity management system.[17] While the potential of this new means of registration and identity management is indeed catching – as it adds value for both individual and institutional actors – , it should be enjoyed with precaution. Embracing a technology that is still in its infancy, as is the case with blockchain, may potentially create risks for those who rely on it before understanding the full extent of it.[18] Furthermore, the fine and delicate line between easing access to crucial services versus requiring identity as a condition to access these services and consequently the establishment of unintended new exclusionary barriers need to be considered.[19] While successful humanitarian use cases of blockchain technology are emerging, one should hardly expect it to become a silver bullet for each and every humanitarian challenge.[20] Rapidly evolving technological innovations are making the political and social context of identity management systems progressively complex – "the need for

[14] Vanessa Ko and Andrej Verity, "Blockchain for the humanitarian sector: future opportunities." Digital Humanitarian Network, November 2016, accessed 7 May 2018, http://digitalhumanitarians.com/resource/blockchain-humanitarian-sector-future-opportunities, 4

[15] Jeffrey Schwartz, "Microsoft among those pitching blockchain at UN summit to end identity crisis", Redmond Magazine, 25 May 2016, accessed 12 May 2018, https://redmondmag.com/blogs/the-schwartz-report/2016/05/microsoft-among-those-pitching-blockchain.aspx

[16] Pisa and Juden, "Blockchain and economic development", 12

[17] BBC News, "Accenture and Microsoft plan digital IDs for millions of refugees", *BBC News,* 20 June 2017, accessed 13 May 2018, http://www.bbc.com/news/technology-40341511

[18] GSMA, "Blockchain for development: emerging opportunities for mobile, identity and aid", *GSMA*, 14 December 2017, accessed 24 April 2018; USAID, "Identity in a digital age"

[19] Alan Gelb and Julia Clark, "Identification for development: the biometrics revolution", CGD working paper 315, Center for Global Development, January 2013, accessed 27 March 2018, http://www.cgdev.org/content/publications/detail/1426862, 5

[20] GSMA, "Blockchain for development", 5-7

clear understanding and informed engagement around ID systems and technologies has never been greater."[21]

Hence, the most important question that needs to be asked: Is a blockchain-based identity/registration system a feasible solution for a community not only from a technological but rather also socio-economic perspective? What are the benefits of this new registration system for the *end-users*, i.e. the beneficiaries of a CTP? Is this new identity system flexible enough to indeed assist the accessing of services and exercising of rights of end-users rather than hinder them from doing so? While a technological innovation may sound plausible from a system's design perspective, it is crucial to analyse and understand how digital tools operate within a given social context and what its added value is for the users in order to avoid unintended negative consequences or rejection.[22] Hence, users' needs are to be prioritized over an organisation's own desires for efficiency in regard to a new system.[23] The goal is thus to design a system that is not only fast, secure and cost-efficient but also accessible for and empowering to users as well as accepted within the given community. Most importantly, an implementing humanitarian organisation should consider if the adoption of a blockchain-based identity registration system can overcome the drawbacks of its traditional counterpart whilst remaining an accessible, socially accepted and empowering means for the beneficiaries.

1.1 Research Aim

The objective of this thesis is to shed light on the *interface between the theoretical construct of a blockchain-based identity and the practical usability and end-user acceptance within a low literacy and low digital penetration setting.* More specifically: to carefully examine *the usability and technology acceptance of blockchain-based identity management for beneficiaries of cash transfer programs.* Although these questions will be applied to humanitarian cash transfer programs, they are up to a certain extent, applicable to the humanitarian sector in a broader sense. The focus hereby lies on the balance between needs of the individual (beneficiary), the institution (humanitarian organisation) as well as technological feasibility. Despite blockchain technology being discussed as a key success factor and silver bullet for many current challenges, including humanitarian and developmental ones, there is currently little academic research available on blockchain technology initiatives in developing countries. There is even less information on projects and

[21] USAID, "Identity in a digital age", 2
[22] Ibid., 5
[23] Ibid., 4

initiatives tackling the identity management issue. With information on such initiatives being limited to a small body of academic literature and little anecdotal information, a large knowledge gap exists that has to a certain degree, facilitated the spread of the blockchain hype. [24] There is a ubiquitous perception that technologies are innately social products – society shaping how technology is harnessed. And yet, the prevalent view today more often than not seems to be the opposite.[25] When exploring innovative approaches and solutions in general, but foremost in cases of vulnerable and aid-inclined people, focus should be laid on *access* and *usability* of new tools. Theories of technology acceptance and usability as well as previous technology deployments have all together demonstrated that without using or (to a certain extent) owning a particular technology, individuals cannot benefit from them.[26]

The research question (and sub questions) of this thesis thus follows:
What are the potentials and challenges of a blockchain-based identity management system for beneficiaries of a cash transfer program in regard to usability and technology acceptance?

Consequently, the sub questions are:

- *What is the rationale of using blockchain technology rather than systems for identity management that have been around longer?*
- *Is blockchain technology better at addressing problems of identity management than existing approaches and technologies?*
- *What are the challenges of using blockchain technology for identity management and what new risks might that create for the beneficiaries of a cash transfer program?*

By means of a graduate position, I have received the opportunity to join the 510 Data Team of the Netherlands Red Cross in researching possibilities of future cash based assistance (FCBA) in humanitarian disasters and crises. More specifically, the 510 Data Team (hereafter referred to as 510) aims to enhance the status quo of current CTPs by designing a potentially blockchain-backed system that incorporates a digital self-sovereign identity upon registration and cash transfers by means of cryptocurrency. As an independent researcher I am part of 510's research team that focuses on digital identities, with the purpose of investigating social implications of digital CTP on beneficiaries of developing countries. The findings of this

[24] Raul Zambrano, "Blockchain – unpacking the disruptive potential of blockchain technology for human development", white paper, International Development Research Centre, August 2017, accessed 24 March 2018, https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf , 14
[25] Ibid.
[26] Ibid.

social interface investigation will, to a certain extent, shape and scope the way in which the FCBA project will be implemented in selected countries – naturally with consideration of technical feasibility for which 510 is collaborating with the Dutch tech-start up Tykn. Hence, this thesis will overall contribute to the academic literature gap on blockchain-based identity management and provide a knowledge basis for the 510 Data Science Team in regard to practical usability and technology acceptance of identity management of the planned digital cash transfer program implementation in developing countries.

1.2 Structure of the thesis

Structurally, this thesis will start off with a background overview of the current state of the art of humanitarian cash-based assistance, including challenges and an outlook to where innovative trends are heading in the near future (chapter 2). Following the scene setting, chapter 3 will provide the reader with a detailed overview of relevant concepts regarding identity and identity systems in order to understand the basis of the discussion. Once the interlinked 'problem fields' (cash-based assistance and identity systems) have been outlined, chapter 4 introduces the proposed 'solution', namely blockchain technology and its potential to tackle the aforementioned challenges. By means of an extensive literature review, the potential and drawbacks of blockchain deployment in managing identity and registration of CTP beneficiaries are highlighted. Derived from the literature review, the most profound knowledge gap is identified as being the understanding of user experience, usability and technology acceptance of this novel technology application. Chapter 5 builds on the previous chapter by elaborating on the actual implementation of a blockchain-based identity in theory on the one hand, and as a visionary concept to solve the registration challenge of a CTP on the other hand. The theoretical framework that underlies this thesis is introduced in chapter 6, using three main schools of thought, namely Technology Acceptance Model, Innovation Diffusion Theory and Human-Computer Interaction. These three approaches focus on determining factors of usability and technology acceptance of end-users, which are taken as a guideline for the subsequent data collection that is presented in chapter 7. Chapter 7 is an analysis of the qualitative data collection, i.e. by means of conducted interviews, divided into focal points relevant to the research question(s). The following section – chapter 8 – recaps and substantiates the most important findings, links them to the applied theoretical framework and responds to the research question(s) outlined at the beginning of this thesis. The concluding chapter 9 presents an outlook to open questions that have yet to be answered through subsequent research.

1.3 Methodology

The methodological approach chosen for this thesis is a qualitative one. In order to gather the necessary data on the applicability and implications for blockchain technology in regard to identity management systems, and to be able to answer my research question, two approaches were chosen:

a) Extensive desk research

Study and analysis of academic literature, white papers and reports by international humanitarian aid organisations such as the International Federation of the Red Cross and Red Crescent Societies, The World Bank, USAID etc.

For the first part, I conducted a desk research, in order to grasp the concept of identity management in CTP and its related challenges. Identity management being a complex issue, I laid out a thorough conceptualisation of the relevant terms (meaning of identity, digital identity, identity management) as a first step. For this, I relied on reports, articles and documents that discuss the meaning of identity, the concepts of identity management and the potential – and challenges – of a self-sovereign blockchain-based identity. Blockchain-based identity management being a relatively new phenomenon, a lack of academic literature was to be expected at the time of this research. Hence I lay my focus mainly on experience-based reports and other sources of grey literature, rather than concentrate on predominantly academic peer-to-peer literature (which was not sufficient in terms of quantity and content).

b) Qualitative Interviewing

As a second step, the objective being to obtain a more detailed and in-depth understanding of identity management in CTPs in general and, furthermore, in technology acceptance of CTP beneficiary registration, I conducted a number of semi-structured interviews. Laying a focus on knowledge and opinion questions[27] enabled me to fill the knowledge gap caused by a lack of extensive literature and case studies up to a certain extent.

I chose to focus on interviewing people who are either experienced on the topic of cash transfer programs and beneficiary registration of cash transfer programs specifically and/or knowledgeable on the topic of digital identity (who were also familiar with blockchain technology). In order to achieve somewhat generalizable and transferable results, I made sure that the response group represented diversity within the field of CTP, i.e. that respondents represent a variety of positions related to CTP in order to shed light on differences in

[27] Michael Patton, *Qualitative Evaluation and Research Methods* (Newbury Park, CA: Sage, 1990)

experience and opinions.[28] The type of interview chosen was semi-structured interviews, conducted remotely via Skype or face-to-face, in a group or on a bilateral means. This being said, all the interviews extended beyond the original questions and thus took on the nature of an exchange of ideas and knowledge rather than a traditional question-answer format. Participants were, on one hand, recruited with help of 'gatekeepers', i.e. people within 510 who were able to help identify organisational members of the Red Cross movement and facilitate access to those potential respondents, and, on the other hand, by conducting online research on CTP on appropriate people outside the Red Cross movement. A detailed outline of the interview questions can be viewed in annex 1. In total ten interviews were conducted, together with Lars Stevens, a graduate student in Systems Engineering at Delft University of Technology simultaneously doing research on the same topic, but from a technical feasibility perspective. The respondents outside of the Red Cross movement were approached by us as independent researchers in order to sustain a neutral stance.

For the discussion of the interviews, i.e. the analysis part of my thesis, I took on a mainly inductive analysis, meaning the discovering of patterns, themes and categories in my obtained qualitative data. The findings thus emerged as a result of my interaction with the obtained data.[29]

2. Cash Transfer Programming in humanitarian aid

Humanitarian action is rooted in the principle of humanity – the universal impulse to assist people in surviving disasters and conflicts. Most commonly, disaster response happens on a local level, where neighbours or communities compile their resources to help each other and the national governments assist their citizens. In cases where local and national capacities are exhausted and a state (normally) requests external assistance, international humanitarian action comes into play.[30] International humanitarian action embodies a complex network of institutions and organisations, the main entities being donor governments, the United Nations and its executing organisations (including but not limited to UNICEF, WFP, UNHCR), the Red Cross and Red Crescent Movement and international NGOs. In the aforementioned cases of national capacity exhaustion, these institutions and organisations aim to complement and/or

[28] Nigel King and Christine Horrocks, *Interviews in Qualitative Research* (London: Sage, 2010)
[29] Patton, *Qualitative Research and Evaluation Methods*, 68
[30] Harvey and Bailey, "Cash transfer programming and the humanitarian system", 2

substitute for national efforts to assist and protect suffering civilians.[31] Assistance provided by humanitarian organisations is based on a set of agreed principles; humanity and impartiality, the latter representing the idea of non-discrimination and non-favouritism in providing aid. In addition, humanitarian organisations strive to adhere to the principles of neutrality and independence in order to gain the trust of authorities as well as affected populations in the case of natural disasters or conflicts.[32]

Humanitarian assistance can take on a multitude of forms, ranging from food, shelter materials, seeds, household goods, blankets or clothes to cash – in the latter case allowing people to decide for themselves what they need most and purchase it in local markets to promote their own well-being.[33] Distributing cash has emerged as an increasing trend within the framework of humanitarian action, and acting as one of the principal tools for disaster and conflict recovery support.[34] Although this form of aid has a long history dating back to the 1870 Franco-Prussian war, its growing implementation compared to in-kind aid is noteworthy and prominent.[35] Cash has been, and to this day, is provided in numerous ways: Conditional cash transfers ties the financial assistance to specific conditions, such as specific actions that need to be undertaken by the beneficiary or particular goods for which it can be spent. Sometimes it is also attached to a work condition. Unconditional cash, on the other hand, refers to money that can be used for whichever goods or services a beneficiary chooses. The ways in which money is delivered to the beneficiaries also varies; from cash in envelope to pre-paid cards or digital transfers via, for example, a mobile phone.[36] In certain cases, beneficiaries are not provided with cash but a paper or electronic voucher instead which can be exchanged for goods at a pre-selected vendor. Naturally, choices of purchase and where these goods are bought are determined by the aid agency and thus limited to a certain extent.[37] However, this form of cash-based assistance is often chosen when cash is seen as an inappropriate or unable form of aid distribution, such as, for example, in cases of market weaknesses, a lack of local infrastructure or security fears.[38] Hence, the appropriateness of cash distribution depends largely on the specific context; whether people can actually buy the

[31] Ibid.,2

[32] Ibid.

[33] Paul Harvey, “Cash-based responses in emergencies”, 1

[34] Harvey and Bailey, “Cash transfer programming and the humanitarian system”, 2

[35] Ibid.

[36] GSMA 2017, „Mobile Money, Humanitarian Cash Transfers and Displaced Populations“, GSMA, 23 May 2017, accessed 10 April 2018, https://www.gsma.com/mobilefordevelopment/programme/mobile-for-humanitarian-innovation/mobile-money-humanitarian-cash-transfers/, 5

[37] Harvey and Bailey, “cash transfer programming and the humanitarian system”, 2

[38] Paul Harvey, “Cash and vouchers in emergencies“, Overseas Development Institute, February 2005, accessed 15 April 2018, https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/432.pdf, 1

goods they need in local markets at a reasonable price and a safe environment and whether cash can be delivered to beneficiaries in a safe manner.[39]

Somewhat unsurprisingly, cash-based response approaches evoke reservations related to a myriad of factors, the most common ones being inflationary risks (cash causing prices for key goods to rise dramatically), increased security risks (moving cash resulting in higher security risks for beneficiaries and staff of cash programmes), targeting difficulties (cash being more attractive than goods may dilute abilities to target the most vulnerable), disadvantaging women (who are less able to have control over cash within a household than with goods), anti-social use of cash, hesitation of donors to provide cash over commodities and increase in corruption.[40] Nonetheless, hesitation is also deeply rooted in the fear about the misuse of cash and the tradition of organisations and governments assuming that people are unable to make sensible decisions by themselves and thus deciding on what they need.[41]

On the other hand, there is emerging evidence of advantages from cash assistance in situations where it is appropriate. It is seen to be more cost-efficient than commodity-based alternatives due to lower logistics and transportation costs, it allows beneficiaries to maintain dignity and choice to decide what they want to use the money for, it can have a knock-on economic benefit for local markets and trade and may stimulate other areas of livelihoods, too. Additionally, unlike commodities, cash circumvents disincentive effects as it usually fosters local markets, trade and production. Overall, growing humanitarian evidence and experience of humanitarian cash transfers suggest that cash represents a favourable form of response and, furthermore, exemplifies good value for money compared to in-kind assistance.[42] CTP can thus be useful in a number of contexts, for example before a disaster strikes[43], in order to provide preparation for a predictable shock or as a risk reduction strategy (retaining walls, irrigation, etc.), at the beginning of and throughout a crisis to cover vital food, non-food and income needs, or during the recovery/transition period to support livelihoods, construct shelters and short-term employment opportunities. Additionally, CTP can be crucial in times of chronic food crises

[39] Harvey and Bailey, "cash transfer programming and the humanitarian system", 3

[40] Overseas Development Institute, "Doing cash differently", Overseas Development Institute, September 2015, accessed 1 May 2018, https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf, 15

[41] Harvey and Bailey, "cash transfer programming and the humanitarian system", 3

[42] Overseas Development Institute, "Doing cash differently", 15

[43] Recent research shows that every euro spent before a disaster saves seven euros (in average) after the disaster happened (Rode Kruis, "1 Euro Voroof scheelt gemiddeld 7 euro achteraf", accessed 4 May 2018, https://voorkomderamp.rodekruis.nl/over-ons)

and droughts or floods to provide communities and families with an income when they are at their most vulnerable.[44]

The humanitarian aid system increasingly being under major strain, cash transfers are likely to proliferate in serving as a mechanism to scale up humanitarian funding in appropriate cases. This would enable a reduction in costs and complexity of humanitarian assistance.[45] This being said, cash transfer programming does not come without a set of challenges – challenges that need to be addressed especially when thinking about scaling the programming up in order to sustainably maintain it. These include, among others, complexity of local situations in regard to access, targeting errors, limited availability of data, collaboration and coordination challenges, monitoring etc.[46] More recently, there has been a shift to cash being distributed digitally, enabled partially by the rise of electronic payment technologies, but also due to the need to transfer money to large numbers of recipients and its consequent level of accountability.[47] Digital means of cash transfers are seen to reduce leakage, improve reconciliation and control of expenditure, be more efficient and reliable, reduce costs for organisations and beneficiaries and improve security for staff and beneficiaries compared to manual payment. This accounts especially for cash transfer programs in isolated rural areas, or areas with limited physical and financial infrastructure.[48] On the other hand, digital transfer mechanisms open the cash transfer programming up to a whole new range of challenges, including poor network and infrastructure, low literacy, lack of training and lack of prior experience with technology.[49]

Of all the challenges, targeting, meaning the process of determining who is eligible to receive aid, remains the hardest one.[50] Targeting is very closely tied to registration, i.e. the process by which an individual's personal information is recorded into the aid providing institutions' register and ultimately acts as a decisive tool of eligibility. Targeting and registration can be characterised by means of three stages: Firstly, policy decisions about who is to be supported through cash transfer programming (e.g. according to age, geographic location, gender, ethnicity, or economic and social status), secondly, the process of

[44] Overseas Development Institute, "Doing cash differently."
[45] World Bank, " Cash transfers in humanitarian contexts: Strategic note", World Bank, 30 April 2016, accessed 18 April 2018, https://interagencystandingcommittee.org/system/files/humanitarian_cash_transfers_final_copyedited.pdf, 2
[46] From notes taken during the interviews with CTP delegates
[47] GSMA, "Mobile Money, Humanitarian Cash Transfers and Displaced Populations", 13; Gabrielle Smith et al., "New technologies in cash transfer programming and humanitarian assistance" CALP, 1 January 2011, accessed 20 April 2018, https://www.humanitarianlibrary.org/resource/new-technologies-cash-transfer-programming-and-humanitarian-assistance-0, ix
[48] Ibid.; Smith et al.,"New technologies in cash transfer programming", 4
[49] Smith et al., "New technologies in cash transfer programming", 5
[50] Harvey and Bailey, "State of evidence on humanitarian cash transfers", 4

identifying the beneficiaries and keeping information about them up to date, and thirdly, design and implementation of mechanisms ensuring that aid is provided to the intended individuals, with minimal inclusion and exclusion errors.[51] A possible and increasingly important, yet in practice often overlooked fourth stage, "is that of ensuring that targeting criteria are simple enough, and information about them presented in a sufficiently accessible way, for even those intended beneficiaries with limited literacy to understand their entitlements."[52]

Evidently, targeting and registering in cash transfer programs need improvement in the long run in order to scale up. The humanitarian sector is thus increasingly seeking solutions to challenges in technology, including tackling the issue of undocumented people (one of the fundamental underlying issues in targeting and registration is the fact that a large percentage, if not the majority, of the intended recipients of aid are undocumented people).

This thesis thus focuses on addressing and potentially overcoming the issue of registration in cash transfer programming – and that of a lack of identity more generally – by turning to technology to find solutions.

This being said, as the issue of beneficiary registration is fundamentally the same as that of any humanitarian crisis: How can people without a legal identity participate fully in social and economic life? In almost all cases a legal identification is a prerequisite for partaking in social and economic life and relates directly to a number of other SDGs.[53] Hence, the potential of this innovative technology to foster social inclusion and facilitate the SDG 16.9 – aiming at widespread legal identity for every individual by 2030 – are interwoven in this research. Throughout the process of research, the questions of 'What is identity?' and 'Why is identity important?' are recurring and pervasive. Thus, before exploring answers to the questions of how to tackle the issue of registration in CTP's, it is crucial to fully grasp the meaning and concept of the underlying and fundamental issue at hand – identity. "Identity

[51] Farrington, Sharpa nd Sjoblom „Targeting Approaches to Cash Transfers: Comparisons across cambodia, india and ethiipoa,", 1

[52] Farrington et al.," Targeting Approaches to Cash Transfers",1

[53] Identification is perceived as a direct enabler in achieving a number of other SDG goals, including but not limited to: **Target 1.3** (Implementation of appropriate social protection systems), **Target 1.4** (Ensure that all men and women have equal rights to economic resources, as well as access to basic services, property, inheritance, natural resources, new technology and financial services), **Target 5a** and **5b** (women's equal access to economic resources and promote women's empowerment through ICT), Target **17.7** (Strengthening of domestic tax collection), **Target 16.5** (Reducing corruption). Source: Mariana Dahan and Alan Gelb, "The role of identification in the post-2015 development agenda", World Bank Working Paper, 7 July 2015, accessed 9 May 2018, https://www.cgdev.org/sites/default/files/CGD-Essay-Dahan-Gelb-Role-Identification-Post-2015-ID4D_0.pdf, 6

will be the most valuable commodity for citizens in the future, and it will exist primarily online."[54]

3. Conceptualisation on identity and identity systems

This chapter aims to offer a narrative overview of the concepts used in this thesis, to define them and, moreover, provide a picture of how they relate to one another.

3.1 What is identity?

By implication identity is a complex social construct, embodying various and multiple meanings depending on the thematic, temporal and territorial context it is placed in. The conception of identity has undergone a greatly explored and multifaceted history in the social science discipline, and indeed significant changes.[55] And yet, in the broadest sense, identity captures the question '*Who am I?'*, covering a multitude of personal, relational and social factors and processes and continuously incorporating input and feedback from the environment.[56] In this sense, identity can be described as a *set of personal and psychological characteristics, physical features, preferences and life experiences that uniquely describes an individual*.[57] It refers to either a) a social category, defined by membership rules, distinctive characteristics or expected behaviour or b) socially distinguished features that a person takes a special pride in and views as immutable but socially significant – or a combination of a) and b). Identity in the modern sense thus symbolises far more than physical attributes, namely also dignity, pride and honour.[58]

Since the early days of civilisation humans use identity to establish interactions with other people, facilitate the actions of those they know and trust, and protect themselves against those they do not know or trust. Therefore, identity is closely linked to a person's

[54] Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business* (Hachette, UK: John Murray, 2013)

[55] Peter Nagy and Bernadett Koles, "The digital transformation of human identity", Convergence, 20, no.3 (2014): 278, accessed 5 May 2018, doi: https://doi.org/10.1177/1354856514531532

[56] Leary et al. "Aspects of Identity and Behavioural Preference: Studies of Occupational and Recreational Choice." *Social Psychology Quarterly* 49, no.1 (1986): 11-18, accessed 6 May 2018, http://dx.doi.org/10.2307/2786853; James Marcia, "Development and Validation of Ego Identity Status," *Journal of Personality and Social Psychology 3,* no.5 (1966): 551-558

[57] Atick et al. 2014, "Digital Identity Toolkit: A guide for Stakeholders in Africa". World Bank Group, Washington, DC, 1 June 2014, accessed 2 May 2018, http://documents.worldbank.org/curated/en/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa; Gelb and Clark, "Identification for Development".

[58] James Fearon, "What is Identity (As we now use the Word)?" (Thesis, Standford University, 1999). 1-3

reputation, which earns trust in the given community. From this perspective, identity is at the core of human-human interactions.[59] This concept will be revisited later on when exploring the transformation from human-human to human-machine system interactions.[60]

In modern societies, the aforementioned relational basis for trust is broken down and many interpersonal interactions, such as banking or voting, are often almost anonymous.[61] Hence, proxy-based systems of establishing trust are crucial when relationships reach beyond communities and countries. These systems usually rely on ID tokens such as an identity document (ID) or other pieces of information such as a PIN or password that can prove identity claims. [62] The concept of identity has thus changed from the early days of civilization, in the sense that is has been institutionalised. This process is more commonly known as *identification* or registration, whereby an individual's official identity is created and/or recorded by an institution. This results in the issuing of an identity document (ID) or an equivalent token.[63] For instance, a birth has to be registered to obtain a birth certificate. This is a formal proof of legal identity, which later enables the individual to enrol in school, vote, and so forth.[64] Identification is ultimately about trust, whereby an ID token can replace anonymity by serving as a trust proxy to support a claim to be a specific person.[65] Recognition by a formal institution increases trust and reduces the institution's risk by enabling it to hold a person accountable in case of unreliability.

Identification is often closely connected to the issuing of a *legal identity*, which signifies the attributes (name, date of birth, sex, current address, nationality, etc.) that an individual uses to identify him- or herself when interacting with formal institutions such as governments, banks or employers. This information is needed to determine a person's identity, which is connected to his or her rights and responsibilities regarding these institutions.[66] Governments have the ultimate accountability over the process of identification and hence almost exclusively generate legal identity.[67] As such, governments are credible legal identity providers, which per se provides them with enormous power and control over

[59] Atick et al., "Digital identity toolkit", 9

[60] Ibid.

[61] USAID, "Identity in a digital age", 3

[62] Ibid.,3-4

[63] Gelb and Clark, "Identification for development", 6

[64] Ibid., 5-7

[65] USAID, "Identity in a digital age", 4

[66] Gelb and Clark, "Identification for development", 5

[67] World Bank, „Principles on Identification", Working Paper 112614, World Bank, Washington D.C., 1 February 2017, accessed 10 May 2018, http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age, 3

their citizens.[68] ID cards that include ethnicity or religion can be – and have been – used to objectify or disguise splits and target specific groups for persecution.[69]

3.2 LEGAL IDENTITY, THE IDENTITY GAP AND IDENTITY SYSTEMS

Globally, every seventh person lacks proof of his or her legal identity[70]. Children and women from rural areas in Africa and Asia as well as the more than 21 million refugees and an estimated 20 to 30 million slaves of human trafficking are disproportionately affected by this problem.[71] Although identification is a component of many rights set out in the United Nations Declaration on Human Rights and the Convention of the Rights of the Child, and is a necessary means to access rights, entitlements, services and ensure political, economic and social inclusion for individuals, an estimated 1.1 billion people are not granted this right.[72] Moreover, it is likely that even more people, especially poor, indigenous, rural, female, refugee or marginalized human beings are undocumented.[73] This impact of lacking legal identification has been acknowledged by the international community, resulting in the establishment of Sustainable Development Goal (SDG) 16.9 relating to providing legal identity, including but not limited to birth registration, for each individual by 2030.[74] As there is no internationally recognised definition of an identity credential set to date[75], and to make this target more tangible, the development community – facilitated by the World Bank and the Center for Global Development – has established a set of principles that ID systems should meet. This entails providing individuals with an identity that is unique, secure, accurate and protecting user privacy.[76] Furthermore, considering the range of SDGs that prerequisites an ID, it is arguable that merely being in possession of an ID in principle is not sufficient. As the ID requirements for different humanitarian organisations and governments differ, this needs to be taken into consideration in order to overcome exclusion. This means that – against widespread contemporary standards – sustainable and robust identification should incorporate

[68] USAID, "Identity in a digital age", 4

[69] Ibid., 4-5

[70] The concept of ‚legal identity' will be explained in chapter 1.3

[71] World Bank Group, "The State of Identification Systems in Africa", 5; Pisa and Juden, "Blockchain and Development", 22

[72] Pisa and Juden, "Blockchain and development", 22

[73] Currently there is no comparable database that tracks legal ID enrollment other than that of the World Bank (coverage until 2016): https://datacatalog.worldbank.org/dataset/identification-development-global-dataset

[74] „Sustainable Development Goal 16.9". United Nations, accessed 21.02.2018. https://sustainabledevelopment.un.org/sdg16

[75] Mariana Dahan and Alan Gelb. "The role of identification in the post-2015 development agenda." World Bank Working Paper, 7 July 2015, accessed 9 May 2018, https://www.cgdev.org/sites/default/files/CGD-Essay-Dahan-Gelb-Role-Identification-Post-2015-ID4D_0.pdf, 8

[76] Pisa and Juden, "Blockchain and economic development", 22-24

an identity that goes beyond a traditional birth certificate.[77] Hence, in an attempt to address these principles and to close the "identity gap", ID experts are turning their focus from a 'centralized' and 'federated' system of identification to the development of a more 'user-centric' and ultimately 'self-sovereign' one. A *centralized* system solution refers to an identity that is established by means of centralized data, i.e. users must provide a set of personally identifying information such as a name, birthday, mother's maiden name, etc. to the organisation that operates a specific e-service. This information is linked to a user ID which is stored in that organisation's database. This often results in a nuisance for users who have various passwords for multiple websites and, more importantly, a huge security risk, as each database is a potential honeypot for hackers.[78] A *federated* system solution is an approach in which users provide identifying information to one authorizing entity, which in return can verify an identity to a number of websites or application. For example, logging in to Google or Facebook is relying on a federated solution. The user experience is simplified and privacy is enhanced, as personal information is only provided to one provider rather than multiple entities. Yet, this approach entails a key vulnerability, namely that an individual's data remains under control of an authorizing entity and tampering or deleting of this data will affect a user's ability to access other services, too.[79]

The aim of a more 'user-centric' and eventually 'self-sovereign' solution is to shift control to individuals by allowing them to "store their own identity data on their own devices [if possible], and provide it efficiently to those who need to validate it, without relying on a central repository of identity data".[80] In contrast to systems where ID credentials are provided by institutions, self-sovereign IDs are made to "empower individuals to control the formalisation of their identity, manage their digital personas and actively monetise their personal data."[81] This type of self-sovereign ID solution (in comparison to a centralized or federated one) was not perceived as being technically feasible in the past – until blockchain technology was put under the microscope.[82] However, before taking a closer look at self-sovereign blockchain-based identity systems, it is important to understand the basic concepts of a digital identity, its challenges and the rationale for looking at blockchain technology to

[77] Dahan and Gelb, "The role of identification in the post-2015 development agenda", 8

[78] Pisa and Juden, "Blockchain and economic development", 24-25

[79] Ibid.

[80] Antony Lewis. "A gentle introduction to self-sovereign identity." *Bits on blocks,* 17 May 2017, accessed 12 May 2018, https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

[81] GSMA, "Blockchain for Development", 12

[82] Beth Kewell et al., Richard Adams and Glenn Parry. "Blockchain for good?" *Strategic Change* 26, no.5 (2017): 429-437. Accessed 26 March 2018. https://doi.org/10.1002/jsc.2143; Paul Dunphy and Fabien Petitcolas. "A first look at identity management schemes on the blockchain." *IEEE Security & Privacy*, (to appear July 2018), accessed 23 March 2018, https://arxiv.org/pdf/1801.03294.pdf;

overcome these challenges. The following paragraphs provide an overview of digital identity and the use of digital identity systems in humanitarian aid.

3.3 Digital identity

Ex ante, a digital identity is a wide-ranging term with differing meanings according to differing contexts. The report 'The value of our digital identity'[83] by the Boston Consultancy Group defines a digital identity as "the sum of all digitally available data about an individual, irrespective of its degree of validity, its form, or its accessibility". Cyber-law lawyer Clare Sullivan describes digital identity as "an identity which is composed of information stored and transmitted in digital form."[84] Most commonly – and in the context of this thesis – digital identity refers to "a set of electronically captured and stored identity attributes that uniquely identify a person."[85] This typically consists of first name, last name, gender, date of birth and at least one piece of identifying information in the form of a signature or a numerical identifier. Importantly, one must not confuse digital identity with the means through which the service requiring identification is delivered, i.e. a user can physically attend the service provider location but affirm their identity through digital means of authentication (e.g. using a smart card or mobile device).[86] Consequently, the notion of *digital identity systems* refers to the processes and systems that manage the lifecycle of individual digital identities – similar to paper-based identification systems or, more specifically: any system where identification, authentication and authorisation of an individual are performed digitally.[87] A digital ID system can be viewed as a 'value chain' comprising of three phases, namely (a) *registration,* including enrolment and validation, (b) *issuance* of documents or credentials and (c) *authentication* and authorisation for service deliveries.[88]

[83] Boston Consultancy Group, "The value of our digital identity", Liberty Global, Inc. November 2012, Accessed 13 May 2018, https://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

[84] Stephen Saxby, "The 2013 CLSR-LSPI seminar on electronic identity: The global challenge - Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11-15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand." Computer Law and Security Review 30, 2 (2014): 112-125, accessed 12 May 2018, https://doi.org/10.1016/j.clsr.2014.01.007, 113

[85] Malik, Tariq and Anita Mittal, "Technical Standards for Digital Identity", International Bank for Reconstruction and Development / The World Bank, 2017, accessed 14 May 2018, http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf, 2

[86] Carly Nyst et al., "Digital Identity: Issue Analysis Executive Summary", Consult Hyperion, 27 July 2016, accessed 8 May 2018, http://www.chyp.com/, 9

[87] Ibid.

[88] Clark et al., "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation", *World Bank Group, GSMA and Secure Identity Alliance,* July 2016, accessed 20 March 2018,

Enrolment. This is the most important step of creating a digital identity, and may involve the process of capturing and recording key identity attributes, including biographic data (e.g. name, age, gender, address), biometric data (e.g. fingerprints, hand prints, iris scans) or other attributes related to this individual.

Validation. This data then has to be verified or validated by checking the presented attributes against existing data, and by establishing whether the claimed identity has the properties of *existence* (the person is alive and can be localised) and *uniqueness* (the person is unique in the database and the information provided is enough in order to prevent de-duplication, i.e. ensuring that a person is different from all other enrolled individuals).[89] These individual attributes are important for the enrolment phase of the digital ID value chain, also known as *identity proofing*, as they need to ensure a sufficiently unique and valid match to the individual over time.[90]

Issuance. After an individual has entrusted an institution or service provider with his or her personal data, and this institution/service provider has verified an individual's attributes, a credential, in the form of a Smartcard, 2D Bar Code card, Mobile Identity or ID in the cloud, for example, is issued to the person. In contrast to traditional forms of ID issuance (e.g. birth certificate or electronic IDs/Documents), the credentials or certificates of a *digital* ID must be electronic, i.e. data must be stored and communicated electronically.[91]

Authentication. After registration and issuance of credentials, digital identity can be used to demonstrate that the ID-issuing institution has accounted for the individual. This grants access to the associated benefits and services,[92] yet still requires authentication ("Are you who you claim to be?") by using a form of authentication 'token'. This can be a smartcard (which can also be used for offline digital authentication locations with limited connectivity because data is stored locally on a chip), mobile identity (using SIM cards or SMS-based authenticators) or ID in the cloud (relying on a computer or any other device with a biometric reader that connects to the cloud).

By implication many stakeholders with varying roles are involved in the processes of identification and authentication, depending on the type of the issued digital identity and the country or organisational context (foundational versus functional). Typically, individuals are

http://docplayer.net/62557738-Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation.html, 16

[89] Ibid., 18-19

[90] USAID, "Identity in a digital age", 9

[91] Clark et al., "Digital Identity", 18-19

[92] Ibid., 11

the primary end-users of an identity system, while government bodies, private firms or organisations are the main providers of digital identities and related services. In addition, public actors are responsible for regulation and public and private actors for standard setting and trust building.[93] In this digital identity 'ecosystem', there is yet another major stakeholder, namely donor agencies and development partners. Organisations such as UNICEF, UNHCR, UNDP, USAID, IOM, the World Bank and regional development banks and many others provide support in a number of ways, including but not limited to funding and technical assistance for the development of digital identity systems. Support can be aimed at strengthening a country's identity system in general or as a component of a specific program that requires identification (e.g., cash transfer programs, electoral campaign).[94] A donor organisation may also act as a provider of identity, authentication and services all at the same time, such as for example in a cash transfer program.

Having established the meaning, components and involved stakeholders related to digital identity in general, it is imperative to mention the role of digital identity in the humanitarian context, respectively that of humanitarian aid, for the purpose of this thesis.

3.4 Digital identity management systems in humanitarian aid

Humanitarian organisations require identification – and consequently identification services/identity systems – for a number of reasons, including streamlining humanitarian services and managing recipients' eligibility of benefits.[95] A lack of basic identity documentation therefore presents itself as a key challenge in humanitarian response and early recovery systems.[96] The actors who are behind funding and designing an identity system mostly (and importantly) do so within the context of a specific project, tailoring it to a particular unique environment in order to achieve the program objective.[97] Hence it seems valid to say that identity systems in the humanitarian context are more often than not of functional rather than foundational purpose.

A growing number of aid organisations including WFP, UNHCR and USAID have begun to reform existing identification systems and furthermore build new ones – including

[93] Clark et al., "Digital Identity", 22-24

[94] Ibid., 23-24

[95] USAID, "Identity in a digital age", 16

[96] ICRC Advisory Service on International Humanitarian Law, "Means of Personal Identification", accessed 5 February 2018, www.icrc.org/eng/assets/files/other/means_of_personal_id_eng.pdf

[97] USAID, "Identity in a digital age", 16

biometric identification[98], electronic credentials (smart cards and mobile IDs) and online authentication infrastructure in order to manage distribution more efficiently[99]. These innovations have the potential to leapfrog the shortcomings of paper-based identification systems – especially when in combination with associated digital technologies such as mobile payment systems. But at the same time, means of digital identification pose a number of challenges and shortcomings related to data protection and privacy, financial sustainability and the choice and use of different technology options.[100] Furthermore, understanding the components and interactions of a digital identity system is essential when thinking about its design – especially in regard to its vulnerabilities and the consequential implications on its end-users.

Digital ID systems in humanitarian aid have gained rapid adoption due to various reasons – including but not limited to: Improving aid distribution management by decreasing duplication, reducing fraud, simplifying monitoring and reporting processes, driving down (long-term) costs and reaching those entitled to benefits more reliably. Naturally, these factors are mainly encountered for in theory – in practice, outcomes will depend on various other factors than just the identity system. Improvement in terms of simplifying monitoring and reporting processes as well as reducing costs may, however, not necessarily improve the aid beneficiary's experience. Nonetheless, potential benefits of storing identification information digitally over paper-based storage can include the following: Rigging digital records in multiple databases is harder than getting hold of falsified paper documents, data on paper-based evidence is static compared to digital data where data history can be verified more easily, digital evidence can be sampled remotely and with greater accuracy, and in comparison to paper evidence, digital evidence can be forged or bought less easily.[101]

Enrolling everyone can be a challenge; people who live in remote areas can be marginalised within a society and/or pose a hard-to-reach group of people (e.g. elderly people, or second wives in a polygamous household). Hence *inclusion of a target population* – referring to the enrolment stage of the identity scheme – is one main functional goal.[102] This may involve mobile or women-only enrolment centers, as well as community collaboration to

[98] Biometrics can be defined as „any automatically measureable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual", (John Woodward, Nicholas Orlans and Higgins Peter. *Biometrics: Identity Assurance in the Information Age*. New York: McGraw-Hill Osborne Media, 2002.)

[99] USAID, "Identity in a digital age",19

[100] Malik and Mittal, "Technical Standards for Digital Identity", 1

[101] Geraint Price, "The benefits and drawbacks of using electronic identities", Information Security Technical Report 13, 2 (2008): 95-103. Accessed 26 March 2018, https://doi.org/10.1016/j.istr.2008.07.002, 96

[102] USAID, "Identity in a digital age", 19

include all eligible people. However, inclusion is more often than not just the first of more specific goals such as " […] inclusion in the ID system makes more data available. These data 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".[103] Essentially, digital identity systems are information systems about people, providing data to improve the design of programs to better address the needs of individuals or populations they serve. Identification data can thus be used to establish who is accessing services, where additional outreach is needed, which services are valued over others and so forth. One functional goal for the identity scheme is therefore to improve programming and service delivery efforts.[104] World Vision estimated that the introduction of their digital benefit distribution system resulted in cost savings of 15-40%,[105] while the World Food Programme (WFP) reported monthly savings of $1.5 million after introducing fingerprint verification in a Kenyan refugee camp.[106]

One of the ground-breaking technological innovations is *biometrics* used for identifying and authenticating an individual. Biometrics can be defined as "any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual."[107] Using biometrics for identity-related purposes cannot only enable individuals to authenticate themselves against a database rather than compel them to carry around a physical identity card, but furthermore improve accuracy and security, facilitate fast data processing and collection and create verifiable transaction records – all of which has the potential to aid development planning, improve service delivery and prevent fraud.[108] Consequently, biometric identification technology – respectively, advanced human recognition (AHR) – has gained increased application in the humanitarian sector, offering the most accurate tool available for identification and authentication.

Biometric technology has reinforced a range of efforts to improve identification (among other benefits including democratic participation and service deliver) in the

[103] Ibid.

[104] Ibid., 20

[105] Keith Chibafa, "Why not digital? Technology as an interagency tool in the Central African Republic", Humanitarian Practice Network at ODI, *Humanitarian Exchange 62,* (September 2014): 19-21, accessed 18 March 2018, https://odihpn.org/magazine/why-not-digital-technology-as-an-interagency-tool-in-the-central-african-republic/

[106] World Food Programme, "WFP and Digital Innovation", October 2016, accessed 12 May 2018. http://documents.wfp.org/stellent/groups/public/documents/communications/wfp287655.pdf

[107] Woodward, et al., *Biometrics: Identity Assurance in the Information Age*. New York: McGraw-Hill Osborne Media, 2002, 27

[108] Gelb and Clark, "Identification for development", 9

developing world. Gelb and Clark estimate that worldwide projects with the aim of improving pension management, reducing fraud and corruption in the civil service, creating new voter rolls, providing health services, verifying teacher attendance, and improving cash and in-kind transfers have biometrically enrolled over one billion people in low and middle-income countries.[109] However, one needs to keep in mind that even though institutions benefit from improved technology, individual's experience may not automatically be enhanced. The use of iris-scanners on refugees, for example, can work well if it is integrated within cultural practices, but it can also further stigmatise a refugee population if they have to share biometric information and the resident population is excepted from this. Receiving aid may be tied to providing biometric data or interfacing with technologies of international aid organisations they may not feel comfortable with – or flat out do not trust.[110] For many Syrian refugees in Jordan, for example, discretion about revealing personal information online is a very sensitive matter. Phone calls are monitored and emails and texts are read in Syria to this day; personal information revealed online can lead to devastating consequences, such as imprisonment or forced disappearance. Biometric registration with UNHCR thus prompts mixed feelings among the Syrian refugee population. Some worry that the information provided may somehow wind up in the hands of the Syrian government, its secret police or the Hezbollah fighting alongside the Syrian military – or even that international NGOs are potentially and/or unintentionally working for the interests of certain governments.[111]

Returning to the institutional efficiency of digital identity systems: The concepts of *transparency* and *accountability* can also be enhanced, as digital enrolment of individuals generates a digital 'paper trail' of information linking them to unique entries in digital databases (e.g. transactions). This data offers more transparency about the program registration, distribution of resources and delivery of services – and in turn may promote greater accountability. This is especially the case when data is accessible to numerous actors, making it harder to nebulise.[112] Digitising voter records in developing democracies is an example where digital registration systems is a means to promote transparency, promote accountability and build trust. Technology implies objectivity, neutrality and hence trust – which, however, does not mean that fraud is impossible.

[109] Ibid., 19

[110] Katja Jacobsen, "On humanitarian refugee biometrics and new forms of intervention", *Journal of Intervention and Statebuilding* 11, no.4 (2017): 529-551, accessed 26 March 2018, DOI: https://doi.org/10.1080/17502977.2017.1347856

[111] Rachel Townzen. "Trusting Tech Initiatives isn't Easy for Most Syrians." News Deeply, 21 September 2016, accessed 23 March 2018, http://pulitzercenter.org/reporting/trusting-tech-initiatives-isnt-easy-most-syrians

[112] USAID, "Identity in a digital age", 21

And yet, as with every technological innovation, building (digital) identity systems does not come without a number of challenges and drawbacks, including issues related to data protection, privacy, cost, sustainability, political complexity and lack of an up-to-date legal framework.[113]

3.5 Challenges of digital identity management systems in humanitarian aid

This and the subsequent section addresses challenges of currently widespread digital identity systems and consequently leads to the first sub question *What is the rationale of using blockchain technology rather than systems that have been around longer for identity management in humanitarian aid?* Although answers to this sub question are explored in chapter 4, the following paragraphs of this sub chapter provide an outline of the issue at hand, leading up to the rationale of blockchain-application.

The challenges can be divided into technical and non-technical aspects, i.e. the technical challenges from a system's design perspective versus issues related to logistics, interoperability, sustainability and fragmentation of a digital identity system.

Most current identity management systems are based on a centralised or federated model.[114] These models are increasingly challenged as a result of regular data breaches, identity fraud and, most of all, a loss of privacy for end-users.[115] Threats, vulnerabilities and limitations of a digital identity management system fall into one of the three broader categories:

- *Confidentiality of the identity management system* (threats to the privacy of the end-user)
- *Integrity of the identity management system* (alteration or theft of personal data on the identity management system by an unauthorised party)
- *Availability of the identity management system* (related to the service, i.e. by means of disruption of the enrolment or the later provision of related services)[116]

Consequently the list of vulnerabilities that may arise in a digital identity system include (but are not limited to): unnecessary data collection, linkable identifiers, lack of blinding information, lack of pseudoanonymisation, lack of transparency in regard to data collection, implicit data collection where an individual is unaware of collected data etc.[117] These

[113] Clark et al., "Digital identity", 14
[114] Malik and Mittal, "Technical standards for digital identity."
[115] Ibid., 1
[116] Nyst et al., "Digital identity", 32-33
[117] Ibid., 32-38

vulnerabilities can be facilitated either by means of a) *malicious threats* such as unlawful disruption of a digital identity service, undermining its integrity or that of an individual's privacy, e.g. data breach, identity theft, individual or mass surveillance, b) through *legitimate business that upholds legal business practices* but possibly compromise the privacy of a person's information, including the repurposing of data, the passing of personal data with a user's consent to unvetted parties, publication of personal data, or c) *negligence or incompetence of those responsible for the identity service provision*, such as poor operation processes or poor operational security as well as failure to keep up with the changing security landscape. These incidents illuminate a lack of control and ownership for holders of digital identities.[118]

Leakage of personally identifiable data is especially critical in sensitive contexts than can result in discrimination, exclusionary policies or the sparking of targeted violence. Even without specific identification of individuals, discriminatory policies may be established based on data that has been leaked or stolen from a centralised database.[119] Although there is a growing consideration of how to limit data harm among various organisations – including the ICRC[120] and World Vision[121] – only so much can be done to protect sensitive data if the system itself is vulnerable.

Apart from drawbacks from a system design perspective, there are also non-technical challenges of current digital identity/registration systems, namely those of logistics, fragmentation and sustainability.

In many cases, the registration process of a humanitarian organisation is very time-consuming – independent of the purpose, i.e. voter registration or beneficiary registration of a CTP. If, however, these registration drives are limited to record people for a single election or CTP cycle, and databases are not maintained from one election or CTP cycle to another, the process must be repeated, thus resulting in duplicative costs, as many of the same people must be re-registered each time.[122]

Furthermore, identity/registration systems are, many a time, subject to pressure by technology vendors in charge of supplying components of the identity system. Vendors

[118] Dunphy and Petitcolas, "A first look at identity management schemes on the blockchain" 1

[119] "Secret aid worker: we don't take data protection of vulnerable people seriously", *The Guardian,* accessed 20 May 2018, https://www.theguardian.com/global-development-professionals-network/2017/jun/13/secret-aid-worker-we-dont-take-data-protection-of-vulnerable-people-seriously

[120] Christopher Kuner and Massimo Marelli, *ICRC Handbook on Data Protection in Humanitarian Action*, Geneva: ICRC, 2017, accessed 20 May 2018, https://www.privacy-web.nl/cms/files/2017-07/handbook-data-protection-and-humanitarian-action-2-.pdf

[121] Al Lutz et al., "Data protection, privacy and security for humanitarian and development programs", World Vision, Discussion Paper, 2017, accessed 18 May 2018, http://wvi.org/health/ict4d

[122] USAID, "Identity in a digital age", 26

currently more often than not use proprietary software for identity/registration management. Compared to open-source solutions, reliance on proprietary solutions results firstly in dependence on a specific vendor and secondly in repeated investments and increased costs, as proprietary systems often cannot be reused. Similarly, tight and inflexible project timelines limit the design of systems that are context-sensitive as well as compatible across various programs.[123] "Without deliberate efforts to collaborate and develop relationships, the default approach is to use a system that will most quickly meet the needs of a single program. This typically means working independently and building project-specific ID systems."[124] In the case of humanitarian aid, when deployed in quickly worsening crises, this is particularly acute.

Fragmentation and sustainability of digital identity/registration systems intrinsically tied to *interoperability* of humanitarian organisations. Most organisations build their own registration/identity system rather than cooperate with each other to share resources. Naturally, coordination and adoption of a registration/identity system is not always applicable and suitable, as they may contain features tailored for a specific program. Nevertheless, in many cases, an interoperable solution could mitigate fragmentation and foster sustainability.[125] Implicit within interoperability is firstly inter-organisational trust and secondly relinquishing traditional notions of power and control. Not all humanitarian organisations are open for collaboration, especially in regard to data sharing. This is mainly a result of a lack of universal data responsibility protection standards.[126] Although some organisations are taking first steps to initiate collaboration – for example the World Food Programme's data privacy guidelines[127] or recommendations on harmonising ID requirements related to humanitarian CTP's by the Cash Learning Partnership (CALP)[128] –, stark inter-organisational hesitancy remains. Secondly, humanitarian actors acknowledge that the current humanitarian system needs greater collaboration, which is likely to result in "more human, procedural and technical compatibility across organisational boundaries, an embracing of diversity, alignment around common values, a quicker and more complimentary humanitarian financing architecture, a realignment of aid investment into local response

[123] Ibid., 33

[124] Ibid., 33

[125] Ibid., 35

[126] Personal notes from interviews

[127] World Food Programme. "WFP and Digital Innovation."

[128] Levin Avner et al. "Know your customer standards and privacy recommendations for cash transfers. Enhanced Response Capacity Project 2014-2015, UNHCR and World Vision, April 2015, accessed 15 April 2018, http://www.cashlearning.org/downloads/erc-know-your-customer-web.pdf

capacity […] and the suppression of organisational ego in favour of the greater endeavour for humanity.”

However, the feasibility hinges on traditional power holders in the system. If these traditional powers holders are indeed willing to accept this shift of power, i.e. distribution of control among a number of organisations or not, remains unanswered despite the talk of transformation.[129]

These non-negligible drawbacks of current digital identity management systems have led governments, NGOs and private organisations to explore alternative approaches and models of digital identity management systems, seeking to enhance data privacy, trustworthiness, reach and sustainability of digital identities.[130] Prioritising long-term goals of registration increases the opportunity to develop safer and more sustainable systems – for end-users as well as implementing humanitarian organisations.[131]

As the scope of this thesis does not allow for an adequate analysis of multiple innovations of digital identity management, the focus is set on one of the potential approaches, namely blockchain technology. The rationale behind looking at blockchain technology for identity management is mainly due to its promising and innovative characteristics that address many of the identity-attributed challenges. At the same time, its uncharted use in identity management and, more significantly, the humanitarian aid sector provides another strong rationale for careful evaluation.

4. Blockchain technology for identity management

What is the rationale of using blockchain technology rather than systems that have been around longer for identity management? – This question was posed as one of the sub questions in the beginning of this thesis. Chapters 2 and 3 provided detailed information on the current, commonly used identity-for-registration-systems and its respective challenges and limitations. The following and the subsequent chapter will provide support for the rationale of considering blockchain deployment for beneficiary registration and identity management.

[129] UNOCHA 2014 ECOSOC Humanitarian Affairs Segment. Side-event on Interoperability, Panel note led by the Permanent Mission of Turkey, 25 June 2014, accessed 17 April 2018, https://www.unocha.org/sites/unocha/files/dms/Documents/HAS%20Interoperability%20Side-Event%2024%20JUNE%202014%20FINAL.pdf

[130] Thomas Smedinghoff, “Solving the legal challenges of trustworthy online identity.” Information Security Technical Report 28, 2 (2012): 532-541, accessed 9 May 2018, https://doi.org/10.1016/j.clsr.2012.07.001, 532; Dunphy and Petitcolas, “A first look at identity management schemes on the blockchain”, 1

[131] USAID, “Identity in a digital age”, 26

While blockchain innovation has acted mainly as a new disrupter to financial services for the past ten years, initiating an increasing impact on banks in terms of risk and associated benefits[132], attention is now beginning to shift toward the appropriation of social and environmental use cases that aim to tackle global challenges.[133] With limited understanding and little consensus about the potential social, ethical and legal impact of blockchain innovation on global challenges, it is apparent that serious analysis of this technology is required.[134] However, before immerging into the academic and practitioners' debate on a blockchain-based approach to identity management, a clear understanding of this disruptive technology is needed. The following paragraphs provide a brief overview of blockchain's promising and innovative features in general and, more specifically, in the use of identity management by means of a literature review.

4.1 What is blockchain technology?

Fundamentally, a blockchain is a shared database, or a so-called *distributed ledger* allowing for information to be recorded (but not altered or erased) and shared between numerous entities.[135] This distributed ledger contains a chain of information 'blocks', each block being identified by a cryptographic signature, making the exchanged information transparent.[136] Blockchains can be seen as independent digital document sharing platforms, distributed across a network of computers, where all participants within the blockchain network are given equal status to submit, review and verify records and transactions (or 'blocks' of information) in real time. It is thus a *decentralised* scheme, with no single authority holding ownership over the 'database'. However, unlike online document sharing platforms, blockchains are *immutable,* hence ensuring the integrity of blockchain-stored data.[137] Once a 'block' of information is added and accepted by the network – may this be a financial transaction, a record of a farmer's land ownership or a person's identifying details – it is given a time-stamp

[132] Commonwealth Partnership for Technology Management (CPTM), "Adaptive flexibility approaches to financial inclusion in a digital age." Smart Partners Hub, 6 October 2016, accessed 30 April 2018, http://www.cptm.org/documents/CFMM_Brief_%202016.pdf, 23

[133] Kewell, Beth, Richard Adams and Glenn Parry. "Blockchain for good?" *Strategic Change* 26, no.5 (2017): 429-437, accessed 26 March 2018, https://doi.org/10.1002/jsc.2143, 429

[134] Ibid., 431

[135] Lana Swartz, "Blockchain dreams: imagining techno-economic alternatives after Bitcoin", In *Another economy is possible: culture and economy in a time of crisis,* ed. by Manuel Castells et al., 82-105. (Malden: Polity, 2017), 83, http://llaannaa.com/papers/Swartz_Blockchain_Dreams.pdf

[136] Ori Jacobovitz, "Blockchain for identity management", Technical Report, The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel, 11 December 2016, accessed 15 March 2018, https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf

[137] Kewell, Adams and Parry, "Blockchain for good?", 431

and cannot be altered.[138] Additionally, some blockchains have implemented secure transactions (e.g. Qorum) in the sense that the information it stores is confidentiality-protected by public key cryptography. This 'key' system can be compared to the two-key system used for safety deposit boxes; one key is kept privately and enables the user to 'lock' or 'unlock' their personal information (e.g. a PIN or password) and to control who has access to this information as to when and to what extent, while the 'public key' can be given to a trusted party in the network (e.g. a bank, an international aid organisation) in order to read and double-check the unlocked information necessary for a specific service.[139]

Blockchains are designed to be public *(permissionless)* or private *(permissioned)* – depending on their purpose –, resulting in differing distributed ledger technology design architectures.[140] As such, blockchains come in multiple types; the original Bitcoin blockchain being the most well-known albeit not the only one. A number of independent blockchains have been developed in recent years, such as for example Ethereum, Litecoin and Ripple Transaction Protocol, to mention just a few.[141] A permissionless blockchain is sometimes seen as the 'pure' form, containing a network of participants unknown to each other yet with equal access to read, write and validate information on the blockchain and participate in the consensus process.[142] An often-cited advantage (and equally often omitted drawback) of a permissionless blockchain is that information contained on the blockchain cannot be controlled by an individual or a group of individuals – thus maintaining its original characteristic of neutrality. However, this neutrality can only be assured as long as an individual or group controls less than half of the participants. Public blockchains can be an esteemed facilitating tool in supply chain management; tracking movements of assets, thus improving transparency and hindering fraud.[143] A permissioned, or private blockchain, on the other hand, is operated by a single organisation or multiple organisations, where only authorised parties may access information on the blockchain, and consensus process is usually

[138] GDSM, "Blockchain for Development", 4-5

[139] Ibid., 6-7

[140] Juri Mattila, "The blockchain phenomenon – The disruptive potential of distributed architectures." ETLA Working Papers No.38, 10 May 2016, accessed 15 March 2018, https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-38.pdf

[141] Deloitte, "Blockchain – Enigma. Paradox. Opportunity.", Deloitte University Press, 2016, Accessed 17 March 2018 https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf 6

[142] Kewell, Adams and Parry, "Blockchain for good?", 432

[143] GSMA, "Blockchain for development", 6

carried out by trusted actors of the network (where relationships are governed by formal contracts or confidentiality agreements).[144]

Centralised organisations, including humanitarian ones, are increasingly beginning to investigate how blockchain technology can be used to collaborate with partner agencies and/or improve their internal processes – so-called 'incorporative' blockchain projects.[145] The advantages of a private blockchain include the following: They can be designed with a specific functionality in mind, they can be more efficient and faster than public versions (offering alternative validation incentives to purely economic ones), [146] and they are particularly beneficial when organisations want to preserve confidentiality of the information they store on the blockchain.[147] For example, in line with the UN SDG 16.9, Accenture, Microsoft and Avanade are building a permissioned blockchain which brings together already existing record-storing systems from public and private institutions into one database. As a result, individuals have a set of portable personal credentials that have been validated by a number of trusted entities, such as, for example, in the case of a refugee; voter documents provided by electoral commissions, birth registration data issued from UNICEF, refugee registration data from UNHCR and medical records from Doctors without Borders (MSF). An aid-seeking refugee arriving at a border could potentially make use of this information stored on the blockchain to prove his or her origin of a conflict-stricken area or his or her need for medical assistance.[148] However, considering that centralised intermediaries are inevitably part of a public blockchain, it is debatable to which extent these blockchain projects are still fully peer-to-peer and to what extent security, immutability and censorship-resistance is compromised.[149]

4.2 LITERATURE REVIEW ON MANAGING DIGITAL IDENTITY ON THE BLOCKCHAIN

Undoubtedly, identity management, i.e. the provision of digital identities, is one of the fields in which blockchain-approaches aim to upend existing dominant approaches. Although advances in this field date only a few years back, a small body of recent academic literature as well as white papers and organisational reports has been composed. As the existing literature

[144] CPTM, "Adaptive flexibility approaches to financial inclusion in a digital age."
[145] GSMA, "Blockchain for development", 6
[146] Kewell, Adams and Parry, "Blockchain for good?", 432
[147] GSMA, "Blockchain for development", 7
[148] Jeff Roberts, "Microsoft and Accenture Unveil Global ID System for Refugees." *Fortune*, 19 June 2017, accessed 10 March 2018, http://fortune.com/2017/06/19/id2020-blockchain-microsoft/; GSMA, "Blockchain for development", 7
[149] Mattila, "The blockchain phenomenon"; GSMA "Blockchain for development", 6; Kewell, Adams and Parry, "Blockchain for good?", 432

on blockchain-based identity management systems is very small at the time of research, there will be no division of literature according to specific use cases, i.e. government-based identity management systems versus humanitarian identity management systems. Instead, the following paragraphs discuss the benefits and drawbacks of blockchain for identity *in general*, according to the revealed trend in the field and the issues connecting the multiple sources. The literature has a twofold purpose: Firstly, to identify the knowledge gap within the blockchain-based identity management literature body and secondly, to address the remaining two of the three sub questions posed at the beginning of the thesis: *Is blockchain technology better at addressing problems of identity management than existing approaches and technologies?* And: *What are the challenges of using blockchain technology for identity management and what new risks might it create for the beneficiaries of a cash transfer program?* The following paragraphs will outline focal points of identity being managed on a decentralised ledger, clearly distinguishing the gains as well as the drawbacks and risks of the technology in this case.

Much of the literature dealing with distributed ledger technology for identity management focuses on the aptitude of the *decentralised architecture* of blockchain technology in comparison to centralised identity management systems. Wolfond Greg claims that public and private sector organisations have employed multiple identity management solutions – most of them relying on federated authentication provided by a centralised broker architecture. While these solutions indeed provide great utility for the end-users, allowing them to provide their identity data claims using already trusted third-party credentials (e.g. banks), they also pose various security and privacy limitations. These limitations are caused largely by the principles of their centralised design. Wolfond emphasises that a decentralised model based on blockchain is needed in order to meet necessary privacy and data integrity goals. This model would reduce reliance on a single point of trust and failure while at the same time prevent any single entity from tracking a user's data, prevent data mining and maintain a verifiable und unalterable trail.[150] The authors Dunphy and Petitcolas[151] affirm Wolfond's opinion; illustrating how centralised identity management models operated by a single entity increasingly face data breaches, which lead to identity fraud, loss of privacy for users and to reputational damage. Moving from a centralised to a decentralised network could

[150] Greg Wolfond, "A Blockchain ecosystem for digital identity: Improving services delivery in Canada's public and private sectors", *Technology Innovation Management Review* 7, no.10: 35-40, accessed 12 March 2018, http://doi.org/10.22215/timreview/1112

[151] Dunphy and Petitcolas, "A first Look at Identity Management Schemes on the Blockchain."

strengthen the security of personal data, as it significantly lowers the risk of a mass data security breach, according to the author Juri Mattila.[152] Kewell, Adams and Parry further allege that a decentralised characteristic of identity management schemes is likely to ease the problem of "identitylessness". Rather than having a person's identity authenticated by some authority, blockchain technology application can facilitate a gradual accumulation of different attributes of identity, thus allowing for a bottom up approach. As a result, an individual's identity is not under the control of any unique authority, nor is it vulnerable to tampering from potentially malicious third parties.[153] Jacobovitz states that although digital identity authentication may appear to be an intractable difficulty without overseeing global entity – compared to a government-issued physical identity – blockchain technology may ease this concern by presenting a secure and feasible solution without the need for a trusted, central authority.[154]

However, the praised decentralised character of blockchain technology also gets challenged, for example by the authors Dunphy and Petitcolas, who point out that blockchain technology is often seen as a silver bullet for system architectures dominated by intermediaries and central authorities, while in reality the role of centralisation and intermediaries is often simply *reshaped* rather than eradicated. Especially in the case of permissioned blockchain projects, such as, for example, uPort (relies on central authorities to provide trusted identity attributes) or ShoCard, which acts as an intermediary storing encrypted identity attributes and further mediates between end-users and relying parties. The authors further challenge the negatively connoted concept of an intermediary or central authority. They see the research challenge of blockchain-based identity management in finding a balance between centralisation and decentralisation in order to create interoperable and privacy-respecting identity systems that do not place too much trust in a single authority.

Literature highlights that perceived weaknesses of centralised and federated identity management solutions provoke the desire for *control over personal data*, *increased data security*, and *improved privacy protection*.

The authors Zyskind, Nathan and Pentland affirm that a decentralised blockchain-based identity system not only enables individuals to prove their identity, but moreover also allows them to *own* and *control* their data. In line with this, Jacobovitz's technical report provides a list of organisations and projects which are currently using or exploring means of blockchain

[152] Mattila, "The Blockchain Phenomenon."
[153] Kewell, Adams and Parry, "Blockchain for good?", 2017
[154] Jacobovitz, "Blockchain for Identity Management", 2016

for identity management, arguing by means of these use cases that individuals have the ability to create and manage their own digital identities through the distributed ledger technology, offering them greater control over their personal data.[155] Indeed, Dunphy and Petitcolas state that regular data breaches and, consequently, the loss of privacy of centralised models of identity management highlight a lack of control and ownership that end-users undergo with their digital identities. Identity management on the blockchain, on the other hand, enables a user-centric approach, placing administration and control of personal identity information in the hands of the individuals.[156] The authors of the GSMA[157] and the Sustania[158] reports further accentuate that control over personal identity information is enabled on the blockchain through public and private key cryptography, where an individual can control which data to share with whom. This ability to selectively share personal information, i.e. the so-called *secure blinded infrastructure* enabled through "privacy-by-design" is a blockchain characteristic that other authors praise, too. Privacy-by-design – also known as "zero-knowledge-proof" – is the cryptographic technique behind the idea of selectively sharing personal information, allowing an identity attribute claim to be made without the need to share any additional data other than the explicit identity attribute in question.[159] Notably, Pisa and Juden propose that individuals use a digital wallet on a blockchain to store identifying attributes from trusted authorities. In this way, a person can select which of these identifying attributes he or she wants to share with a service provider (depending on the specific information this provider needs) without having to share additional information.[160] Thus, receiving medical assistance in a health center would require only revealing one's medical records, but not, for example, one's religious affiliation, address or place of birth. In practice, Augot et al. introduce a schema of identity management on the Bitcoin blockchain, assuring that users are able to disclose selective elements of their identity, which is in line with the idea that only necessary information about an individual should be accessible publicly.[161] In a nutshell: A user-centric identity management system translates into a 'self-sovereign' identity management system. Christopher Allen explains 'self-sovereign identity' as a concept in

[155] Jacobovitz, "Blockchain for identity management."

[156] Dunphy and Petitcolas, "A first look at identity management schemes on the blockchain."

[157] GSMA, "Blockchain for Development."

[158] Sustainia, "Hack the Future of Development Aid", Sustainia, The Danish Ministry of Foreign Affairs and Coinify, 2016, accessed 12 March 2018, https://reliefweb.int/report/world/hack-future-development-aid

[159] Nyst et al. "Digital identity", 17

[160] Pisa and Juden, "Blockchain and Economic Development."

[161] Daniel Augot et al.. "Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain", Cornell University Library, 9 October 2017, accessed 14 March 2018, https://arxiv.org/abs/1710.02951

which trust is enabled without compromising individual privacy.[162] Wolfond emphasises that current non-blockchain identity systems do not support self-sovereignty, relying instead on processes, methods and physical identity documents that do not allow for trusted third parties to add identifying attributes to a person's identity nor for a person to safely authenticate themselves and interact with online services.[163] The authors Al-Saqaf and Seidler, on the other hand, call for precaution, stating that while blockchain technology indeed holds a lot of potential for self-sovereign identity, it is imperative to remember that "this is a domain where there are challenges, including the extent to which personal information would be exposed and possibly subject to attacks".[164]

Incorporated in the concept of a self-sovereign identity is not only control over personal data, but moreover also improved *data security* and *privacy protection*. Greg Wolfond argues that digital identity based on blockchain may help combat rising rates of cyber-fraud and cybercrime in relation to digital transactions and identity theft.[165] A report by Deloitte highlights that although no technology to this day is downright secure, "no one has yet managed to break the encryption and decentralised architecture of a blockchain."[166] An article by Ron Miller citing 'blockchain experts' on the potential of the distributed ledger technology in relation to identity management reveals mixed opinions on the matter. While Jerry Cuomo, IBM Fellow and VP of blockchain technologies sees the technology already demonstrating a large impact in regard to self-sovereignty of identity management, Eve Maler (VP of innovation and emerging technology at the identity management firm ForgeRock) sees hardly any potential in blockchain-based identity management. She believes that placing personal identity information on a public permissionless blockchain results in increased attack surface, i.e. that the distributed element of the technology is not appropriate when recording sensitive information and rather results in increased privacy considerations.[167]

Another recurring theme in literature is the notion of *interoperability* that authors perceive as an added value (and to a certain extent also as a key challenge) of blockchain-based identity management systems. The authors Ko and Verity believe that blockchain can

[162] Christopher Allen, "The Path to Self-Sovereign Identity." Life with Alacitry. 25 April 2016, accessed 15 March 2018, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[163] Wolfond, 2017
[164] Walid Al-Saqaf and Nicolas Seidler. "Blockchain technology for social impact." *Journal of Cyber Policy* 2 (2017): 338-354, accessed 12 March 2018, https://doi.org/10.1080/23738871.2017.1400084
[165] Wolfond, "A blockchain ecosystem for digital identity."
[166] Deloitte, "Blockchain – Enigma. Paradox. Opportunity."
[167] Ron Miller, "The Promise of managing identity on the Blockchain." *Techcrunch*, 10 September 2017, accessed 17 March 2018, https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/

greatly address one of the key barriers in humanitarian information management, namely information silos between multiple humanitarian actors. Providing a data sharing information marketplace on the blockchain that is accessible to all involved users and, at the same time, ensures data protection can transcend barriers of unreliable information and information silos between different humanitarian stakeholders. In addition, combining time-stamped and digitally verified information hosted on an accessible ledger could contribute to an increase of transparency of humanitarian data and a decrease of related costs. With the advent of big data in humanitarian response, blockchain's distributed nature makes it possible to have different humanitarian actors being able to collect, share and add data on the same network.[168] In endorsement, author Mattila avers that blockchain-based technology for identity verification allows for a more standardised documentation of identity, which again can be used across multiple services.[169] In contrast to the other authors, the GSMA report sees interoperability as a challenge, as self-sovereign identity systems will require willingness from governments, organisations and other service providers to share sensitive data outside their internal and trusted silos. The report mentions its hope that the transparency, security and trust elements offered by blockchain "will remove any remaining excuses organisations might have for avoiding collaboration and data-sharing, helping the sector move from an 'organizational focus' to an 'issue focus'" – however, the risk remains that permissioned blockchains will foster the fragmentation of identity management by keeping data and knowledge trapped in organisational silos.[170] Similarly, Nir Kshetri sees interoperability, or moreover the agreeing on common standards for an invoicing platform and common messaging standards between multiple agencies as a key challenge.[171] Furthermore, the question of controlling access and accountability has not yet been tackled in this regard, i.e. who controls access to this data? And who is responsible for this data in an interoperable system involving numerous stakeholders?

Contradictions in the literature are also visible regarding *costs* of blockchain-based identity management. According to Wolfond, high registration costs coupled with privacy and security risks, together with low convenience processes for users, are the result of today's inefficient identity-verification methods. Hundreds of millions of dollars per year could be

[168] Ko and Verity, "Blockchain for the humanitarian sector."
[169] Mattila, "The blockchain phenomenon."
[170] GSMA, "Blockchain for development."
[171] Nir Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the Global South?" *Third World Quarterly 3*8, no.8 (2017): 1710-1732, accessed 11 March 2018, https://doi.org/10.1080/01436597.2017.1298438

saved through increased identity management efficiencies – password management costs ranging in the millions alone could be optimised with a shift from legacy to blockchain-based identity management systems.[172] This conclusion is shared only partly with the report by Deloitte and by the author Nir Kshetri, which uncover the cost-related concern of high energy consumption, resulting in high aggregate costs caused by the speed and effectiveness of blockchain-based information transactions. Kshetri illustrates that writing data in a blockchain results in exceedingly high consumption of electricity and use of computing power.[173] This is due to the burden of proof-of-work (PoW) consensus. PoW refers to repeated calculations, that is, hashing, to solve a complex computer calculation (also known as 'mining'). This is necessary to validate the legitimacy of the transaction and then create a new block (i.e. trustless transactions) on the distributed ledger. In essence this means that firstly, transactions are grouped together in a so-called 'block', secondly, miners (i.e. nodes of systems) solve a mathematical puzzle (the so-called proof-of-work problem) to verify the legimitacy of the transaction. As this is a timely and costly endeavour, miners are incentivised to taking on the burden of the work by receiving a reward – whichever miner solves the puzzle first receives a reward paid in cryptocurrency.[174] The PoW mechanism presupposes that a number of miners work on the same computational puzzle at the same time, thus resulting in high energy consumption. This being said, there is an alternative means to PoW to validate transactions on the blockchain that needs less energy, namely by means of proof-of-stake (PoS). As the name suggests, PoS relies on the stake, i.e. the wealth in form of cryptocurrency coins someone holds in the network, rather than on calculating power. The more coins a validator (equivalent to a miner in PoW) has, the more possibilities to 'validate' (rather than 'mine' as in PoW). The rationale behind this approach is that "entities who hold stake in the system are well-suited to maintain its security, since their stake will diminish in value when the security of the system erodes."[175] The main difference between PoW and PoS is that in PoS the "creator of a new block is chosen in a deterministic way, depending on the respective stake", i.e. wealth.[176] The reward comes in form of transaction fees rather than in form of a block reward. Overall, PoS needs a significantly smaller amount of energy/electricity to secure a blockchain and is,

[172] Wolfond, "A blockchain ecosystem for digital identity."

[173] Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the Global South?"

[174] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, accessed 5 June 2018, https://bitcoin.org/bitcoin.pdf

[175] Bentov, Iddo et al., "cryptocurrencies without proof of work", *arXiv*, 22 June 2014, accessed 9 June 2018, https://arxiv.org/abs/1406.5694, 1

[176] "Proof of work vs proof of stake: basic mining guide", *Blockgeeks*, accessed 10 June 2018, https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

consequently, less costly.[177] And yet, costs and disadvantages related to security, energy consumption and risk of centralisation aside, PoW and PoS mechanism nonetheless raise a paradox and a number of ethical questions in regard to the nature of the technology's decentralisation. In practice, the supposedly decentralised system could be viewed as biased in favour of miners with more computational power (in PoW) or more coins (in PoS).[178] Participants with more computational power or more cryptocurrency tokens profit disproportionately from mining – due to the fact that rewards are not given to miners proportional to computational resources, which this results in an unbalanced reward allocation.[179] If, in essence, power over the network is tied to wealth (in form of computational power or cryptocurrency tokens), this means that those with computational power/excess capital in forms of coins can set the rules, which leads to a centralisation of the system.[180]

In relation to humanitarian aid, a number of authors also touch upon the element of *inclusiveness* when relating blockchain technology to identity management. The scholars Kewell, Adams and Parry[181] as well as the authors of the GSMA[182] report affirm that individuals originating from vulnerable, poor or disconnected society segments may never have access to government-issued identity documents, due to a number of reasons: The government lacks the capacity or will to issue legal identification documents to its citizens, the application and registration process is too costly or inconvenient or an individual is considered to be stateless. A bottom-up digital identity composed of multiple attributes compiled by bits of identifying information of third parties and stored on the blockchain may provide a viable solution for many "identityless" individuals.

As with every technology, blockchain is also a double-edged sword – containing promising and concerning characteristics. Alongside the favourable prospects of blockchain-based identity management, a number of concerns and limitations have been raised by the same authors, mainly regarding user experience, legal and regulatory challenges as well as general concerns regarding the novelty of the technology (especially when applied in the humanitarian context).

[177] Ibid.
[178] Yonatan Sompolinsky and Aviv Zohar, "Bitcoin's underlying incentives", *acmqueue* 15, no.5 (2017): 1-24, https://queue.acm.org/detail.cfm?id=3168362, 8
[179] Ibid.
[180] Lana Swartz, "Blockchain dreams: imagining techno-economic alternatives after Bitcoin", 91-92
[181] Kewell, Adams and Parry, "Blockchain for good?"
[182] GSMA, "Blockchain for development."

One of the main areas of concern relates to *user experience* and *usability*. The Deloitte report discusses how blockchain represents a complete shift away from traditional ways of doing things, not only for industries and individuals used to significant digital technology transformations, but even more so for digitally inexperienced users. Trust and authority are placed in a decentralised intricate network rather than a known and tangible central institution. This loss of control can be deeply unsettling and unnerving.[183] Dunphy and Petitcolas exhort that there is a noticeable lack of contextual understanding of user experience of blockchain-based identity management schemes. According to the scholars, "usability is a particular pressing unknown since there appears to be a widespread assumption that users are equipped to conduct effective cryptographic key management, and would intuitively understand the implications of referencing identity data or attributes in a DLT [distributed ledger technology, i.e. blockchain]."[184] Similarly, Ko and Verity mention technical barriers in understanding the complex composition of blockchain technology, i.e. apart from access to the Internet, the digital divide also extends to those who understand how to navigate securely in the Internet – and those who do not. In addition, more appropriate and user-friendly applications need yet to be developed.[185] Pisa and Juden, on the other hand, reason that a decentralised blockchain-based identity management scheme allows for a simplified usability, as users are able "to provide verified personal data with the touch of a button rather than having to access and submit a wide variety of documents."[186] On this matter, the GSMA report argues that a private blockchain platform (compared to a public one) might not only be less risky with fewer unknowns (as all participants on the network are known to each other) but moreover may also appear to feel less radical for the end-user. In this sense, users may not know exactly that blockchain is being employed – for example with the permissioned blockchain platform Building Blocks, which creates digital identities for refugees – and the way users manage their cash or identities can remain unchanged. And yet, key questions such as 'How will users know that their personal data is sustainably secure on the platform?' will remain. "Despite the widely accepted belief that blockchain technologies replace the need for human trust, it is crucial to point out that with permissioned ledgers the user must still trust the people who designed the application, the platform owners and the verifiers of data that is recorded on the chain," so the authors of the report.[187] Analogue to a potential lack of technological understanding of end-users, Nir Kshetri uncovers further obstacles, including

[183] Deloitte, "Blockchain – Enigma. Paradox. Opportunity."
[184] Dunphy and Petitcolas, "A first look at identity management schemes on the blockchain."
[185] Ko and Verity, "Blockchain for the humanitarian sector."
[186] Pisa and Juden, "Blockchain and economic development."
[187] GSMA, "Blockchain for development."

the lack of education and information among end-users but moreover also among implementing actors.[188]

Lastly, but not less importantly, governance-related *legal* and *regulatory challenges* are raised by a number of authors. The GSMA report claims that legal and regulatory frameworks around identity are often vague and fragmented in emerging markets and, additionally, that there are no standards as to how to use unproven technology such as blockchain, to store, manage and share personal data. Consequently, the question of who bears legal responsibility for data in self-sovereign identity systems – the user or the platform provider – remains unclear.[189] Dunphy and Petitcolas highlight the globally tightening regulatory landscape for storing personal data, including, for example, the General Data Protection Regulation (GDPR) under which end-users are granted new powers over personal data and data controllers are issued with new obligations. This in turn challenges the design of an immutable public ledger which references personal data and provides inherent transparency to stored data.[190] In line with conflicting regulatory requirements of blockchain implementation, Kshetri underlines that information stored on a public blockchain cannot be modified or deleted – in line with the technology's principle of immutability –, this feature contradicting the right to be forgotten.[191] Ko and Verity warn that the social, legal and regulatory frameworks relating to blockchain – including applicable privacy norms – are developing at a slower pace than the technology itself.[192] Furthermore, Pisa and Juden expect that the step from pilot projects to large-scale implementation of blockchain-based identity management systems will take longer than expected, as organisations will face a number of challenges related to operational resiliency, governance and data privacy. They believe that organisations and agencies adopting blockchain-based identity management systems must inevitably work closely with government entities to ensure that the legal and regulatory environment supports the use of these chosen solutions – "the key challenge for any user-centric ID system is that key central authorities must buy into the system for it to be effective."[193]

Although the literature in general presents a predominantly positive outlook of blockchain-based identity management, it does, at the same time, recognise that this new technology is not a universal panacea. Distributed ledger technology is still in a very early

[188] Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the Global South?"
[189] GSMA, "Blockchain for development."
[190] Dunphy and Petitcolas, "A first look at identity management schemes on the blockchain."
[191] Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the Global South?"
[192] Ko and Verity, "Blockchain for the humanitarian sector."
[193] Pisa and Juden, "Blockchain and economic development."

stage of development – especially in identity management – and the direction it will take is yet to be decided. As Kewell, Adams and Parry put it: “The essential premise of technology affordance is that to understand the uses and consequences of technologies, they must be considered in the context of their dynamic interactions between people and organizations.”[194] *Is blockchain indeed beneficial and/or necessary for the improvement of a digital identity system?* This question needs to be considered very carefully, when thinking about its application.

It is apparent that while current blockchain-based identity management literature delivers insights regarding the advantages (decentralised, immutable, confidentiality-protecting) and challenges (costs related to high energy consumption, legal and regulatory questions, interoperability) of its structure, specific insights in regard to user experience, usability and acceptance are very limited. The following chapter thus provides some insight into practical examples of blockchain-based identity systems in humanitarian aid use cases.

4.3 USE CASES ON BLOCKCHAIN-BACKED IDENTITY SYSTEMS IN HUMANITARIAN AID

The following section offers a brief overview of use cases of blockchain-backed identity systems in humanitarian aid:

World Food Programme: “Building Blocks”

Since early 2017, Syrian refugees in the Jordanian refugee camp Zaatari are able to purchase goods at the Tazweed Supermarket by scanning their iris, which thus confirms their identity and hence their allocated aid. This new form of cash-, credit card- and voucherless payment is the result of the programme “Building Blocks”, one of the first uses of blockchain technology for humanitarian aid, run by the World Food Programme in collaboration with the biometrics company “EyePay”. Beneficiaries’ personal information is stored in a centralised UN database kept on a variant of the Ethereum blockchain.[195]

Born out of the necessity to save money lost through high transaction fees of local or regional banks, this cash-for-food aid programme turned to blockchain technology in order to reduce such fees. According to the WFP executive Houman Haddad, the blockchain-backed programme has the potential to go beyond saving money, namely to tackle the identity issue

[194] Kewell, Adams and Parry, “Blockchain for good?”

[195] Russ Juskalian, “Inside the Jordan refugee camp that runs on blockchain.” *MIT Technology Review*, 12 April 2018, accessed 10 May 2018, https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain

of many Syrian refugees through means of a self-sovereign identity[196]. Haddad envisions Syrians leaving the Zataari camp one day with a digital wallet filled with a number of personal identifying attributes, camp transactions and access to financial accounts – interlinked by means of a blockchain-based identity system. This digital wallet, so Haddad, could enable individuals to partake in the economic world, as employers could transfer his or her pay, a bank could view his or her credit history and a border agent could check his or her identity attested by the Jordanian government, the UN or possibly even a peer.[197] Furthermore, educational credentials and relationships to family members could be proven and the identity would be portable and could not be revoked by any government or other authority.[198]

Initially, in its pilot phase in Pakistan, Building Blocks was running on the public Ethereum blockchain, ensuring a tamper- and forge-free system. However, with transaction fees adding up and transactions being too slow, Haddad and his team changed to running the system on a permissioned Ethereum blockchain. Although transactions are now faster and the costs are lower, the main drawback accounts to the fact that a central authority (the UN, i.e. its WFP) now has the control over who can participate or cannot and can rewrite transaction histories. Rather than getting rid of the banks as intermediaries, the WFP has essentially become one.[199] This I not only the case of BuildingBlocks, but moreover also in the following two examples of BanQu and the Accenture/Microsoft/Avanade.

BanQu: Providing Economic identities for the unbanked people

The software company BanQu's mission is to include the world's poorest and most marginalised individuals in the global economy by providing unbanked people[200] with a portable and digital "economic identity". An economic identity translates into digital credentials defining a person's history of local, regional or global economic interactions.[201] More specifically, this allows individuals to accumulate identifying, tractable and vetted credentials by connecting with various stakeholders who authenticate these credentials such as, for example, humanitarian aid organisations, governments, banks and peers.[202] These accredited credentials have the potential to meet KYC requirements or unlock credit, thus

[196] The concept of a self-sovereign identity is discussed in the following chapter 4

[197] More about peer-to-peer validation in chapter 7

[198] Juskalian, "Inside the Jordan refugee camp that runs on blockchain."

[199] Ibid.

[200] An „unbanked" individual accounts for an adult who does not own an account at a formal financial institution, i.e. at a bank

[201] Banqu, "Dignity through identity", accessed 15.05.2018. http://www.banquapp.com/our-solutions/how-it-works/

[202] GSMA, "blockchain for development", 17

encouraging formal institutions (e.g. banks) to trust individuals lacking legal identities or credit histories. In short: Blockchain is used to verify new digital traces.[203] These records, which are stored on a permissioned Ethereum-based blockchain platform, can include credit histories, education records, health documents, property and land records, cash disbursements and remote purchases among others[204]. By means of this economic identity, BanQu aims to create economic opportunities for refuges and/or people living in extreme poverty. Moreover, they aim to provide users with more control over their own identity, i.e. users are able to decide what personal data they want to share with whom due to blockchain's blinded infrastructure/zero-knowledge proof.[205]

Economic identities have been created for refugees in Kenya, with the aim to establish long-term secure economic profiles that would leverage for financial access as well as access to government services. Furthermore, smallholder women farmers in Latin America – who face hindrance in financial access due to outmoded property registries and missing land rights – have been provided with these blockchain-backed identities.[206]

Accenture in partnership with Microsoft and Avanade: Blockchain solutions to support ID2020

In support of the UN's SDG 16.9 of providing legal identification to 1.1 undocumented billion people worldwide by 2020, Accenture and Microsoft have teamed up to build a blockchain-backed digital identity system.[207] An identity prototype based on blockchain technology was developed, building on the existing biometric identity system used by the UNHCR, enabling numerous parties to access and share data with high levels of security and confidence. "The prototype is designed to empower individuals with direct consent over who has access to their personal information, and when to release and share data."[208] Similar to the system developed by BanQu, this prototype runs on a permissioned Ethereum blockchain with the idea of allowing users to accumulate verified personal data.

[203] USAID, "Identity in a digital age", 2017,

[204] Banqu, "Dignity through identity."

[205] Ibid.

[206] Ibid.

[207] Anna Irrera, "Accenture, Microsoft team up on blockchain-based digital ID network." *Reuters,* 19 June 2017. https://www.reuters.com/article/us-microsoft-accenture-digitalid/accenture-microsoft-team-up-on-blockchain-based-digital-id-network-idUSKBN19A22B

[208] Sean Conway and Joanne Veto, "Accenture, Microsoft Create Blockchain Solution to Support ID2020", *Accenture*, 19 June 2017, accessed 15 May 2018, https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm

Direct ownership and control over personal data are thus the main focus of the designers.[209] The prototype is still at an early stage of development, but its developers are aiming to finalise technical proof-of-concept and deploy numerous pilot projects by 2020.[210]

While organisations and start-ups have been relatively quick to publicize pilot successes, they seldom, if ever, deliver supporting data to elaborate on usability, user experience and social acceptance of this novel technology. An absence of quality project data may hinder their ability to do so – which makes it all the more important to take this into consideration when designing and implementing effective solutions. After a detour in chapter 5, which explains the concept of a self-sovereign identity, the issue of usability and acceptance of technology as identified by means of the literature review will be re-visited in chapter 6 (dealing with theories of technology acceptance and usability) and consequently chapter 7 (discussing the data analysis).

5. Self-Sovereign Identity

Ultimately, the main question with any blockchain-based identity system is whether its purpose is to put ownership of digital identities in the hands of its users or if it simply eases the way for organisations and states to control people's digital existence. Differing opinions and a battle over this issue – and moreover if it necessarily has to be an either-or decision – is to be expected in the upcoming years.[211] For now one can say that blockchain-based identity systems can thus either fall into one of the two categories:

Blockchain technology as a back-end database

As in the aforementioned use cases of blockchain in humanitarian aid – Building Blocks, BanQu and Accenture & Co.'s prototype in support of ID2020 –, blockchain is mainly used as back-end database by means of a permissioned blockchain. Permissioned blockchain implies that a central authority has control over who can participate or not. This type of blockchain-based identity system simply uses a distributed ledger as its back-end database for a more traditional digital identity system. More specifically, a centralised agency

[209] Sujha Sundararajan, "Microsoft, Hyperledger, UN joint blockchain identity initiative", *Coindesk*, 23 January 2018, accessed 24 April 2018. https://www.coindesk.com/microsoft-hyperledger-un-join-blockchain-identity-initiative/

[210] Michael Del Castillo, "Power to the User: Accenture and Microsoft are changing identity with Ethereum." *Coindesk*, 22 June 2017, accessed 17 March 2018, https://www.coindesk.com/power-to-the-user-accenture-and-microsoft-are-changing-identity-with-ethereum/

[211] Juskalian, "Inside the Jordan refugee camp that runs on blockchain."

(e.g. a humanitarian organisation) provides an identity by performing identity verification of individuals based upon already existing credentials such as a birth certificate or government-issued identity card. These identity attribute attestations are then recorded on a blockchain in order for third parties to validate this at a later stage.[212] The benefit of this permissioned system is – apart from faster and cheaper transaction processes – that identifying information of individuals is stored safely, it cannot be taken away and cannot be lost. However, the downside is that the responsibility of this information remains in the hands of a single entity, such as, for example, an implementing humanitarian organisation. Although this approach improves transparency and safe data storage, the humanitarian organisation has control over who can join the network and, furthermore, can rewrite transaction histories.

Blockchain technology aims at creating decentralised and disintermediated systems.[213] But yet, paradoxically, running a narrow permissioned blockchain brings forth the question if this is not in fact just a re-allocation of an intermediary? Rather than creating a decentralised infrastructure that is controlled by numerous entities in a peer-to-peer network – thus eliminating the need of a centralised authority to regulate and control – a system run on a permissioned blockchain has led to exactly this unwanted centralisation.[214] Can such a network still be described as a 'peer-to-peer' one if it is limited to a few selected peers within a closed network? On a second through, what actually accounts for the 'peerness' in a peer-to-peer network?[215] These issues raises questions in regard to the legitimacy of a blockchain-backed application, i.e. is the use of blockchain an *actual* beneficial improvement of the system or not more than a gimmick.

Hence, the full potential and innovative characteristics of blockchain technology come into play with the second category, namely an "accretionary"[216] or 'self-sovereign' identity.

Self-sovereign identity

Following centralised, federated and user-centric identity, self-sovereign identity is the next step, implicating ownership, control and hence autonomy of one's own identity. Although there are differing views on what *exactly* constitutes as a blockchain-based self-sovereign identity, the definition used for this thesis is as followed: A self-sovereign identity is a digital record of identity attributes that end-users control themselves, i.e. they can add

[212] Ibid.
[213] Swartz, "Blockchain dreams: imagining techno-economic alternatives after Bitcoin", 91-92
[214] Ibid.
[215] Taylor Nelms et al., "social payments: innovation, trust, Bitcoin, and the sharing economy", *Theory, Culture and Society 35*, no.3 (2018):13-33, accessed 10 June 2018, http://journals.sagepub.com/doi/abs/10.1177/0263276417746466, 25
[216] USAID, "Identity in a digital age", 44

more personal data themselves or ask other entities to do so and consequently are central to the administration of their identity.[217] Individuals are put in charge of decisions about the nature and extent of disclosure of their personal identity information rather than external authorities, as in the traditional way, thus creating user autonomy. Claims about identity attributes can be either self-affirmed or asserted by a third party, whose authenticity then can be verified independently by a relying party. Digital identities are thus no longer issued by third parties, however the central element of *trust* – that these self-affirmed or asserted identity claims are true – must still be provided. Hence, the person or organisation acquiring evidence for the accuracy of the credentials constituting the digital identity from third parties must attain credibility.[218] The issue of credibility is thus moved: rather than proving the authenticity of the identity information, the authenticity of the *evidence* must be proven. [219] Third-party credentials claims are thus the core of self-sovereign identity[220].

However, in regards to the actual implementation of self-sovereign identities, the main problem is as followed: decentralised identity is a challenge, as one of the main necessities of a functional identity is discovery, i.e. if a personal identifier is presented, it needs to be verified by a trusted authority. This leads to centralised directories and again to centralised identity systems.[221]

This is now exactly where blockchain's potential comes into play: Distributed ledgers, i.e. blockchain technology can be used in self-sovereign identity systems in order to look up decentralised identifiers *without* having to involve a central directory.[222] "These ledgers are a type of cryptographic database that is provided cooperatively by a global pool of participants instead of a single giant database with a central administrator."[223]

Furthermore, a self-sovereign identity can use blockchain technology, i.e. distributed ledger technology to establish a web-of-trust, as digital identities are no longer issued by third parties. A single blockchain containing a set of information is copied multiple times in many places to create this web-of-trust. This means that no single organisation controls a central

[217] Allen, "The path to self-sovereignty."; Asem Othman and John Callahan, "The Horcrux Protocol: A method for decentralized biometric-based self-sovereign identity", *ArXiv*, 20 November 2017, accessed 1 May 2018, https://arxiv.org/abs/1711.07127

[218] Uwe Der, Stefan Jähnichen and Jan Sürmeli. "Self-sovereign identity – opportunities and challenges for the digital revolution.". *ArXiv*, December 2017, accessed 3 May 2018, https://arxiv.org/pdf/1712.01767.pdf

[219] Ibid.

[220] Philip Windley, "How blockchain makes self-sovereign identities possible". *Computerworld*, 10 January 2018, accessed 3 May 2018, https://www.computerworld.com/article/3244128/security/how-blockchain-makes-self-sovereign-identities-possible.html

[221] Ibid.

[222] Ibid.

[223] Sovrin Foundation, "The inevitable rise of self-sovereign identity." White Paper, 20th September 2016, accessed 20 March 2018, https://www.evernym.com/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

database, but instead transactions are orchestrated by a number of computers.[224] This entails not only interoperability of an identity across multiple locations and services with the user's consent, but also transportability in the sense that it cannot be controlled by one authority (or organisation) or even multiple authorities, nor can it be taken away. In other words; it constitutes a decentralised identity system that is robust to system failure and information hacking as well as enables the recording and interchange of identity attributes by the user itself or by trusted third parties.[225] Importantly, it is not the actual document or information that is stored on the blockchain (this stays with the owner), but rather a record of the validated claim.[226]

In practice this could look as followed: An individual has a so-called "digital wallet" which can be envisioned as the digital version of a regular paper wallet where important documents such as ID, driver's licence, credit card, etc. are stored. This digital wallet – empty at first – could be filled (by the individual him or herself) with identity claims (e.g. birthday, address, health information, etc.). These identity claims would then need to be attested by the relevant authorities, i.e. passport agencies, driving licence authorities, government entities would need to digitally sign these to verify them. Once the claims have been attested, an individual could then use these as personal identity information.

"Rather than just advocating that users be at the center of the identity process, self-sovereign identity requires that users be the rulers of their own identity", says Christopher Allen, one of the pioneers of self-sovereign identity. It is thus a shift from a "silo mentality" to a layer mentality", meaning that the data layer – where an individual makes claims about who he or she is, i.e. date of birth, address, gender, university degrees, etc. – shall be separated from the verification layer where the verification that this information is true takes place[227]. One of the underlying ideas of a self-sovereign identity is that "a simple question needs to get a simple confirmation or answer without having to reveal more about ourselves".[228] This means that when, for example, a person is asked to prove he or she is over the age of 18, he or she would not have to provide his or her birthday as is usually the case,

[224] Othman and Callahan, "The Horcrux Protocol"

[225] Dunphy and Petitcolas, "A first look at identity management schemes on the blockchain."; Allen, " The path to self-sovereign identity."; Othman and Callahan, "The Horcrux Protocol."

[226] Ibid.

[227] Kai Wagner, "Identity as a bottleneck for blockchain: the road to self sovereign identity." *Jolocom*, 18 January 2018, accessed 22 April 2018, https://jolocom.com/identity-bottleneck-blockchain-road-self-sovereign-identity/

[228] Alex Preukschat, "Self sovereign identity – a guide to privacyyou're your digital identity with blockchain", *Medium*, 11 January 2018, accessed 20 April 2018, https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

but could instead provide an attested claim that he or she is “over 18”.[229] The same goes for driving abilities; when renting a car, an individual would not have to provide his or her driver’s licence number (which again is usually linked to a Name, birthday and address) but could instead provide a claim – attested by the driving licence authorities – that he or she “is eligible to drive”. This would mean that only minimal personal identifiable data would be shared with a third party, thus reducing the potential of identity loss or theft in case of a data breach of the respective third party.

All this being said, it is apparent that these promising attributes of a self-sovereign identity vision really only can excel if its theoretical concept can be translated into practical use – not only in means of technical feasibility but moreover for the end-users. This is especially true, when the implementation of this new technology aims to benefit and empower vulnerable end-users, such as for example beneficiaries of a CTP. For example, what does it imply for an end-user to have more control over his or her own digital appearance, but at the same time be responsible for establishing and maintaining privacy of this appearance all of a sudden? How does a digitally inexperienced person understand what it implies to have ones personal information stored on a decentralised ledger? To what extent is secure blinded infrastructure (selective disclosure) really secure, if a person does not fully grasp the concept behind disclosing certain personal information to a service provider? Are people willing to place trust in a decentralised network rather than a known and tangible central institution? If the concept of blockchain-based identity management is looked at from a user rather than from a systems design perspective, its implementation starts to raise numerous questions in relation to its usability for end-users. As the scholars Dunphy and Petitcolas state: “If it isn’t usable it isn’t secure.”[230]

6. Theories on technology acceptance and usability

Much of the research on the interface between the somewhat theoretical construct of a blockchain-based self-sovereign identity and the practical usability for end-users hinges on whether this new form of identity management is in fact ‘usable’ and accepted by its intended users. Implementing a new technology system without user acceptance and usability may significantly hamper the success of it.[231] Even if using the new technology system leads to

[229] Lewis, “A gentle introduction to self-sovereign identity.”

[230] Dunphy and Petitcolas, “A first look at identity management schemes on the blockchain.”

[231] John Gould et al., “Making Usable, useful, productivity-enhancing computer applications.” *Communications of the ACM. 34*, no.1 (1991):74-85, accessed 19 March 2018, https://dl.acm.org/citation.cfm?id=99993

significant amendment of a user's status quo, the user is often reluctant to engaging with it.[232] Hence, the crucial defining factor of the success or failure of any technological implementation is perceived to lie with user acceptance – as trivial as it may sound it is an often-overlooked component of a new systems development.[233]

Analysing and predicting usability, user experience as well as user acceptance of blockchain-based identity management thus presupposes an in-depth understanding of the *influencing factors*. Understanding what makes people accept a new technology is key not only for researchers, but furthermore also practitioners, in order to improve system design methods and to predict user response to it as best as possible.[234] If and to what extent user-experience and usability feedback can be translated into specific interface design enhancements naturally depends on a multitude of factors. But again, understanding how one links to another is the basis for a sustainable user acceptance. This is especially true in modern times when technology innovations are spreading across societies increasingly, more people becoming dependent on it and questions of appropriate and ethical technology designs are increasing.[235]

The focus of this thesis lies on the factors of usability and user acceptance, i.e. indicators that may predict the level of acceptance of a blockchain-backed identity system. For the purpose of clarity, *user acceptance* here is defined as the attitude towards a technology and the willingness to engage with the technology for the intended purpose"[236]. Not equivalent to the notion of acceptance, but closely related is that of *usability*: Commonly understood in terms of "ease of use" and "user-friendliness", yet lacking a precise definition in much of the related literature. The International Organisation for Standardisation (ISO) proposes an international standard for usability, whereby the usability of an application refers to the "extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use".[237]

[232] Burton Swanson, "Information Channel Disposition and use." *Decision Science 18*, no.1 (1987): 131-145. https://doi.org/10.1111/j.1540-5915.1987.tb01508.x

[233] Fred Davis 1993, "User acceptance of information technology: Systems characteristics, user perceptions and behavioural impacts." *International Journal of Man-Machine Studies 38*, no.3 (1993): 475-487, accessed 19 March 2018, https://doi.org/10.1006/imms.1993.1022; Andrew Dillon and Michael Morris, "User acceptance of new information technology: Theories and models", In *Annual Review of Information science and technology Vol.31*, edited by Martha Williams, 3-32. Medford: Information Today, 1996

[234] Dillon and Morris, "User acceptance of new information technology."

[235] Ibid.

[236] Andrew Dillon, "User acceptance of information Technology", In *Encylcopedia of Human Factors and Ergonomics*, edited by Waldemar Karwowski. London: Taylor and Francis, 2001, accessed 17 March 2018, https://www.researchgate.net/publication/279683883_User_acceptance_of_information_technology

[237] International organisation for standardization (ISO). "Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability." 9241-11:1998, 15 March 1998, accessed 20 April 2018, https://www.sis.se/api/document/preview/611299

The manner in which a new technology transfers from invention to widespread use (or does not) can – among a number of other theories – be explained by means of the Innovation Diffusion Theory (IDT).[238] This conceivably fundamental theoretical perspective on technology diffusion suggests that an innovation offering *relative advantages* over presently available alternatives, *compatibility* with social norms and practices of the user, *low complexity* and *ease of use*, the possibility to explore the use of the technology before committing to it, i.e. *trialability*, and apparent gains of the innovation (*observability*) will diffuse more extensively than a new technology with the opposing attributes. The scholars Gary Moore and Izak Benbasat extend these characteristics to an information technology-specific context, adding an emphasis on *discretion* and *ease of use* as decisive elements to evaluate technological diffusion.[239] This, of course, does not exclude individual end-users' factors such as personality traits, wealth or education, just to mention a few, which also play an important role in innovation diffusion.[240]

Evidently, innovation diffusion theory provides a framework to study the *diffusion* or *adoption* of new (information) technology, however provides little insight into actual *user acceptance*. Compared to technology adoption, which portrays a process starting with technology awareness and ending with technology embracing and making full use of it by the user, technology acceptance represents an attitude towards a technology. Acceptance thus poses a prerequisite to adoption.[241] This attitude can be influenced by different factors. One school of thought dealing with the design and development process of new information technology is the Technology Acceptance Model (TAM) developed by Fred Davis.[242] The aim of this model is to address and predict acceptance and design problems at the onset of technology development rather than once users are already exposed to it.[243] The factors believed to determine user acceptance are firstly, *perceived usefulness* (the extent to which a user perceives the system to improve his or her status quo) and secondly, *perceived ease of use* (the extent to which a user perceives the system to be free from effort). These two factors are seen by TAM to have a pivotal influence on a user's acceptance of a new system, with a

[238] Dillon and Morris, "User acceptance of new information technology."

[239] Gary Moore and Izak Benbasat, "Development of an instrument to measure the perceptions of adopting an information technology innovation", *Information Systems Research 2,* no.3 (1991): 192-222

[240] Ibid.

[241] Karen Renaud and Judy van Biljon. "Predicting Technology Acceptance and Adoption by the Elderly: A Qualitative Study." In Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists, Wilderness, South Africa, (6-8 October, 2008): 210-219, accessed 19 March 2018, https://dl.acm.org/citation.cfm?doid=1456659.1456684

[242] Fred Davis, "Perceived Usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, 13, no.3 (1989): 19-34, accessed 19 March 2018, https://www.jstor.org/stable/249008?seq=1#page_scan_tab_contents

[243] Dillon and Morris, "User acceptance of new information technology."

special emphasis on the latter. Ease of use of a system can be translated into effort expectancy and is closely related to complexity, which is significant especially at the beginning of the technology implementation and becomes insignificant with extended and sustained usage.[244]

Besides the already above-mentioned factors, *facilitating conditions* are also perceived to portray an influencing factor in technology acceptance (in innovation diffusion theory, technology acceptance model and theory of planned behaviour). Facilitating conditions can be explained as the extent to which a person identifies the existence of a technical or organisational infrastructure to support them in the use of the system.[245] This ranges from guidance in the selection of the system, over specialised instruction to personalised assistance with system difficulties.[246] Linked to facilitating conditions is perceived behavioural control, indicating an individual's being in control when using the system, an individuals' available resources that are necessary to use the system adequately, and possibly also the compatibility with previously used systems.[247]

One may argue that a prerequisite of technological diffusion and acceptance is the actual *usability* of a technology. Research that focuses profoundly on this concept and subsequently the development of more user-centered technology is that of Human-Computer Interaction (HCI) – "though not equivalent to the concept of acceptance, most HCI researchers assume that the more usable a technology is made, the greater its chances of proving acceptable to users."[248] HCI concerns itself not only with the actual human-computer interaction, but moreover also the knowledge about that socio-technical interaction.[249] A *user* is seen as anyone trying to accomplish whatever he or she set out to do using the technology, by *computer* any technology from general desktop computer-to-computer systems and control systems is referred to, and interaction relates to the direct or indirect communication between a user and a computer.[250] An important aspect to consider when talking about the concept of usability is that it depends largely on the specific "product" that is to be implemented, i.e. reaching conclusions about ease of use is very difficult as intercultural differences in the understanding of and concern for use variables differ, making it hard to universalise them.[251]

[244] Venkatesh et al., "User acceptance of information technology: Toward a unified view", *MIS Quarterly 27*, no.3 (2003): 425-478.

[245] Ibid.

[246] Gary Moore and Izak Benbasat, "Development of an instrument to measure the perceptions of adopting an information technology innovation."

[247] Venkatesh et al., "User acceptance of information technology."

[248] Dillon and Morris, "User acceptance of new information technology."

[249] Frank Maddix, *Human-Computer Interaction: Theory and Practice*. New York: Simon & Schuster, 1990.

[250] Alan Dix et al., Human-Computer Interaction", Essex: Pearson Education Limited, 2004, accessed 15 March 2018, http://fit.mta.edu.vn/files/DanhSach/__Human_computer_interaction.pdf

[251] Gabriel Acosta et al. "Addressing human factors and ergonomics in design process, product life cycle and innovation: trends in consumer product design." In *Ergonomics and human factors in consumer product design*,

According to Paul Booth, unravelling the correlation between the functionality of a system and the understanding of it, is a challenge and furthermore "the way a user understands a system mediates the user's perception of functionality."[252]

Evidently, researchers and practitioners trying to develop more usable and humanly accessible systems come to a set of common factors regarding technology acceptance and usability – thus blurring the fine lines between the different theories and research traditions. While there is no comprehensive theory or model (yet) that can explain and predict user acceptance wholly, common factors across all above-mentioned models can be identified as perceived ease of use and perceived usefulness. Numerous system designers consider a lack of user-friendliness of systems as being the key barrier to user accessibility, usability and evidently user acceptance. "For a complex system to be well designed we need to rely on something more than simply our intuition", meaning that with complex new systems, our personal notion of good and bad are not sufficient.[253]

All this being said, one important aspect to mention in regards to usability – or moreover acceptance – is that it depends largely on whether the use of the technology is mandated or voluntary[254] – this is particularly interesting to remember when implementing a technology in a humanitarian aid context, where participation is hardly ever mandatory (i.e. food distribution, cash transfers), but people are often faced with no other choice than to participate.

The 'hypotheses' of the just outlined theories and models will guide the following analysis of this thesis by exploring which *influencing factors* are pivotal for the successful implementation of a newly proposed blockchain-based identity system in CTPs in regard to end-users. The aim is to analyse if and to what extent the pivotal factors of user acceptance and usability as portrayed in the above-mentioned theories can help understand and help draw a nuanced conclusion on the usability and user acceptance of a blockchain-based identity management system. As such, derived pivotal factors are interwoven into the interview questions directed at the CTP/digital identity/blockchain experts.. The aim of the analysis in the following chapter is the discovery of patterns that appear among numerous data

ed. Karwowski Waldemar, Marcelo Marcio Soares and Neville A. Stanton (CRC Press: Talyor and Francis, 2011), 133-154, accessed 14 March 2018, https://www.researchgate.net/publication/215607788_Addressing_human_factors_and_ergonomics_in_design_process_product_life_cycle_and_innovation_trends_in_consumer_product_design

[252] Booth, *Errors and Theory in human-computer interaction*, 70

[253] Dix et al., "Addressing human factors and ergonomics in design process", 6

[254] Visvanath Venkatesh and Fred Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies." *Management Science* 46, no.2 (2000): 186-2004.

observations, i.e. interview respondents' answers, which point to – and reveal – a better understanding of user acceptance and usability.

7. Data analysis

This chapter tackles the main research question: *What are the potentials and challenges of a blockchain-backed identity management system for beneficiaries of a cash transfer program in regard to usability and technology acceptance?* It does so by addressing these potentials and challenges as seen by experts of the field of humanitarian CTPs and relevant secondary sources. The following sections are divided into six sub sections according to overarching themes based mainly on a comprehensive content analysis of the interviews[255] conducted with people affiliated either with cash transfer programming, and/or digital identity and/or blockchain technology. The sub sections are made up of two parts: The first part addresses the findings based on responses of interviewees – and in order to underline the respondents' arguments or to complement said information with supplementary evidence, secondary sources are incorporated into the analysis. The second part includes approaches and explorations of 510's planned CTP system as a case study.[256] The idea is to give an overview of the foreseen challenges and potentials by a number of respondents and the literature and subsequently demonstrate how 510 as a case study is tackling these issues with its own project on future cash based assistance.

7. 1 Infrastructure and access to (mobile) digital devices

7.1.1 Discussion of the issue

The most straightforward and unsurprising main challenge in creating digital identities based on blockchain technology is the issue of *infrastructure* and *access*. More often than not, humanitarian aid is either provided in areas of low digital penetration and low Internet connectivity, such as in remote or rural communities, or in situations of conflict, where an Internet connection may be down for long periods of time. Digital penetration is spreading across the globe – while in 1995 only 16 million people, i.e. 0.4% of the world population used the Internet in some form, usage spread up to 4157 million, accounting for 54.4% of the

[255] The interview transcriptions are in possession of the author in order to safeguard the privacy of the respondents (who in certain cases preferred to stay anonymous in order to speak freely and from a personal rather than an organisational perspective).

[256] The findings are based on numerous conversations with 510 employees and volunteers who are partaking in the FCBA project in some form or the other. As the project is still in its initial stage, none of the findings are final and could take on a different form throughout the development of the project.

world population by 2017[257] – but needless to say that not all parts of the globe are included in this global grid of connectivity. Although current Internet penetration and mobile phone growth rates are increasing largely in developing countries[258], recent data shows that nearly four billion individuals in the developing world lack access to the Internet.[259] Hence, digital (self-)registration creates an inescapable access issue for individuals without a personal digital device (e.g. mobile phone, computer or tablet), as well as for those without the possibility of access through the device of a family member or acquaintance. This foundational issue remains an unresolved problem. The most commonly adopted solution is one of the following: Facilitate access through a delegate of a humanitarian organisation providing digital devices (e.g. tablets, mobile phones) and assistance or implement this new identity system solely in places of widespread digital connectivity. If and to which extent the challenge of infrastructure and access will dissolve in the next five to ten years and consequently make a high-tech identity solution more usable for end-users remains yet to be answered.

7.1.2 Case Study: 510's fcba

510 envisions a fully digital system with widespread use of self-registration that enables people to have more ownership over their data which is stored on their own device and/or is accessible by them directly. Nonetheless, currently and most likely in the nearer future, local context does not allow for a fully digital option due to various reasons – including connectivity, digital infrastructure and access to this infrastructure. Hence, 510 is adapting to the given situation. This means that registration can happen twofold: Firstly, through a delegate, i.e. a volunteer or staff member of the implementing humanitarian organisation. It should always be possible to conduct registration by delegate (as is the status quo), not simply due to a lack of access to mobile infrastructure but, moreover, due to challenges of interaction with the registration system caused by illiteracy and/or disabilities (e.g. blindness, lacking a body part needed for biometric registration or a signature and so forth). It is thus inevitable to exclude the option by delegate in order to safeguard widespread inclusiveness. Secondly, in an increasingly digitised world, 510 is eager to tap into the possibilities of self-registration. By designing a system that does not only serve the option of input by a delegate but,

[257] "Internet growth Statistics 1995 to 2018", Internet World Statistics, accessed 30 April 2018, https://www.internetworldstats.com/emarketing.htm

[258] Mark Graham, ""Inequitable distributions in Internet geographies: The Global South is gaining access, but lags in local content." *Innovations* 9, no.3/4 (2014): 3-19, accessed 28 April 2018, https://doi.org/10.1162/inov_a_00212

[259] Zambrano, „Blockchain", 9

additionally, also self-registration, the system can be sustainable and profitable in the long-run – presuming that in the future, self-registration may very well be a valid option for many people of 510's target group.

7. 2 Topicality of personal information and the added value of an identity

7.2.1 discussion of the issue

Once initial registration has taken place, either through self-registration or with the help of an intermediary – say a staff member or volunteer of a humanitarian agency – individuals must be able to keep their information up to date in order to live up to the idea of a self-sovereign identity. Hence, the issue of *topicality* arises, i.e. keeping personal data up-to-date. This is seen as a challenge, as described by one of the respondents:

> *"If money is involved, all would register, that would not be the issue, but keeping it up to date is the most difficult part [...] when a baby is born, or when someone gets lost or dies: How to keep it up to date? What if during a situation of armed conflict there is no access to the Internet for over a year and a child is born during this time, how can information be updated, registered?"*[260]

Keeping personal data up-to-date, thus, unsurprisingly depends heavily on access to and understanding of the digital device. However, the topicality of a person's personal information hinges not only on the access to and understanding of digital devices, but furthermore also on the *incentive* to do so. One of the respondents raised this issue with the following concern: *"Within a community there must be an incentive for people to keep their data up-to-date, but this incentive is not sure yet."* Believing that individuals will use their personal digital devices to update their personal information or travel long distances to a place of digital connectivity to do so is a premature presumption. Keeping this personal information up-to-date is an investment that requires time and trust of sharing personal information.[261] In this regard, the added value of keeping this information up-to-date seems to be missing for the end-users.

This being said, there are differing views between some of the responders and the literature regarding the added value. While much of the academic and grey literature stresses the value of an ID for each and every individual, the respondents, on the other hand, were

[260] All notes in quotation marks and italic are responses of the interviewees. In order to guarantee the interviewees anonymity (as some of them requested), all names and respective association to organisations are left away on purpose.
[261] USAID, "Identity in a digital age."

more reluctant to this notion, the main reason being the question: Who actually benefits most of an intact identity system – the aid-providing agency or the individual him- or herself? As one of the respondents says:

> *"There must be an added value for a beneficiary to provide personal information [to create a digital ID]. Once the service is done, what's left for the beneficiary should have added value that stays. At the moment they give us [humanitarian organisation] more than we give them by registering them, i.e. information that they provide is being used."*

Benefits for organisations and transparency for donors hence (still) seem to be more highly prioritised than the direct value for the beneficiary; this is actually the message of this respondent. This challenge is also recognised by a report of USAID, stating that "an initial investment to support the formation of a DID [digital identity] system will get it off the ground, but long-term viability requires more."[262] By 'more', the report refers to "access to a broad range of widely valued services".[263] Having an ID that can be used across a number of programs, offering access to more than one service would thus be an added value and could possibly account as an incentive. "As ID systems are increasingly linked to a variety of services, their value increases; this in turn supports inclusion and continued participation in the ID system. Increased inclusion promotes data availability, and more data can help the system run more efficiently, which creates value for the institutions investing in the DID systems."[264] If the system thus takes user satisfaction into consideration – rather than only organisational needs – the identity system has a higher chance of growth and sustainability.

This important identity element strengthens the rationale for a self-sovereign identity, which, among other things, aims at a blockchain-backed interoperable identity usable across various sectors. Nonetheless, more often than not, interoperability hinges on the willingness of organisations and institutions to do so, as discussed in chapter 4 on the challenges of digital identity systems.

Another challenge closely related to topicality of data that was raised by the respondents, is *the right to be forgotten*, i.e. "the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed"[265] which came into effect by May 25th 2018 under the EU's General Data Protection Regulation (GDPR). This data subject

[262] Ibid., 29
[263] Ibid.
[264] Ibid.
[265] Art.17 'Right to Erasure' and Recital 66 'Right to be forgotten' GDPR (Source: https://gdpr-info.eu/art-17-gdpr/, accessed 23 May 2018)

right could prove to be problematic when considered against one of the key characteristics of blockchain, namely immutability of data. Article 17 of the GDPR requires the "erasure" of personal data of individuals when they invoke their right "to be forgotten" – or more simply to delete or correct a falsely put in piece of information.

> *"In terms of GDPR, if you think of the nature of the blockchain – a blockchain is immutable, so once data would be committed there you, let's say you or someone on behalf of you inserted this information which wasn't correct – or the data contained something you didn't want to know – you cannot overwrite the data, which is not a good thing."*

Although the interpretation of the obligation to "erase" data is not yet clearly defined, a literal reading of article 17 could be problematic, i.e. it is unclear how the blockchain-backed storing of personal data can comply with this GDPR requirement.

7.2.2 Case Study: 510's fcba

As discussed in the aforementioned section, keeping personal information up-to-date after initial registration has taken place is twofold: Firstly, there needs to be a technical solution and secondly, there also needs to be an incentive for end-users to do so. In regard to the technical component, a potential solution of 510 lies in incentivising agents to keep information up-to-date by means of a reward. This reward could be either financial or targeted at reputation. This would work in a similar fashion as the PoW or PoS protocol with blockchain (as discussed in chapter 4), where miners receive a reward for having solved the hash puzzle and thus having up-to-date ledgers. However, in the case of a financial reward, this would imply that the amount of funding for people in need would be reduced (unless validators are also people in need of aid) and in the case of reputation, the exact mechanism would need to be designed. Could, for example, a validator's own trust score increase with the amount of claims he or she attested?

From an end-user perspective, 510 is focussing on community engagement to find out more about what such an incentive could embody. By nature of design a self-sovereign identity has the potential of being interoperable – that is, usable for a variety of services of differing humanitarian organisations. From a beneficiary perspective 510 sees added benefits/incentives in the feature of re-usability and interoperability of a self-sovereign identity, which has the potential to reduce the times individuals need to re-register as well as time spent queuing in line to re-register. Comprehensibly, registration is almost always linked to expectation (of receiving aid) – which can result in frustration in case of an unfulfilled outcome (if an individual turns out not to be eligible for aid). 510 is aware that the emotional aspect that naturally comes with registering for a CTP – that is hope, expectation, disappointment and frustration – cannot be changed by means of a new system. But what can be changed is the speed at which aid can be delivered to the beneficiaries, which can be decisive in situations of humanitarian crises. These arguments, however, are based on the assumption of what end-users (should) find important – which may not be in line with what they themselves find important. The balance of a humanitarian organisation such as the Red Cross lies between their responsibility in "protecting" beneficiaries with regard to their personal data versus the beneficiaries' right to decide whether they care about their data's safety or not. This raises an interesting debate on its own, which, however, cannot be discussed in the scope of this thesis but needs to be kept in mind.

In regard to the compatibility of GDPR regulations – especially the right to be forgotten – 510 does not yet have a clear approach. GDPR and blockchain are not compatible, especially not in the case where identity information is stored on the blockchain. However, there are ways to tackle this problem to be GDPR-compatible, for example when the identity credentials themselves are not stored directly on the distributed ledger, but instead only a hash of these identity files. This means that the identity itself is stored on a local device or a cloud storage or the like, which is encrypted end-to-end. The blockchain itself only stores the hash, which means that if something in the original document is changed, i.e. an identity credential, the hash won't match anymore, showing that there has been an alteration. Although individuals may not be able to delete the evidence that they were once assigned an identity on the blockchain, they are, however, able to delete the identifying credentials. Especially in the case of a system designed with zero-proof-knowledge, these can be revoked. This may suggest that the right to be forgotten might not be *the necessary* factor anymore. Evidently, 510 still needs to puzzle out this challenge in order to make it GDPR accordant.

7.3 Complexity of Cryptographic tools and end-user private and public key management

7.3.1 discussion of the issue

Using and applying blockchain technology in the humanitarian and development sector poses challenges similar to the adoption of new technology in general – for end-users as well as for humanitarian and development practitioners. Nonetheless, the *complexity of blockchain technology* itself introduces new hitches particularly for end-users, thus furthering this challenge even more.[266] Research and respondents suggest that using complex cryptographic tools remains a challenge and contains noteworthy room for development in order to be understood by and appeal to a wide range of users.[267] This is especially the case for users who are unfamiliar with the Internet and digital devices. The literature review in chapter 4 already touched upon this issue, one of the main findings regarding usability being that blockchain represents a complete shift away from traditional ways of doing things, especially for digitally inexperienced users.[268]

The challenge thus lies in the management of end-user private and public keys. More often than not, there seems to be the supposition that end-users are able to conduct effective cryptographic key management.[269] More specifically, "blockchain technology wallets can and have provided friendly interfaces that facilitate public key cryptography. But users need to manage their private keys and safely store them somewhere, somehow."[270] Storing a private key could be in the form of a paper containing a QR code or a password. The respondents' opinions on the ability of people to store important 'papers' or documents differ, i.e. there seem to be cultural differences in the understanding and perception of storing a document. Losing a private key poses a grave menace, and to date there are no existing solutions to physical theft of private keys.[271] Two respondents mentioned that there were incidents in which distributed information flyers were brought back to the organisation the next day, rather than keeping on to them, as the purpose of holding on to the flyer was unclear to the recipients. It is noteworthy to mention that the ability to store – and how to store – a document naturally depends hugely on the local context. Hence it is crucial to explore local conditions and customs before deciding on what form a document-holding information to their private key should/could take on in order to be locally appropriate. One could argue that the use of biometrics, for example a fingerprint or an iris scan, instead of a password or PIN code, poses an alternative and 'loss-resistant' method of identification. Nonetheless, this again raises a whole new set of questions: In cases of identity theft, a body part naturally cannot be exchanged, using a body part rather than a password can be very invasive for individuals and so forth.[272]

[266] Zambrano, "Blockchain", 12
[267] Ibid., 9-12
[268] Deloitte, "Blockchain – Enigma. Paradox. Opporunity."
[269] Dunphy and Petitcolas, "A first look at identity management schemes on the blockchain."
[270] Zambrano, "Blockchain", 9-12
[271] Ibid.,31
[272] "Cashing in on Crisis? The Refugee Eye Scan Experiment", Redfish video documentary, 11 March 2018, accessed 25 May 2018, https://www.youtube.com/watch?reload=9&v=oUtl8Hpg15w

Additionally, engagement with cryptographic tools presupposes the individual's understanding of the implications of storing and handling identity data in a distributed ledger.[273] A widespread adopted approach seems to be that "end-users do not need to own or directly use the technology to benefit from its deployment".[274] Meaning that only because the technology of the system changes, it does not mean the user interface needs to change, too. Aid:Tech is an organisation that has deployed blockchain for humanitarian purposes. Although using blockchain for the digital transaction and not the identity registration, one of the co-founders mentioned: *"They [the beneficiaries] had no idea that they were on the blockchain, using cutting-edge technology [...] it all worked."* However, this approach raises doubts and ethical questions related to consent, which will be discussed in more detail in section 7.4.

Taken together, these above-mentioned challenges might prove too demanding for individuals and populations with relatively low levels of literacy and education (if not for the majority of average Internet users). And yet, the authors Pisa and Juden offer a contrary argument, emphasising that more often than not digital tools handling identity allow for simplified usability, as users are able "to provide verified personal data with the touch of a button rather than having to access and submit a wide variety of documents."[275] Furthermore, people's capabilities in general and moreover in crisis should not be underestimated, as one of the respondents mentioned:

> *"People in crisis are very resourceful: If you give them something to allow them to build on their capability to adapt, then they will use it. Give people something that is useful for them. If you build something that is only useful for the NGO, then you will be passing on the cost of the use on to the beneficiary and the beneficiary will not want to use it."*

Solutions to tackle the issue of handling complex cryptographic tools could thus take the form of one of the following ways (or as a combination of both). Firstly: compatibility with familiarity, that is, using the knowledge and resources of the target population to bridge the gap between the new tool and what they already know. By allowing for methods that build upon an already familiar foundation of knowledge or practice, people can adapt and hence use the new tool/system. Secondly: making use of intermediaries that can facilitate end-users with access to cryptographic tools: "The only way to break out of this impasse is to devise alternatives that furnish end-users with access to cryptographic tools via intermediaries such

[273] Dunphy and Petitcolas, "A first look at identity management schemes on the blockchain."
[274] Zambrano, "Blockchain", 12
[275] Pisa and Juden, "Blockchain and economic development."

as community-based organisations, small enterprises and/or local governments."[276] It appears to be evident that the role of an intermediary is inevitable in certain cases and in the near future. And yet, the intermediary role is somewhat ambiguous and paradox. On the one hand, an intermediary seems to be the best solution for widespread inclusion. On the other hand, respondents mention that dependency on an intermediary may actually foster exclusion through, for example, favouritism of the community leader, fear instilled by the community leader, gender disparities on a community level or within households and so forth. The intermediary thus indeed portrays a predicament.

In the long run, the idea of a self-sovereign identity would be for the individual to have complete control over his or her identity, without the influence or dependency on an intermediary. However, if self-registration and self-management is the full way to go, or if intermediaries are needed, this depends largely on the local context. Currently, it appears to be inevitable to exclude the powerful role of an intermediary, i.e. facilitator in the form of an NGO staff member, a volunteer or a community leader, in order to transmit information and smooth the path to widespread end-user usability.

7.3.2 Case Study: 510's FCBA

A number of issues related to the complexity of cryptographic tools were revealed during the interviews with respondents, including the support role of intermediaries, blockchain technology wallets, the storing of documents per se and, lastly, the user-friendly interface. In the case of the proposed FCBA project, the Red Cross has a big advantage: They usually have a large local network of Red Cross and Red Crescent branches containing local volunteers who are part of the communities. Currently, for the proposed project pilot in Malawi, they are hence engaging with staff members of the Malawian Red Cross to disclose challenges and possibilities of a new system. Community engagement, including interviewing potential end-users of the system, is on the agenda as one of the consequent steps needed to proceed prior to implementation. The fear that dependency on an intermediary may actually foster exclusion naturally cannot be fully eliminated as long as intermediaries are involved. However, the likelihood of exclusion should be relatively small considering the Red Cross movement and its involvement of local volunteers.

Attention must be laid on the inclusion of people who do not own a digital device or cannot access one if needed. In cases like this, 510 proposes centralised registration centres where a person will be able to register in the system by interacting with a Red Cross delegate

[276] Zambrano, "Blockchain", 9-12

without any need of digital knowledge. The credentials will then most likely be stored on paper, i.e. a so-called digital paper wallet which the end-user will keep with him- or herself. If and how this document can/will be stored by the end-user depends largely on the local context and is currently being explored.

Another question mark that has been raised is that of a “friendly interface”. Although often mentioned in literature and in colloquial language, there arises a legitimate issue *What constitutes a user-friendly interface?* This is a question that 510 will have to tackle once the back-end part of the system has been designed and the focus will be shifted to the front end, that is, the interface. Although 510 is relatively far in thoughts about the user interface, local application has yet to be explored. The team is planning a pilot project run with staff members of the Netherlands Red Cross in July 2018 to test the system mainly from a back-end perspective (Can people register successfully? Can users receive digital cash in form of a token? etc.), but will also make note of the usability of the system from an interface perspective (Can people interact with the mobile application? Is the interface clear to them? etc.). These insights will be used to optimise the design of the system for actual use cases planned in the near future, which inevitably will have to be adapted depending on local contexts (established through careful considerations of local context and respective community engagement).

7.4 User consent and control over personal data – innovation versus exploitation

7.4.1 discussion of the issue

Tightly interwoven with the issue of the complexity of cryptographic tools is that of user consent and being in control of one’s personal data. User consent is mentioned by the respondents as being one of the main challenges of a (self-)registration system based on technology. Personal data protection is an integral part of protecting the integrity and dignity of individuals and, hence, of fundamental meaning for humanitarian organisations.[277] Consent is “any freely-given, specific and informed indication of agreement by the Data Subject to the collection and processing of Personal Data relating to him or her”, by means of a written or oral statement.[278] However, the crucial detail lies within the difference between consent and

[277] Christopher Kuner and Massimo Marelli. *ICRC Handbook on Data Protection in Humanitarian Action*. Geneva: ICRC, 2017. https://www.privacy-web.nl/cms/files/2017-07/handbook-data-protection-and-humanitarian-action-2-.pdf

[278] “Data Responsibility Policy“, 510, accessed 10 May 2018, https://www.510.global/wp-content/uploads/2017/11/510_Data_Responsibility_Policy_V.2_PUBLIC-1.pdf

informed consent. Informed consent boils down to an individual's understanding of risks associated with providing personal data. One of the respondents described this challenge in the following example of individuals' registering for a CTP in Nigeria:

> *"In Nigeria, where there is a low literacy rate and people are limited in their data preparedness [...] For example, people could not write so they just gave a fingerprint because they could not provide an autograph. So even though consent was asked, it is doubtful that those who registered truly understood what consent meant – and even less what they actually consent to."*

Informed consent is exceedingly complicated, because data protection regulations are increasingly complex, i.e. including the GDPR guidelines. Humanitarian staff members understanding the legal framework of GDPR is one factor, but explaining this to another person is something else. In line with this, a respondent also mentioned the correlation between a lack of *understanding of data value* and consent. More specifically: It would be difficult or even unrealistic to expect beneficiaries to give informed consent considering the lack of understanding of data value. Although the majority of the responders mentioned that people were not reluctant to provide personal information to a humanitarian organisation, the example of Nigeria cannot be generalised. An anecdote of one of the respondents regarding refugee registration in a UNHCR refugee camp in a European country[279] demonstrates the opposite:

> *"In [country name kept anonymous] they were very weary of their data. Especially, providing it to UN bodies as they thought it might have further consequences for request for asylum."*

Even without – or possibly as a consequence of not – fully understanding to what they were consenting to, individuals can be hesitant to provide personal data. Another related fundamental issue is that of *free consent*. Although giving consent incorporates "any freely-given […] indication of agreement", it is questionable how far consent is indeed "free" if it is pegged to humanitarian aid. People in crisis often have no other choice than to hand over their data and information in order to receive much-needed aid.

> *"Does an individual in crisis really have a choice not to give consent? If you are offering people in crisis something which they need, they will take it, and as such they have no real free consent [...] people in crisis take more risk and have less choice [...] Getting someone's consent today might not be in line with the risks of the future, as*

[279] The respondent's wish was to not include any country names nor the name of her organisation in the interview transcription in order to guarantee her anonymity, as she spoke from freely from her personal views and opinions, rather than from an organisational perspective.

> *technology and therefore the uses of data change. So the question lies in the legitimacy of this consent. With CTP you often collect more data and then you share it with a third party service provider who may then use this data for more than just making the transfer of cash requested by the humanitarian agency. What are the risks for the individual and what is going to happen to this data?"*

A journalistic video published by the Grassroots media start-up 'Redfish' in March 2018 further illuminates the issue of free consent in relation to the Refugee Iris scan pilot project deployed by the UNHCR in Jordan. In the Zataari and Azraq refugee camps, Syrian refugees can obtain humanitarian aid through scanning their irises. In the video documentary, the reporter Yasmin Fanselow criticises that Syrian refugees have no other choice than to give their consent to iris scan registration in order to receive the aid that is necessary to survive. Furthermore, she raises the question of who actually benefits most from the deployment of new technology and if vendors are not simply cashing in on crises by using vulnerable people as guinea pigs.

With the involvement of new technologies in the data collection process, the difficulty to understand the risks and benefits of giving consent to data collection increases.[280] The deployment of a complex cryptographic tool such as blockchain technology in all likelihood is thus expected to intensify this challenge (as outlined in section 7.2). Hence, is it valid to say that – from a beneficiary's perspective – a system can be accepted if it cannot incorporate free consent? Pegging identity management to humanitarian aid programmes – including CTP's – opens up a whole new set of ethical questions. To date, there seems to be no solution to this challenge.

> *"We have not yet cracked the nut of getting consent from people; it is more about covering oneself [the organisation] rather than getting actual consent."*

However, approaches in tackling this challenge did come through in the discussions, namely by means of, firstly, protection through laws and regulations and, secondly, as far as possible: education for those implementing the new system as well as for its end-users.

Firstly, most humanitarian organisations are required to take more responsibility for the consideration of risks and benefits when collecting an individual's personal data. This can, for example, be through regularly reviewing their adopted data responsibility and protection mechanisms and training of implementing staff in the field. This is especially crucial in the advent of new technologies, which tend to run ahead of local policies and regulations.

[280] Kuner, "ICRC Handbook on Data Protection in Humanitarian Action", 45

While industrialised countries are slowly catching up with their regulatory and legal framework in regard to blockchain technology, most developing countries' regulatory capacities are still emerging. Humanitarian organisations thinking of implementing a new digital (identity) system should thus ensure that local development priority is not bypassed nor that the lack of regulatory knowledge is exploited[281].

> *"If you want to bring aid, you want to focus on bringing aid, and not lose time by focussing on first getting to know the laws. But there were talks to local community and governors before aid was distributed; but in those talks the data responsibility as not brought up."*

When confronted with the question on data protection laws and regulations, a number of respondents answered that data protection laws do exist in theory, yet in practice they are often either left out due to unfeasibility and time pressure related to the crisis, or not transparent to them at all.

Furthermore, targeted individuals or communities should receive appropriate and context-sensitive information and education on what it means to give consent to data collection and processing. Most people are not hesitant to provide personal information, but *"vulnerabilities are a big concern",* states one of the respondents. Therefore, in order to create awareness and sensitisation, if applicable, community meetings are typically conducted prior to the registration process where the procedure is explained to the community.

Naturally, it is necessary to balance consent with the given situation, i.e. such as in a situation of precarious crisis, where the distribution of aid were to be hampered, delayed or prevented due to the difficulty of getting informed consent prior to data collection. In this case, the aid-providing organisation could provide information regarding conditions of data collection in a less targeted and individualised way, such as by means of public notes or community gatherings.[282] More than one respondent mentioned that there *"simply was no time"* to ensure informed consent of all the beneficiaries due to time constraint and the urgency of the aid distribution.

The second aspect mentioned in the opening sentence of this paragraph is that of *control over personal data*. One of the main goals and prerequisites of a self-sovereign identity is to provide end-users with more control over their data, *inter alia*, through consent. The importance of being in control of one's own data depends largely on the local context, so said a number of respondents. For example, in Afghanistan many people were well aware that they could be geo-located through mobiles and were very cautious about the fact that they

[281] Zambrano, "Blockchain", 10

[282] Kuner, "ICRC Handbook on Data Protection in Humanitarian Action", 21

could be tracked. The risk of sharing data was perceived as being very high for them. In the Ukraine, on the other hand, most people under the age of 60 had smartphones and were aware of the "risk" of being geo-located or of having personal data taken without their consent, but perceived it as less important.[283] On the other hand, in all fairness: How much does the average person really care about being in control over personal information?

> *"Nobody really reads terms and conditions – how much do people really think about data protection in daily life? [...] But people who have fled because of conflict may well be more aware of risks than the 'average' person. It is thus important to discuss with affected communities how they understand risk and the likely impact on them. Only through a conversation with a wide cross section of the community can the impact of risk from a community perspective be understood."*

Based on the respondents' answers, it seems fair to conclude that the importance of control over personal data seems to vary depending on the local context, i.e. the perceived risk associated with personal data. In cases of armed conflict and forced displacement, personal information is associated with a higher value and risk than in situations of natural disaster.

7.4.2 Case Study: 510's fcba

510's mission is to use data in order to improve the timeliness and (cost) effectiveness of humanitarian aid and to enhance preparedness and coping capacities for people in disaster and crises areas.[284] To this end, 510 is extremely aware of the responsible use of beneficiary data guided by its protection mandate as a Red Cross organisation and its mission to ensure the applicability of the fundamental Red Cross principles while using data. In line with rapid technological developments and the increasingly inter-connected world, 510 sees the potential and obligation to make use of these developments in order to provide adequate humanitarian assistance. Nonetheless, technology not only poses potential for enhancement of processes but, moreover, also new challenges. Hence 510 has developed a Data Responsibility Policy with the purpose of incorporating concise and workable principles for a responsible use of data in its projects, programmes and overall work. "While legal instruments on data protection are an important step to enhanced transparency, data responsibility takes into account ethical considerations that go beyond compliance".[285] The policy has been complemented with additional resources – such as training materials and a guideline for a threat and risk assessment – to safeguard feasible implementation.[286]

[283] From an interview with an ICRC delegate who wishes to remain anonymous.
[284] 510, "Data Responsibility Policy", 1
[285] Ibid.
[286] Ibid.

In regard to the issue of consent, 510 lays emphasis on getting *informed consent* by means of an oral or written statement or a clear affirmative action. Again, this raises questions regarding the underlying issue of informed consent versus informed *free* consent. More specifically, when individuals register for a digital blockchain-backed identity, they are *required* to provide a certain set of identifying credentials to be able to register. In this sense – as with any targeted aid distribution – the issue of free (informed) consent is not solved. However, by designing a blockchain-backed self-sovereign identity allowing for data minimisation and selective disclosure by design, i.e. by means of a cryptographic technique known as zero-knowledge proof, 510 aims at providing owners of the identity control once they have registered – and for the remaining time thereafter. Individuals can be in control over their identity by means of controlling the private key linked to the digital identity.

7.5 THE HUMAN AS INTERMEDIARY AND VALIDATOR

7.5.1 DISCUSSION OF THE ISSUE

Having a human in the identity/registration process is a double-edged affair, as touched upon in section 7.3. On the one hand, it seems inevitable to have an intermediary/facilitator for those who are in need of assistance due to digital inexperience or other hindrances such as blindness, illiteracy, etc. Assistance is especially crucial in a more complex system, such as a blockchain-backed identity system. On the other hand, there cannot be a fully self-sovereign ID system as long as there is an intermediary in the loop, and dependency on an intermediary can also foster exclusion through favouritism, gender disparities, etc. In reality though, as long as digital penetration and access to digital devices remains low, it is inevitable to exclude the intermediary in the process of identity registration. The key in this situation is *trust*. Respondents' prevalent opinion is that trust from an end-user's perspective lies with the people collecting the information rather than with the actual technology. Engaging in face-to-face conversation with people, responding to questions and uncertainties in real time and representing a familiar face or organisation conveys trust and thus access to affected people. For a humanitarian organisation this means that the *perception* of the people is crucial:

> *"[The key to a successful program implementation] goes beyond the risk management, beyond legal aspects and beyond security – of course all these frameworks are needed to not be porous to attacks, but the particular community needs to trust you."*

Hence, two factors should be taken into consideration by the humanitarian organisation in order to potentially achieve acceptability and consequently widespread use of a newly implemented system. Firstly, partnerships with other local or community-trusted entities as well as deployment of local volunteers play an important role in creating trust and spreading acceptance. Secondly, designing solutions by understanding the needs of the target group is important, i.e. designing together *with* the community, rather than solely *for* the community. This involves community engagement and education on the proposed new system/technology. Whether the intermediary will remain in the loop or not will therefore depend largely on the local conditions:

> *"In situations of severe humanitarian crisis, for example remote or very poor places, or in the depth of a war, the role of the human will hardly if ever change dramatically. There are always going to be humanitarian actors there, but that is a niche, that is not the bulk of the humanitarian field. The bulk of the money of humanitarian work is in those places where you cannot tell the difference between development and humanitarian: people are above or below the poverty line due to shock or other causes. And in those places, people have mobile phones."*

Apart from embodying the assisting or facilitating intermediary role, humans currently also portray the validator role. In a proposed self-sovereign ID, the idea is for individuals to collect identifying credentials that accumulate to a strong personal identity over time. This, however, presupposes that these identifying credentials need to be verified and validated by someone. "Any documents or assets stored using blockchain need to be verified […]; the integrity of the data is only protected after it is entered".[287] As mentioned a few times previously, validation is closely interrelated with trust. And currently, this trust lies in institutions, i.e. mainly NGOs and state institutions. This however, takes control from the individuals over their identity and gives it back to a centralised institution – diminishing the potential of a self-sovereign identity.

> *"NGOs have value because they have experienced people that know what to look for [in targeting and registering people]. NGOs will continue to survive if they continue to capitalise on their validator role. That validator can go back into the system and insert subjective information, but that is not reducing the inclusion/exclusion error as the information is still input by a human."*

A potential solution to this drawback is seen in the so-called *peer-to-peer validation* – envisioning "an ecosystem of trusted identity verifying nodes" enabled by a public-

[287] USAID, "Identity in a digital age", 57

permissionless blockchain.[288] In this validation mechanism, a person can verify another person's identity claims by digitally signing and immutably storing a hash of the respective identity on the public-permissioned blockchain. This validation mechanism would enable not only members of institutions to validate an individual's information, but moreover also private people, i.e. a neighbour, a friend, a family member, a former employee and so forth. It seems reasonable to say that a relative can verify a claim about his or her family member's date of birth with a greater degree of reliability than the government or any other institution. The same accounts for neighbours attesting to claims about residential addresses.[289]

To a certain degree, the idea of a peer-to-peer validation originates from the notion of *liquid democracy*, an innovative voting model for collective decision-making in communities. Liquid democracy aims at creating a sincerely democratic voting system by enabling voters to vote in issues directly or to delegate one's personal vote to a trusted person. Delegation of voting power implies better overall governance of the state, as "decisions are mainly made by those who have the kind of knowledge and experience required to make well-informed decisions on issues."[290] This form of decision-making holds a lot of potential for local communities and governments to foster trust and transparency in voting. Moreover, it also holds potential for a peer-to-peer validation mechanism, as it places validation of personally identifying information into the hands of exactly those who have the required knowledge, such as for example a neighbour, a family member or a co-worker. In theory this should account for well-informed claims.

Unsurprisingly, this raises doubts about misuse and fraud. A trustless ecosystem that can protect and validate the integrity of people's identities appears to be an unsolved design problem.[291] This being said, pioneers of this validation method are positive that there is a way to bypass this design puzzle: "Such a system can be insulated from misuse through a sound reputation engine which incentivises identity verifiers to act in good faith."[292]

Though a digital peer-to-peer validation system to date has not been implemented by any (humanitarian) organisation, yet the first documented example of a blockchain-based peer-to-peer validation of identity has already taken place: On November 8th 2015 the first ever birth certificate was registered on a blockchain[293]. The blockchain-based proof of

[288] Adithya Kumar, "The missing 1.1 billion: blockchain-based digital identities as a driver of inclusion", *Procivis*, 4 April 2018, accessed 19 May 2018a https://procivis.ch/2018/04/04/the-missing-1-1-billion-blockchain-based-digital-identities-as-a-driver-of-inclusion

[289] Ibid.

[290] https://medium.com/organizer-sandbox/liquid-democracy-true-democracy-for-the-21st-century-7c66f5e53b6f

[291] Kumar, "The missing 1.1 billion."

[292] Ibid.

[293] On a Bitcoin Blockchain to be more specific.

identity of a new-born girl with the name Roma Siri was not established through a government or institution, as is usually the case, but instead on a decentralised database by means of her father's self-sovereign power.[294] The baby's father produced a video stating the new-born's full name, date and place of birth and then hashed it on the blockchain using Proof of Existence, a blockchain verification service. This way, the father ensured that the birth certificate was notarised and validated by the global network of computers, i.e. the Bitcoin's mining network. In order to validate the birth registration, the father included a testimony of himself, of the baby's mother as well as her two grandmothers. In addition, a hospital birth certificate was added as well as a screenshot displaying the last mined block of the respective blockchain containing the personal information of Roma Siri. The father stated that the birth registration file was a valid certificate of the hashed events, preventing anyone from challenging the fact that the birth registration file was not created on the stated date and time. Nor could its content be modified without altering proof.[295] This example of a peer-to-peer identity validation sets an example of how end-users can control their own data. Santiago Siri, the entrepreneurial father of Roma Siri, believes that blockchain-based identity management has a huge potential in developing countries where the need for alternative systems to remodel the status quo is imminent: "In my view, what the web has done for media and culture, the blockchain will do for institutions and human organisations."[296]

Another form of peer-to-peer validation has been demonstrated by a digital version of Bryan Ford's *Proof-of-Individuality (POI)* system[297]. The proposed idea is digital gatherings (by means of video chats) across the world – so-called pseudonym parties – to validate the individuality of the participants. These gatherings can take place in applications such as Google Hangouts or Microsoft Holoportation and are based on Ford's pseudonym parties' algorithm, meaning randomly assigned and simultaneous gatherings all over the world repeated throughout the year. The idea of these gatherings is to tackle the issue of "How to prove that a person only has one account [identity] within the system?"[298] The peer-to-peer verification works as followes: Users of the system are randomly grouped together and take part in a video-chat lasting approximately ten minutes during which users cross-check each other (simply by ensuring that group members' attention is not split) ensuring that their group

[294] Sandra Stephens. "Dive into liquid democracy", Democracy Earth, 9 November 2017, accessed 27 May 2018, https://words.democracy.earth/dive-into-liquid-democracy-cded2d9ba1d6

[295] Ibid.

[296] Ibid.

[297] Bryan Ford, "Pseudonym Parties: An offline foundation for online accountability", MIT, 27 March 2007, accessed 28 May 2018, http://www.brynosaurus.com/log/2007/0327-PseudonymParties.pdf

[298] "Proof of Individuality", Whitepaper, accessed 27 May 2018, http://proofofindividuality.online

members are not partaking in other video chats at the same time.[299] If successful, they distribute so-called crypto tokens among each other and sign and verify each other's POI (in the form of smart-assets hosted on the blockchain-powered Ethereum network), proving that "You cannot exist in two different spaces at the same time."[300] The incentive/reward to partake in these video-chats can be incorporated into the system, i.e. by means of crypto tokens that participants can distribute among each other (depending on how much you believe a person is telling the truth about him-or herself, you can distribute more or fewer tokens). The more tokens you have selected, the more credible your individuality gets.[301] The practicality of this peer-to-peer validation mechanism has, however, yet to be tested.

The idea of a peer-to-peer validation can be spun even further, i.e. one respondent highlighted the idea of ideally having an identity system based entirely on self-registration and self-verification through available personally identifiable data points and consequently eliminating the need of a human validator.

> *"If enough data points are actually available through social media, community based targeting, etc. you will not need the human to verify information of others, but people can self-register. […] if you look at the ways donors are pushing NGOs to operate, is to push them to a place where they only have the human [in the loop] when it is needed, not as a default. […] the change is happening, regardless of what is happening in the technology sphere."*

As innovative and bottom-up a peer-to-peer or self-registration verification system sounds in theory, it yet again hinges on the aforementioned challenges of access to digital devices, infrastructure and understanding of complex tools. Peer-to-peer validation can only be realised if it is accessible, acceptable and usable for the people. Furthermore, in the case of humanitarian aid, one cannot underestimate the importance of local knowledge – which no form of technology can replace fully (to date).

7.5.2 Case Study: 510's FCBA

The key outcomes of the above paragraphs were, firstly: Gaining trust to local communities by means of a trusted intermediary is important as long as a human is in the registration loop. This prerequisite is given in the case of 510, as the Netherlands Red Cross has a broad local

[299] Crypto_Future. "Ethereum based proof-of-individuality prevents Sybil attacks*", Decentralize Today*, 9 April 2016, accessed 28 May 2018, https://decentralize.today/ethereum-based-proof-of-individuality-prevents-sybil-attacks-9757864bbf61

[300] Crypto_Future, "Proof of Individuality."

[301] Gautham, "Proof of individuality, the New-Age security of blockchain", News BTC, 5 April 2016, accessed 28 May 2018, https://www.newsbtc.com/2016/04/05/proof-of-individuality-blockchain-security/

network of Red Cross and Red Crescent branches that include local volunteers of the communities. This means that the Red Cross already works closely with volunteers who are part of a community and can thus relatively easily create trust and spread acceptance among communities.

Secondly, peer-to-peer validation is seen as a potential solution to speeding up the validation process and making it less dependent on a central entity. Although this approach has not been fully developed yet, the idea suggests that a person inserts self-asserted information into his or her digital wallet, which consequently can be validated by a trusted community member. This community member could, for example, be pre-appointed by the implementing humanitarian organisation to validate these individuals' claims by meeting them in person. 510 has designed a system that incorporates peer-to-peer validation in theory. If, how and to which extent this validation mechanism method will be used is yet to be decided upon. Currently the system is designed in such a way that everyone within the network can theoretically attest each other transparently. However, only once the Red Cross has also attested an individual does this allow him or her to be eligible for a Red Cross-implemented cash transfer.

In practice this means that people within a community may attest each other, which may act as a proxy for the Red Cross to directly attest an individual or, on the other hand, raise the red flag. In case of uncertainties, i.e. if say within a community a number of individuals are attested for, but one or two fall out of the pattern, this may indicate that a person is not who they claim to be, or that a specific identifying attribute is not perceived to be true by the community members. In this case, Red Cross delegates meet up with the person in question to verify these attributes themselves and thus have the final say. This, however, stands in contradiction with blockchain's principle of disintermediation, as the system still relies on a central authority. If and to which extent this peer-to-peer validation mechanism can and will be implemented again depends largely on the local context. Furthermore, 510 highlights the importance and value of local knowledge in regard to targeting and inclusion without which it would not be comfortable to advance at this stage.

7.6 Feedback mechanisms

7.6.1 discussion of the issue

Having an intact feedback mechanism is inevitable for any sustainable service and can foster acceptance and usability among end-users. In a CTP, a feedback mechanism has two levels:

Technical support (for example when facing problems with accessing a personal account) and programme-feedback (targeting process, management of programme, possibility to provide feedback and place complaints about the process and its respective system, etc.). Important characteristics that a feedback mechanism should incorporate, according to the respondents, are the following: Accessibility in the sense of multiple and context-appropriate methods such as, for example, a telephone hotline, a community center that has a contact person or an e-mail address that can be consulted. Secondly, language: The respective feedback mechanism (hotline, community center, Internet website, etc.) should be accessible in as many local languages as possible. Thirdly, the feedback mechanism should be independent of the system at best in order to allow for anonymity. This way, if desired, feedback cannot be traced back to the petitioner, which may inhibit him or her to make use of the mechanism due to fear of negative consequences of a community leader, government or even humanitarian organisation.

Acceptability of a system, furthermore, does not end with the actual beneficiaries, but moreover also with those who could not register and who are not eligible for aid, as their negative experience with a system could influence their peers and hence promote rejection among them. Feedback mechanism should thus be open to those within the system (those who have been registered) as well as for those outside the system (those who were not able to register, those not eligible for aid, etc.).

7.6.2 Case Study: feedback mechanism in 510's FCBA

510 is aiming to specifically target technical feedback (relating to creating a digital identity) versus programme feedback (relating to whether or not a person is eligible for aid). This translates into potential differing feedback mechanisms depending on where a user finds him- or herself in the registration process. To date these have been identified as being important during the phases of registration, inclusion-criteria and distribution. More specifically this means that users should be able to flag their issue firstly, when attempts to register fail or when they have not been included in the eligibility criteria set by the Red Cross. Secondly, once registration has been successful (that is, once a user is registered with the system), individuals should have the possibility to flag a concern and/or ask a question to clarify uncertainties. Thirdly, during the process of cash distribution, beneficiaries should be given the opportunity to give feedback on all distribution-related matters.

According to many respondents, non-digital feedback should always be an option, i.e. through a telephone hotline or a representative at the community center, etc. However, with the long-term/ideal idea of scaling up the program, 510 sees a challenge in providing sufficient and well-functioning non-digital feedback possibilities for users. Assuming 510 themselves will not have the capacity to take care of this, it would presuppose that they will need to rely heavily on local Red Cross employees and volunteers. However, in order for them to be able to help an individual, local Red Cross employees and/or volunteers would need in-depth knowledge and understanding of the system that goes beyond the ability to register someone. In addition, this is based on the assumption that they will have enough capacity to carry out this task. A potential solution to this issue would be to include other humanitarian organisations, i.e. other future users of the system, to partake in aspects like this. However, this on the other hand may increase the risk of a fragmented feedback system that will cause challenges in the long run.

7.7 Limitations to the data analysis

This bottom-up research question aimed at discussing usability and user acceptance of a blockchain-based identity system. Answers to the research question were sought through extensive literature review and discussions with experts. Although these findings are insightful and an effort was made to talk to people with actual field experience, they are, nevertheless, fully representative of a bottom-up approach. For this, actual end-users (i.e. beneficiaries of current CTPs) would have had to be involved in the form of focus groups or interviews. However, due to access issues of end-user population of current use cases, as well as time and scope restrictions of this thesis, this important aspect of input was not included in the findings.

Another limitation can be attributed to the novelty and complexity of the research field. Although questions were adapted to the individual background and area of expertise of each respondent if necessary, the general impression is that the concept of a blockchain-based ID system did encounter some incomprehension among some of the respondents. It is not unlikely, that this incomprehension potentially influenced the results, i.e. that questions would have been answered in a different way had the respondent fully understood the characteristics of blockchain technology applied to identity management. Nonetheless, the best was done to incorporate thoughts, ideas and reservations of both CTP *and* blockchain experts, in order to get a representative overall picture.

Furthermore, one needs to keep in mind that the analysis is based on a small number of expert interviews, thus portraying only a limited number of opinions. In many cases, respondents are knowledgeable in a specific regional area, which is very beneficial for a specific community, however, these opinions may not appropriately portray the circumstances of another community. It is thus important to mention that these inductive results are based heavily on personal and professional opinions rather than on opinions of a large sample size.

Naturally, as with every qualitative data collection, my presence as a researcher during data gathering, my affiliation with the Netherlands Red Cross 510 Data Science Team and my personal unconscious bias and idiosyncrasy had their influence on the results as well. By means of consciousness about personal bias and maintaining a stance of an independent researcher (i.e. not mentioning my 510 affiliation if interviewing people outside of the Red Cross and Red Crescent movement), I tried to keep the initial position as neutral as possible.

This chapter included a detailed analysis of challenges of a blockchain-based registration system in regards to usability and acceptance *from an end-user perspective*. This following concluding chapter recaps and substantiates the most important findings, links them to the applied theoretical framework and responds to the main research question outlined at the beginning of this thesis.

8. Synthesis and conclusion

This thesis aimed at presenting an innovative approach to the identity challenge faced in a number of humanitarian aid contexts, one of them being the registration process of a humanitarian cash transfer program. Based on the shortcomings of most current registration systems, an initial yet ever-increasing trend is moving away from centralised or federated identity systems and towards a more 'user-centric' one. Presumably, the creation of a self-sovereign identity presents the ultimate form of a user-centric identity. By suggesting a blockchain-backed self-sovereign identity, some technologists are envisioning a silver bullet to overcome a number of challenges previously associated with digital identities. No doubt, the potential of blockchain innovation is substantial and serves as a likely game-changer in various identity-related issues.

The main perceived advantages of a blockchain-backed identity come from enhanced speed of aid delivery, reduced time for the registration process, potential interoperability of a digital identity across various services and humanitarian organisations, privacy and data integrity benefits fostered by blockchain's decentralised architecture, more control over personal data and the elimination of a central authority. In addition, blockchain has the potential to include the undocumented in the case of a self-sovereign identity – which can be composed of multiple identifying attributes rather than a state-issued legal identity.

Yet these potential advantages need to be enjoyed with caution. Firstly, as the technology is still in its infancy, it is too early to draw conclusions on how it will evolve in the years to come. “As is often the case with technologies, hype is leading the charge, but current evidence suggests blockchain technology deployments are still in proof-of-concept stage”.[302] Secondly, blockchain-backed identity management systems are not all to be lumped together, i.e. there is a non-negligible difference between using blockchain technology as a centralised back-end database versus as a means to create a self-sovereign identity, as well as between a permissioned and permissionless design choice. In the case of a permissioned blockchain, for example, the highly praised traits of decentralisation and disintermediation are in fact simply re-allocated rather than eliminated. In the case of a self-sovereign identity, ownership belongs in the hand of the end-user. And yet, who validates the input claims? As seen with most examples so far, access is still controlled by an authority, thus building on a centralised system similar to the legacy ones. So although blockchain innovators present a number of advantages over current digital identity systems – tackling data protection weaknesses, centralised databases and information silos of humanitarian organisations among others – they need to be scrutinised. Is the digital identity challenge indeed solved with a blockchain-backed system, or are the problems merely redistributed and concealed behind complex terminology?

Furthermore, the conducted research unveiled a myriad of challenges regarding the implementation of a blockchain-backed identity system.[303] Unmistakably, some of these challenges are not novel to the humanitarian aid sector; however, the complexity of blockchain technology itself adds a new element to the mix. Apart from legal and regulatory challenges caused by the novelty of the technology and the speed at which it is being deployed, one of the main unanswered issues relates to usability, user experience and user acceptance. These challenges result mainly from the complexity of the technology, access to and understanding of digital devices, understanding of how to securely navigate the Internet, applications that lack user-friendly interfaces as well as placing trust in technology rather than in humans to mention the most common ones.

According to practice and theory of human-computer interface, usability and technology acceptance are crucial to the sustainability of a new technological innovation. Hence, a number of experts in the field of humanitarian aid – more specifically CTPs – as well as a few selected individuals knowledgeable in blockchain technology were consulted to

[302] Zambrano, “Blockchain”, 12

[303] There are a number of further challenges related to technology, regulation, governance, etc. however the focus of this thesis is set specifically on the end-user potentials and challenges

find out what the challenges and opportunities of a blockchain-backed identity system in CTP in developing countries *could* be. Existing technology acceptance and usability models derived from literature were considered and from them a set of potential influencing factors was extracted. The factors were validated by means of semi-structured interviews with CTP experienced field workers. Following the Technology Acceptance Model (TAM), perceived usefulness and perceived ease of use are the two main pivotal factors in determining *user acceptance*. From an Innovation Diffusion Theory perspective, these factors are compatibility with previous systems, low complexity and ease of use, trialability, observability and relative advantage. In line with this, the Human-Computer Interaction theory summarises crucial factors of *usability* of new technology to be social influence and facilitating conditions. The common influencing factors of all the three theories can be summarised as *ease of use* and *perceived usefulness* of the technology at stake.

This thesis sought to determine whether these influencing factors grounded by TAM, HCI and IDT approaches would predict of the user acceptance and usability of a new identity management system in CTP. This thesis finds that the crucial elements and hence usability of a blockchain-based identity system hinge on the following factors: Continuous accessibility and infrastructure, ability to interact with the complexity of the technology, added value, the role of a facilitating intermediary and the means of validating personal data. Control over personal data and user consent on the other hand seem to be of less pivotal importance for the end-users as predicted.

Although of grave importance for each and every individual and a solemnly important concept for humanitarian work more generally, the majority of the interview respondents answered that end-users are either unaware of the value and importance of personal data and frequently do not care about where their data is stored nor what happens to it. More often than not, however, end-users see no other choice than to consent and participate. Most likely, the combination of a lacking awareness over the value of personal data as well as the severity of an individual in need diminishes the importance of control and consent in this situation.

This being said, acceptance cannot be accurately explored nor sufficiently inferred from the available data. Although presumably interlinked, usability cannot assume acceptance or vice versa in the case of a digital identity system in humanitarian aid. The reasons are twofold: Firstly, in order to make valid claims on technology acceptance, actual input of end-users would need to be gathered and analysed instead of relying solely on expert opinions and literature. Secondly, acceptance and usability cannot be assumed on the basis of interaction with a technology if this interaction is not completely voluntary. Although participating in a new registration system of a humanitarian aid organisation is not obligatory per se, it is often the only way for people in crisis to receive the aid they so desperately seek. Linking the adoption of a technology to the delivery of aid thus results in a quasi-mandatory situation. In this regard the introductory quote of this thesis should be re-introduced, as it highlights the fundamental underlying issue of any type of identity management that is pegged to humanitarian aid. *"Identity is far more than just a card with a name and a photograph. ID technologies sit at the interface between the power and prerogatives of institutions and the rights and needs of individuals."*[304] While a CTP-triggered blockchain-backed self-sovereign identity system may very well overcome a number of issues related to logistics, timeliness, safety and sustainability, it nonetheless raises a series of ethical issues related to aid distribution and identity management per se. Although this issue opens the Pandora's Box of ethical issues of humanitarian aid more generally – and thus goes beyond the scope of this thesis – it is important to keep in mind that certain issues of CTPs remain unsolved, irrespective of the modality in which they are conducted.

Usability currently poses a greater challenge than acceptability, mainly due to access to Internet and digital devices, the nature of blockchain's complex technology and the required infrastructure and knowledge it presupposes to make it usable.

> *"None of the people registered [referring to CTP beneficiaries in rural Nigeria] would probably ever come across their information on any website, so they would never complain, i.e. they would not know how/where to complain; they do not know what to do about it."*[305]

However, with increasing deployment of new technology in the humanitarian and development sector, and with a growing number of Internet users familiar with its potentials and pitfalls, this difference may invert. Familiarity with Internet applications and digital tools may possibly further usability of complex tools, but acceptability hesitancy may increase too. Data breach incidents such as the 2018 Facebook-Cambridge Analytica data scandal – where personally identifiable information of over 87 million Facebook users worldwide were collected to allegedly influence voter opinions on behalf of politicians[306] – may very well shape the future of technology acceptance aiming at personal data management.

Although these findings are insightful and an effort was made to talk to people with field experience, they are nevertheless not fully representative of a bottom-up approach. In

[304] USAID, "Identity in a digital age", 2

[305] Quote of a respondent

[306] Neue Zürcher Zeitung (NZZ), "Bis zu 29'000 Schweizer Facebook-Nutzer sind vom Datenskandal betroffen", NZZ online, 5 April 2018, accessed 23 May 2018. https://www.nzz.ch/wirtschaft/facebook-cambridge-analytica-koennte-daten-von-87-millionen-menschen-missbraucht-haben-ld.1374393

order to have a truly representative overview of usability and end-user acceptance, actual CTP users would need to be consulted. More specifically, opinions of CTP users of the region in which a humanitarian organisation aims to implement such a registration system need to be taken into consideration.

9. FUTURE WORK

This thesis opens up possibilities for future research on the vast (and largely unexplored) topic of blockchain-backed identity systems in general and in humanitarian aid more specifically. Future research could consider exploring the possibilities of a peer-to-peer validation mechanism more thoroughly, i.e. taking a closer look at the incentive mechanism where verifiers digitally sign another person's identifying attributes. To be more specific: Where Proof-of-Work (PoW) and Proof-of-Stake (PoS)[307] account for viable incentive mechanisms for miners of cryptocurrencies, there needs more insight on the equivalent reward for 'miners' in a peer-to-peer identity credential validation mechanism. Is this financial? Or reputational? Could a reward, for example, be increasing a 'validator's' trust score with the number of attestations he or she verifies? Or could it be the number of common attesters, thus factoring in the likelihood of peers actually knowing each other in real life? This presupposes that validators are interested in strengthening their own identity claims. Whatever the incentive may be, its relevance is not to be underestimated, as it bears the crux of sustainability in a peer-to-peer validation mechanism.

Another relevant topic would be to explore the potential interoperability of blockchain-backed identity systems. As discussed in this thesis, blockchain could offer a proxy for trust to entities who, under normal circumstances, would not trust each other. The important question to explore thus follows: *Does blockchain foster this trust not only in theory but moreover also in practice?* Researching this question would imply analysing not only the technical possibilities of a blockchain-backed identity system, but also the underlying power structure of humanitarian organisations – including controlling access to highly sensitive information – as well as the relation between humanitarian organisations themselves and between humanitarian organisations and governments and/or the state.

Additionally, it would be timely to explore legal and regulatory challenges that arise when blockchain-backed applications are used to store, manage and share personal data. Who

[307] As discussed in chapter 4

bears legal responsibility for data in self-sovereign systems – the user or the platform provider? These are only a few potential topics to tap into, there are undoubtedly many more, some of which will only unfold once the use of blockchain for identity management has been further explored and implemented.

10. Bibliography

Acosta, Gabriel, Karen Lange Morales, David Ernesto Puentes Lagos and Manuel Ricardo Ruiz Ortiz. “Addressing human factors and ergonomics in design process, product life cycle and innovation: trends in consumer product design.” In *Ergonomics and human factors in consumer product design*, ed. Karwowski Waldemar, Marcelo Marcio Soares and Neville A. Stanton (CRC Press: Talyor and Francis, 2011), 133-154. Accessed 14 March 2018. https://www.researchgate.net/publication/215607788_Addressing_human_factors_and_ergonomics_in_design_process_product_life_cycle_and_innovation_trends_in_consumer_product_design

Atick, Joseph, Alan Gelb, Seda Pahlavooni, Ramos Gasol and Elena Zaid. “Digital Identity Toolkit: A guide for Stakeholders in Africa”. World Bank Group, 1 June 2014. Accessed 2 May 2018. http://documents.worldbank.org/curated/en/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa

Allen, Christopher. “The Path to Self-Sovereign Identity.” Life with Alacitry. 25 April 2016. Accessed 15 March 2018. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Al-Saqaf, Walid and Nicolas Seidler. “Blockchain technology for social impact.” *Journal of Cyber Policy* 2 (2017): 338-354. Accessed 12 March 2018. https://doi.org/10.1080/23738871.2017.1400084

Augot, Daniel, Hervé Chabanne, Olivier Clémot and George William. “Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain.” Cornell University Library. 9 October 2017. Accessed 14 March 2018, https://arxiv.org/abs/1710.02951

Banqu. “Dignity through identity.” Accessed 15 May, 2018. http://www.banquapp.com/our-solutions/how-it-works/

BBC News. “Accenture and Microsoft plan digital IDs for millions of refugees”. *BBC News*, 20 June, 2017. Accessed 13 May 2018. http://www.bbc.com/news/technology-40341511

Blockgeeks. “Proof of work vs proof of stake: basic mining guide.” Accessed 10 June 2018, https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Bentov, Iddo, Ariel Gaizon and Alex Mizrahi. “Cryptocurrencies without proof of work.” *Arxiv*, 22 June 2014. Accessed 9 June 2018. https://arxiv.org/abs/1406.5694

Booth, Paul. Errors and Theory in human-computer interaction. *Acta Psychologica*, 78 (1991): 69-96; drawing on notes forwarded by Jones S. (1984) „Preliminary observations of Macintosh Plus users. Department of Computer Science, Stirling University. Accessed 15 March 2018. https://ac.els-cdn.com/000169189190005K/1-s2.0-000169189190005K-main.pdf?_tid=c486c4fa-ed37-44d4-94c8-7ccf845b230f&acdnat=1528454314_8c65d32f40a2a707ccf7a0b4641c9288

Boston Consultancy Group. "The value of our digital identity." Liberty Global, Inc. November 2012. Accessed 13 May 2018. https://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

Camp, Jean. 2004. "Digital Identity." *IEEE Technology and Society Magazine 23*, no.3 (2004) : 34-41. Accessed 5 April, 2018. http://social.cs.uiuc.edu/class/papers/digital_identity.pdf

Chibafa, Keith. "Why not digital? Technology as an interagency tool in the Central African Republic." Humanitarian Practice Network at ODI, *Humanitarian Exchange 62,* (2014): 19-21. Accessed 18 March 2018. https://odihpn.org/magazine/why-not-digital-technology-as-an-interagency-tool-in-the-central-african-republic/

Clark, Julia, Mariana Dahan, Vyjayanti Desai, Marta Ienco, Stephanie de Labriolle, Jean-Pierre Pellestor, Kyla Redi and Yolanda Varuhaki. "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation". *World Bank Group, GSMA and Secure Identity Alliance,* July 2016. Accessed 20 March 2018. http://docplayer.net/62557738-Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation.html

Commonwealth Partnership for Technology Management (CPTM). "Adaptive flexibility approaches to financial inclusion in a digital age." Smart Partners Hub, 6 October 2016, accessed 30 April 2018. http://www.cptm.org/documents/CFMM_Brief_%202016.pdf

Conway, Sean and Joanne Veto. "Accenture, Microsoft Create Blockchain Solution to Support ID2020." *Accenture*, 19 June 2017. Accessed 15 May 2018. https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm

Crypto_Future. "Ethereum based proof-of-individuality prevents Sybil attacks." *Decentralize Today*, 9 April 2016. Accessed 28 May 2018. https://decentralize.today/ethereum-based-proof-of-individuality-prevents-sybil-attacks-9757864bbf61

Dahan, Mariana and Alan Gelb. "The role of identification in the post-2015 development agenda." World Bank Working Paper, 7 July 2015. Accessed 9 May 2018. https://www.cgdev.org/sites/default/files/CGD-Essay-Dahan-Gelb-Role-Identification-Post-2015-ID4D_0.pdf

Davis, Fred. “Perceived Usefulness, perceived ease of use, and user acceptance of information technology.” *MIS Quarterly*, 13, no.3 (1989): 19-34. Accessed 19 March 2018. https://www.jstor.org/stable/249008?seq=1#page_scan_tab_contents

Davis, Fred. “User acceptance of information technology: Systems characteristics, user perceptions and behavioural impacts.” *International Journal of Man-Machine Studies 38*, no.3 (1993): 475-487. Accessed 19 March 2018. https://doi.org/10.1006/imms.1993.1022

Del Castillo, Michael. “Power to the User: Accenture and Microsoft are changing identity with Ethereum.” *Coindesk*, 22 June 2017. https://www.coindesk.com/power-to-the-user-accenture-and-microsoft-are-changing-identity-with-ethereum/

Deloitte. “Blockchain – Enigma. Paradox. Opportunity.” Deloitte University Press, 2016. Accessed 17 March 2018. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

Der, Uwe, Stefan Jähnichen and Jan Sürmeli. “Self-sovereign identity – opportunities and challenges for the digital revolution.” *ArXiv*, December 2017. Accessed 3 May 2018, https://arxiv.org/pdf/1712.01767.pdf

Development Initiatives. “Global humanitarian assistance report 2017.” *Development Initiatives*, June 2017. Accessed 14 April 2018. http://devinit.org/post/global-humanitarian-assistance-2017/

Dillon, Andrew. “User acceptance of information Technology.” In *Encylcopedia of Human Factors and Ergonomics*, edited by Waldemar Karwowski. London: Taylor and Francis, 2001. Accessed 17 March 2018. https://www.researchgate.net/publication/279683883_User_acceptance_of_information_technology

Dillon, Andrew and Michael Morris. “User acceptance of new information technology: Theories and models.” In *Annual Review of Information science and technology Vol.31*, edited by Martha Williams, 3-32. Medford: Information Today, 1996.

Dix, Alan, Janet Finlay, Gregory Abowd and Beale Russell. “Human-Computer Interaction”. Essex: Pearson Education Limited, 2004. Accessed 15 March 2018. http://fit.mta.edu.vn/files/DanhSach/__Human_computer_interaction.pdf

Drescher, Daniel. *Blockchain basics – a non-technical introduction in 25 steps*. Frankfurt am Main: Apress, 2017.

Dunphy, Paul and Fabien Petitcolas. “A first look at identity management schemes on the blockchain.” *IEEE Security & Privacy*, (to appear July 2018). Accessed 23 March 2018. https://arxiv.org/pdf/1801.03294.pdf

Farrington, John, Kay Sharpa and Disa Sjoblom. “Targeting approaches to Cash Transfers: Comparisons across Cambodia, India and Ethiopia.” Overseas Development Institute, June 2007. Accessed 15 April 2018. https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/3924.pdf

Fearon, James. “What is Identity (As we now use the Word)?” Thesis, Standford University, 3 November, 1999.

Ford, Bryan. “Pseudonym Parties: An offline foundation for online accountability.” *MIT*, 27 March 2007. Accessed 28 May 2018, http://www.brynosaurus.com/log/2007/0327-PseudonymParties.pdf

Gautham, “Proof of individuality, the New-Age security of blockchain.” *News BTC*, 5 April 2016. Accessed 28 May 2018. https://www.newsbtc.com/2016/04/05/proof-of-individuality-blockchain-security/

Gelb, Alan and Clark, Julia. “Identification for Development: The Biometrics Revolution.“ CGD Working Paper 315, Center for Global Development, Washington DC, January 2013. Accessed 27 March 2018. http://www.cgdev.org/content/publications/detail/1426862

GSMA. “Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid.” *GSMA*, 14 December, 2017. Accessed 24 April 2018. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf

GSMA. “Mobile money, humanitarian cash transfers and displaced populations.” *GSMA*, 23 May 2017. Accessed 10 April 2018. https://www.gsma.com/mobilefordevelopment/programme/mobile-for-humanitarian-innovation/mobile-money-humanitarian-cash-transfers/

Gould, John, Stephen Boies and Lewis Clayton. “Making usable, useful, productivity-enhancing computer applications.” *Communications of the ACM 34*, no.1 (1991):74-85. Accessed 19 March 2018. https://dl.acm.org/citation.cfm?id=99993

Graham, Mark. “Inequitable distributions in Internet geographies: The Global South is gaining access, but lags in local content.” *Innovations* 9, no.3/4 (2014): 3-19. Accessed 28 April 2018. https://doi.org/10.1162/inov_a_00212

Hammudoglu, Joren, J. Sparreboom, J.I. Rauhamaa, J.K. Faber, L.C. Guerchi, I.P Samiotis, S.P. Rao, J.A. Powelse. „Portable Trust: Biometric-based authentication and Blockchain storage for self-sovereign identity systems.” Student Project, Delft University of Technology, 12 June 2017. https://arxiv.org/pdf/1706.03744.pdf

Harvey, Paul. “Cash and vouchers in emergencies”. Humanitarian Policy Group Briefing Paper, February 2005. London: Overseas Development Institute. Accessed 15 April 2018. https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/432.pdf

Harvey, Paul. “Cash-based responses in emergencies.” Humanitarian Policy Group Report 24, January 2007. London: Overseas Development Institute. https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/265.pdf

Harvey, Paul and Sarah Bailey. “Cash transfer programming and the humanitarian system.” Background note for the High Level Panel on Humanitarian Cash Transfers, April 2015. London: Overseas Development Institute. Accessed 20 April 2018. https://www.odi.org/publications/9455-cash-transfer-programming-and-humanitarian-system

Harvey, Paul and Sarah Bailey. “State of evidence on humanitarian cash transfers.” Background note for the High Level Panel on Humanitarian Cash Transfers, March 2015. London: Overseas Development Institute. Accessed 29 April 2018. https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9591.pdf

Higgs. Edward. *Identifying the English: A History of Personal Identification 1500 to the Present.* London: Continuum, 2015.

ICRC. “Means of Personal Identification”, Accessed 5 February 2018. www.icrc.org/eng/assets/files/other/means_of_personal_id_eng.pdf

International organisation for standardization (ISO). “Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability.” 9241-11:1998, 15 March 1998, accessed 20 April 2018, https://www.sis.se/api/document/preview/611299/

Internet World Statistics. “Internet growth statistics 1995 to 2018.” Accessed 30 April 2018, https://www.internetworldstats.com/emarketing.htm

Irrera, Anna. “Accenture, Microsoft team up on blockchain-based digital ID network.” *Reuters,* 19 June 2017. Accessed 14 April 2018. https://www.reuters.com/article/us-microsoft-accenture-digitalid/accenture-microsoft-team-up-on-blockchain-based-digital-id-network-idUSKBN19A22B

James, Eric. *Managing Humanitarian Relief: An operational guide for NGOs.* Warwickshire: Intermediate Technology Publications Ltd., 2008.

Jacobovitz, Ori. “Blockchain for Identity Management.” Technical Report, The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-

Gurion University, Israel, 11 December 2016. Accessed 15 March 2018, https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf

Jacobsen, Katja. "On humanitarian refugee biometrics and new forms of intervention", *Journal of Intervention and Statebuilding* 11, no.4 (2017): 529-551. Accessed 26 March 2018. DOI: https://doi.org/10.1080/17502977.2017.1347856

Juskalian, Russ. "Inside the Jordan refugee camp that runs on blockchain." *MIT Technology Review*, 12 April 2018. Accessed 10 May 2018. https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain

Kewell, Beth, Richard Adams and Glenn Parry. "Blockchain for good?" *Strategic Change* 26, no.5 (2017): 429-437. Accessed 26 March 2018. https://doi.org/10.1002/jsc.2143

King, Nigel and Christine Horrocks. *Interviews in Qualitative Research.* London: Sage, 2010

Ko, Vanessa and Andrej Verity. "Blockchain for the humanitarian sector: future opportunities." Digital Humanitarian Network, November 2016. Accessed 7 May 2018. http://digitalhumanitarians.com/resource/blockchain-humanitarian-sector-future-opportunities

Kshetri, Nir. "Will blockchain emerge as a tool to break the poverty chain in the Global South?" *Third World Quarterly 38,* no.8 (2017): 1710-1732. Accessed 11 March 2018. https://doi.org/10.1080/01436597.2017.1298438

Kumar Adithya. "The missing 1.1 billion: blockchain-based digital identities as a driver of inclusion." *Procivis*, 4 April 2018. Accessed 19 May 2018. https://procivis.ch/2018/04/04/the-missing-1-1-billion-blockchain-based-digital-identities-as-a-driver-of-inclusion

Kuner, Christopher and Massimo Marelli. *ICRC Handbook on Data Protection in Humanitarian Action*. Geneva: ICRC, 2017. Accessed 20 May 2018. https://www.privacy-web.nl/cms/files/2017-07/handbook-data-protection-and-humanitarian-action-2-.pdf

Leary, Mark, David Wheeler and Brant Jenkins. "Aspects of Identity and Behavioural Preference: Studies of Occupational and Recreational Choice." *Social Psychology Quarterly* 49, no.1 (1986): 11-18. Accessed 6 May 2018. http://dx.doi.org/10.2307/2786853

Levin, Avner, Anupa Varghese and Michelle Chibba. "Know your customer standards and privacy recommendations for cash transfers." Enhanced Response Capacity Project 2014-2015, UNHCR and World Vision, April 2015. Accessed 15 April 2018. http://www.cashlearning.org/downloads/erc-know-your-customer-web.pdf

Lewis, Antony. “Bits on blocks.” 17 May 2017. Accessed 12 May 2018. https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

Lewis, Antony. “A gentle introduction to blockchain technology”. *Brave New Coin*, 2015. https://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf

Lutz, Al, Amos Doornbos, Anna Kehl, Annette Ghee and Laura DePauw. “Data protection, privacy and security for humanitarian and development programs.” World Vision, Discussion Paper, 2017. Accessed 18 May 2018. http://wvi.org/health/ict4d

Maddix, Frank. *Human-Computer Interaction: Theory and Practice*. New York: Simon & Schuster, 1990.

Malik, Tariq and Anita Mittal. “Technical Standards for Digital Identity.” International Bank for Reconstruction and Development / The World Bank, 2017. Accessed 14 May 2018. http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf

Marcia, James. “Development and Validation of Ego Identity Status.” *Journal of Personality and Social Psychology 3,* no.5 (1966): 551-558

Mattila, Juri. “The blockchain phenomenon – The disruptive potential of distributed architectures.” ETLA Working Papers No.38, 10 May 2016. Accessed 15 March 2018, https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-38.pdf

Miller, Ron. “The promise of managing identity on the Blockchain.” *Techcrunch*, 10 September 2017. Accessed 17 March 2018. https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/

Moore, Gary and Izak Benbasat. “Development of an instrument to measure the perceptions of adopting an information technology innovation.” *Information Systems Research 2,* no.3 (1991): 192-222

Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” 2008. Accessed 5 June 2018, https://bitcoin.org/bitcoin.pdf

Nelms, Taylor, Bill Maurer, Lana Swartz and Scott Mainwaring. “Social payments: innovation, trust, Bitcoin, and the sharing economy.” *Theory, Culture and Society 35*, no.3 (2018): 13-33. Accessed 10 June 2018. http://journals.sagepub.com/doi/abs/10.1177/0263276417746466

Neue Zürcher Zeitung (NZZ). “Bis zu 29’000 Schweizer Facebook-Nutzer sind vom Datenskandal betroffen.” *NZZ online,* 5 April 2018. Accessed 23 May 2018.

https://www.nzz.ch/wirtschaft/facebook-cambridge-analytica-koennte-daten-von-87-millionen-menschen-missbraucht-haben-ld.1374393

Nagy, Peter and Bernadett Koles. “The digital transformation of human identity: Towards a Conceptual Model of Virtual Identity in Virtual Worlds.” *The International Journal of Research into New Media Technologies* 20, no.3 (2014): 276-292. Accessed 5 May 2018. https://doi.org/10.1177/1354856514531532

Nickerson, Raymond. “Why Interactive computer systems are sometimes not used by people who might benefit from them.” *International Journal of Man-Machine studies 15,* no.4 (1981): 469-483

Nyst, Carly, Paul Makin, Steve Pannifer and Edgar Whitley. “Digital Identity: Issue Analysis Executive Summary”. Consult Hyperion, 27 July 2016. Accessed 8 May 2018. http://www.chyp.com/

Othman, Asem and John Callahan. “The Horcrux Protocol: A method for decentralized biometric-based self-sovereign identity.” *ArXiv*, 20 November 2017. Accessed 1 May 2018. https://arxiv.org/abs/1711.07127

Overseas Development Institute. “Doing cash differently. How cash transfers can transform humanitarian aid.” Overseas Development Institute, September 2015. Accessed 1 May 2018. https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf

Patton, Michael. *Qualitative Evaluation and Research Methods*. Newbury Park, CA: Sage, 1990.

Paynter, Ben. “How Blockchain could transform the way international aid is distributed.” *Fastcompany*, 18 September 2017. Accessed 23 April 2018. https://www.fastcompany.com/40457354/how-blockchain-could-transform-the-way-international-aid-is-distributed

Pisa, Michael and Matt Juden. “Blockchain and economic development: Hype vs. reality”. CGD Policy Paper 105, Center for Global Development, July 2017. Accessed 5 May 2018. https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality

Pon, Bryan, Chris Locke and Tom Steinberg. “Private-Sector digital identity in emerging markets.” Caribou Digital Publishing, 2016. http://cariboudigital.net/new/wp-content/uploads/2016/08/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf

Preukschat, Alex. “Self sovereign identity – a guide to privacy for your digital identity with blockchain.” *Medium*, 11 January 2018, accessed 20 April 2018.

https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

Price, Geraint. “The benefits and drawbacks of using electronic identities.” *Information Security Technical Report 13*, 2 (2008): 95-103. Accessed 26 March 2018. https://doi.org/10.1016/j.istr.2008.07.002

“Proof of Individuality”, Whitepaper, accessed 27 May 2018, http://proofofindividuality.online

Renaud, Karen and Judy van Biljon. “Predicting Technology Acceptance and Adoption by the Elderly: A Qualitative Study.” In Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists, Wilderness, South Africa, (6-8 October, 2008): 210-2019. Accessed 19 March 2018. https://dl.acm.org/citation.cfm?doid=1456659.1456684

Roberts, Jeff. “Microsoft and Accenture Unveil Global ID System for Refugees.” *Fortune*, 19 June 2017. Accessed 10 March 2018. http://fortune.com/2017/06/19/id2020-blockchain-microsoft/

Rode Kruis. “1 Euro Voroof scheelt gemiddeld 7 euro achteraf.” Accessed: 4 May 2018. https://voorkomderamp.rodekruis.nl/over-ons

Saxby, Stephen. “The 2013 CLSR-LSPI seminar on electronic identity: The global challenge - Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11-15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand.” *Computer Law and Security Review 30*, 2 (2014): 112-125. Accessed 11 May 2018. https://doi.org/10.1016/j.clsr.2014.01.007

Schmidt, Eric and Jared Cohen. *The New Digital Age: Reshaping the Future of People, Nations and Business.* Hachette, UK: John Murray, 2013.

Schwartz, Jeffrey. “Microsoft among those pitching Blockchain at U.N. summit to end identity crisis.” *Redmond Magazine*, 25 May 2016. Accessed 12 May 2018. https://redmondmag.com/blogs/the-schwartz-report/2016/05/microsoft-among-those-pitching-blockchain.aspx

Smedinghoff, Thomas. “Solving the legal challenges of trustworthy online identity.” *Information Security Technical Report 28*, no.5 (2012): 532-541. Accessed 9 May 2018, https://doi.org/10.1016/j.clsr.2012.07.001

Smith, Gabrielle, Ian Macauslan, Saul Butters and Mathieu Trommé. “New technologies in cash transfer programming and humanitarian assistance.” The Cash Learning Partnership (CaLP), 1 January 2011. Accessed 20 April 2018.

https://www.humanitarianlibrary.org/resource/new-technologies-cash-transfer-programming-and-humanitarian-assistance-0

Sompolinsky, Yonatan and Aviv Zohar. “Bitcoin’s underlying incentives.“ *Acmqueue* 15, no.5 (2017): 1-24. Accessed 10 June 2018. https://queue.acm.org/detail.cfm?id=3168362

Sovrin Foundation. “Sovrin Glossary.” White paper, 29 September 2016. https://www.evernym.com/wp-content/uploads/2017/07/Sovrin-Glossary.pdf

Sovrin Foundation. “The inevitable rise of self-sovereign identity.” White Paper, 20 September 2016. Accessed 3 May 2018. https://www.evernym.com/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Stephens, Sandra. “Dive into liquid democracy.” *Democracy Earth*, 9 November 2017. Accessed 27 May 2018. https://words.democracy.earth/dive-into-liquid-democracy-cded2d9ba1d6

Sustainia. “Hack the Future of Development Aid.” Sustainia, The Danish Ministry of Foreign Affairs and Coinify, 2016. Accessed 12 March 2018. https://reliefweb.int/report/world/hack-future-development-aid

Sundararajan, Sujha. “Microsoft, Hyperledger, UN joint blockchain identity initiative.” *Coindesk*, 23 January 2018, accessed 24 April 2018. https://www.coindesk.com/microsoft-hyperledger-un-join-blockchain-identity-initiative/

Swartz, Lana. “Blockchain dreams: imagining techno-economic alternatives after Bitcoin.” In *Another economy is possible: culture and economy in a time of crisis,* edited by Manuel Castells et al., 82-105. Malden: Polity, 2017. http://llaannaa.com/papers/Swartz_Blockchain_Dreams.pdf

Swanson, Burton. “Information Channel Disposition and use.” *Decision Science 18*, no.1 (1987): 131-145. https://doi.org/10.1111/j.1540-5915.1987.tb01508.x

Swanson, Burton. “Information System implementation: Bridging the gap between design and utilization.” Burr Ridge, IL: Richard Irwin, 1988

The Guardian. “Secret aid worker: we don’t take data protection of vulnerable people seriously.” *The Guardian,* accessed 20 May 2018, https://www.theguardian.com/global-development-professionals-network/2017/jun/13/secret-aid-worker-we-dont-take-data-protection-of-vulnerable-people-seriously

Tobin, Andrew and Drummond Reed. “The inevitable Rise of self-sovereign identity.” White Paper, Sovrin Foundation, 29 September 2016. https://www.evernym.com/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Townzen, Rachel. “Trusting tech initiatives isn’t easy for most Syrians.” *News Deeply,* 21 September 2016. Accessed 23 March 2018. http://pulitzercenter.org/reporting/trusting-tech-initiatives-isnt-easy-most-syrians

UNHCR. “Biometric Identity Management System.” Accessed 23 April 2017. http://www.unhcr.org/en-us/protection/basic/550c304c9/biometric-identity-management-system.html

UNOCHA. 2014 ECOSOC Humanitarian Affairs Segment. Side-event on Interoperability, Panel note led by the Permanent Mission of Turkey, 25 June 2014, accessed 17 April 2018. https://www.unocha.org/sites/unocha/files/dms/Documents/HAS%20Interoperability%20Side-Event%2024%20JUNE%202014%20FINAL.pdf

USAID. “Identity in a digital age.” 11 September 2017. Accessed 12 April 2018. dhttps://www.usaid.gov/digital-development/digital-id/report

Venkatesh, Viswanath and Fred Davis. “A theoretical extension of the technology acceptance model: Four longitudinal field studies.” *Management Science* 46, no.2 (2000): 186-2004.

Venkatesh, Viswanath, Michael Morris, Gordon Davis and Fred Davis. “User acceptance of information technology: Toward a unified view.” *MIS Quarterly 27*, no.3 (2003): 425-478.

Wagner, Kai. “Identity as a bottleneck for blockchain: the road to self sovereign identity.” *Jolocom*, 18 January 2018. Accessed 22 April 2018. https://jolocom.com/identity-bottleneck-blockchain-road-self-sovereign-identity/

Windley, Phillip. “How blockchain makes self-sovereign identities possible.” *Computerworld*, 10 January 2018. Accessed 3 May 2018, https://www.computerworld.com/article/3244128/security/how-blockchain-makes-self-sovereign-identities-possible.html

Woodward, John, Nicholas Orlans and Higgins Peter. *Biometrics: Identity Assurance in the Information Age*. New York: McGraw-Hill Osborne Media, 2002.

Wolfond, Greg. “A Blockchain ecosystem for digital identity: Improving services delivery in Canada’s public and private sectors.” *Technology Innovation Management Review* 7, no.10 (2017): 35-40. Accessed 12 March 2018. http://doi.org/10.22215/timreview/1112

World Bank. “Cash transfers in humanitarian contexts: Strategic Note - Final draft prepared for the principals of the inter-agency standing committee.” World Bank, 30 April 2016. Accessed 18 April 2018. https://interagencystandingcommittee.org/system/files/

humanitarian_cash_transfers_final_copyiedited.pdf

World Bank. "Principles on Identification for sustainable development: toward the digital age." Working Paper, World Bank, Washington D.C., 1 February 2017. Accessed 10 May 2018. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age

World Bank Group. "The State of Identification Systems in Africa". Working Paper, World Bank, Washington D.C., 24 August 2017. http://documents.worldbank.org/curated/en/298651503551191964/The-state-of-identification-systems-in-Africa-country-briefs

World Food Programme. "WFP SCOPE – Know them better, to serve them better." March 2017. Accessed 12 May 2018. http://documents.wfp.org/stellent/groups/public/documents/resources/wfp280992.pdf

World Food Programme. "WFP and Digital Innovation", October 2016. Accessed 12 May 2018. http://documents.wfp.org/stellent/groups/public/documents/communications/wfp287655.pdf

World Vision International. "Last Mile Mobile Solutions (LMMS)." Accessed 2 April 2018. https://www.wvi.org/disaster-management/last-mile-mobile-solution-lmms

Zambrano, Raul. "Blockchain – Unpacking the disruptive potential of blockchain technology for human development." White paper, International Development Research Centre, August 2017. Accessed 24 March 2018. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf

510. "CBA: Cash based assistance the future", *510.global,* 26 January 2018. Accessed 15 April 2018. https://www.510.global/the-future-of-cash-based-assistance-2/

510. "Data Responsibility Policy", *510.global,* accessed 10 May 2018. https://www.510.global/wp-content/uploads/2017/11/510_Data_Responsibility_Policy_V.2_PUBLIC-1.pdf

11. ANNEX

Annex 1: Outline of the interview questions

a) For respondents affiliated with CTP

Question	Aim of Question
1. Could you please briefly state your experience with Cash Transfer Programs?	*To get an understanding whether someone has practical and/or theoretical experience with CTPs.*
2. Could you please briefly state your experience with targeting and registration of beneficiaries? Was there any type of digital identity system involved?	*To get an understanding whether someone has targeted and registered themselves or designed the programme, and if they already used some digital tools to enhance efficiency*
3. Are you or your organisation familiar with blockchain?	*To see what level of knowledge the interviewee has of blockchain as many of the perceived benefits are only truly understood if you understand the technology*
4. In your opinion: Is this new way of beneficiary identity management in CBA feasible in regards to beneficiary usability and acceptance?	*To find out what it implies for a beneficiary to have more control over his or her own digital identity, but at the same time be confronted with technology he/she might not be familiar with, which can generate confusion (even if perceived to be 'user-friendly')*
5. From a beneficiary perspective, what do you believe will be pivotal factors for the usability of this proposed identity management system? e.g. compatibility/similarity with previously used systems, social influence, facilitating conditions, etc.	*To find out what (non)-functional application requirements there would be for this system?*
6. Who do you collaborate with when it comes down to targeting and registration?	*To get an understanding of who is involved in targeting and registration according to the interviewee*
7. How would your stakeholders (local authorities, volunteers, headquarters of your organisation, donors) respond if you introduce this system?	*To understand how dependent they are on their environment*

8. Inclusiveness with any given new technology is vital. Speaking from your personal or organisational experience, do you think there may be a segmnet of the beneficiaries that would struggle most with this new form of registration?	*To understand if there is a specific segment of beneficiaries that would be more prone to decline the new system, i.e. for whom it could be less accepted/usable*
9. What would you require of the system for it to convince your stakeholders to use it?	*To find out stakeholder requirements (Self-registration, open/closed, speed, etc.)*
10. What is the importance of beneficiary's being "in control" when interacting with a registration/identity management system in regards to usability and acceptance? (i.e. consent of sharing personal data, knowing what will happen with this data, understanding where and how it is stored)	*Aim of this question is to find out if beneficiaries are willing to place trust in a decentralised network rather than a known and tangible central institution and/or what may this loss of control trigger in the beneficiary*
11. What kind of laws and regulations would apply to such a system in your current environment?	*To find out which regulation should be taken into account when designing the system*
12.. How would you describe the organizational culture when it comes down to targeting and registration? e.g. careful, well-organized, safety- and privacy-first	*To understand what norms there are in their respective organisation*

b) For respondents affiliated with blockchain and/or digital identity

Question	Aim of Question
1. In your opinion, what are the main drawbacks or challenges of current digital identity systems in the humanitarian sector?	*To get an understanding of challenges of current digital identity systems from a mainly theoretical perspective (practical experience an asset).*
2. What are important attributes of a digital identity system from an end-user perspective? And from an "implementer" perspective (i.e. a humanitarian organisation)?	*To get an understanding of what the important attributes of both 'parties' are and if they overlap/differ/collide.*

3. Blockchain promises to store and transmit encrypted data more efficiently and with greater transparency than the current digital system. What are your thoughts on managing identity on a distributed ledger in the humanitarian context?	*To find out which challenges and potentials the expert foresees.*
4. Humanitarian organizations are restricted to share personal identifiable data due to data protection regulations, leading to sub-optimal coordination: Do you think storing personal data on a distributed ledger in a safe and secure way could foster trust and interoperability between different humanitarian organisations?	*To find out if a distributed ledger technology has the ability to act as a proxy of trust.*
5. To ensure inclusiveness of the most vulnerable in the system, identities should be sovereign and not depending on (but possibly strengthened by) the possession of a government recognised form of identification. In line with this thought, do you see potential of self-sovereign identities (managed on the blockchain or not) where individuals can collect identifying attributes to build up a digital identity over time?	*To explore experts' thoughts on the feasibility of a self-sovereign identity (often a very new concept for respondents).*
6. Let's say one of the goals – if not the ultimate one – is to give vulnerable and marginalised people as much control as possible over their lives, including control over their identity. Do you think creating digital identities stored on a decentralised ledger could facilitate this? Or moreover, what is needed in order to give people more control?	*To get an understanding of what is needed to ensure greater control over personal data/identity for end-users.*
7. More generally speaking, what are common pivotal factors of usability and (end-user) acceptance when new technology gets introduced in the humanitarian context?	*To find out what could ensure technology acceptance when introducing a new system and what are factors that potentially hinder the success of implementation.*