Identity Management in Developing Countries:
A SWOT-Analysis

by

Brajan Gruszka

February 2021

A Thesis submitted in part fulfilment of the

Degree of Bachelor of Science in

Economics and Management

Institute of Information Management

Leibniz University of Hannover

Examiner: Prof. Dr. Michael H. Breitner
Supervisor: Christin Karrenbauer

CONTENTS

1. INTRODUCTION

With the advent of the state, loose federations of people became ever more connected. With larger states arose new challenges of overseeing and providing for the citizenry. Modern technology has created new challenges and opportunities for this process. The global north and south have distinctive issues regarding identity management[64]. However, who takes care of those who do not belong to a state or have fled them because of persecution? Who takes care of the people on the social margins? Especially massive nations have struggled with keeping their population documented[54]. Technology seems to be moving in a direction, where this task might become feasible[64]. Nevertheless, it is uncertain if these policies and technologies will include those who have been excluded or create a more significant divide between them and the rest of a country's population. An estimated 1.1 billion people,which equals to about a seventh of the world's population, lack a proof of their legal identity[63]. Most affected are rural areas in Africa, Asia and more importantly the 21 million refugees, a population equivalent to New York's, with the majority of them being women and children [63]. Access to health, education, and bank services becomes excessively difficult for them. It is estimated that around 2.5 billion people worldwide lack access to basic financial services[34]. Moreover, the number of stateless people and refugees has increased[63]. Over the years, government initiatives regarding the promotion of digital IDs have increased drastically, because advances in technology have made it easier to implement them and the share of business that is conducted online continues to grow[48]. Numerous countries
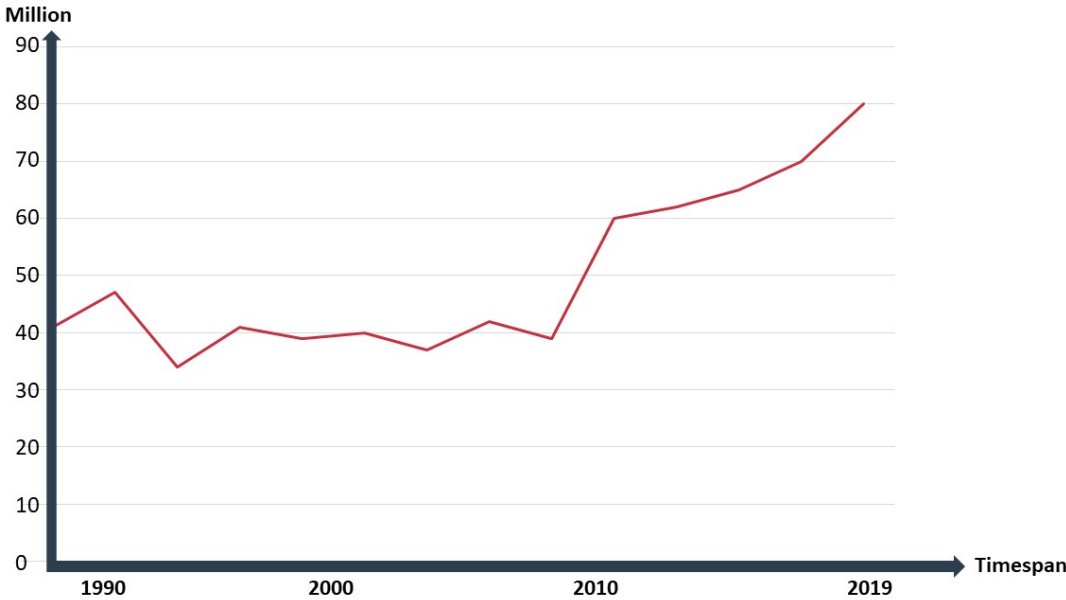

Figure 1.1: Number of displaced people in the world in 2019 in which refugees make up 21 million, adapted from[63]

incited new projects in the area of identity management systems to reduce these numbers and increase inclusion[54]. The Main drivers behind identity Management (IDM) are improving

authentication and identification mechanism, thus reducing crime, combat terrorism, eliminating identity theft, controlling immigration, providing better governmental services to citizens and immigrants and stopping benefit fraud[23]. Blockchain technology has been known for a while, however the "mega trend"[60] of cryptocurrency was the impetus that shifted the technology into the public sphere. This was the focus of blockchain technology for the years to come[70], but in recent years, it has found its way into identity management[3]. Identity management has been struggling in various areas of application. Data redundancy being the most prominent[38]. Digital identity management systems lack crucial differentiation between classical paper-based methods of identification[12]. Especially periphery countries suffer from various degrees of technological mismanagement[30]. There exists no formal registration with the associate authorities in African countries[29]. There is no overview of which people are eligible to receive state aid[29]. The countries currency is not being used in parts of the countries[29]. The main victims of this mismanagement are marginalized groups in these countries[64]. The World Bank has been actively advocating for a proof of identity for these groups[34]. Identity is a key component for the state and also for inclusion into the financial sector and to have access to services and rights[64]. There are more than 1,5 billion people with no access to these services and rights because they lack proper proof of identification[34]. Most of these people live in Africa and Asia[63], countries where the number of registered births drops as low as 39%[64]. They generally belong to the poorest strata in the world[35]. Together with the UN ID2020 has been created to combat these numbers[34]. New development in blockchain and identity management might hold the key to solving these problems[64]. New Methods of decentralized identity management are being tested[64]. Some of these in Combination with Self-Sovereign-Identity, a new approach to identity management often closely linked with blockchain technology[57]. Some of these methods are already being used by humanitarian organizations[17]. This bachelor thesis will explore the current problems with identity management in developing countries, thus establishing a status quo on the topic. It will take a closer look at the emerging new concept of SSI and determine if it can be used for the socio-economic inclusion of marginalized groups and how it compares to the status quo.

Based on a literature review on the topic of identity management, this thesis presents the following three research questions:

- What is the impact of identity management systems in developing countries?

- How do they contribute to the socio-economic inclusion of marginalized groups?

- How can Self-Sovereign Identity management systems impact this status quo?

The following chapter will establish a theoretical background to answer the research questions. In the third chapter, the research methodology will be established. In the fourth chapter, the status quo of identity management in developing countries will be established based on the literature review. For this purpose, a SWOT-matrix will be developed. This will lay the foundation for further discussion on the topic with regarding marginalized groups in periphery countries.

8.   CONCLUSION

The increasing identity management problems in the developing world need to find a solution. Marginalized people are ever more left behind by new IDM projects and require special attention when designing such systems. The thesis's main goal was was to show the current state of identity management in developing countries, how it affects marginalized groups and finally to determine how the new identity management concept of SSI could contribute in this area. The conclusion of this thesis shall present an answer to the thesis's three research questions :

In order to answer the **first question:** "What is the impact of identity management systems in developing countries?" the main section presented a literature review and a subsequent SWOT-analysis, thus presenting the current status quo. The current trend shows identity management systems in developing countries as a double-edged sword. On the one hand they provide the goals they seek after. They create social and financial inclusion, strengthening the efficiency of governmental services and reduce fraud. On the other hand, they often suffer from poor design decisions and mismanagement[30][69]. They create new problems and often amplify already existing problems. While some forms of inclusion are successful, other forms of exclusion are generated by the technology[38][51]. Central to most IDM projects in developing countries is the lack of security and privacy[53][33]. Both on the technological end and in the lack of fitting policies. This lack of political motivation can be observed among a majority of these projects, often leading to failure at the enrollment state[30]. Significantly, the usage of biometric data is often out of place and without considering the technology's limitations[69]. KYC requirements and SIM registration prove to be major obstacles to the financial inclusion of marginalized groups[41]. IDM projects seek to ease these processes, yet governmental intervention proved otherwise[41]. This puts to question whether IDM projects are truly for purpose of integration or to foster exclusion of certain peoples' groups such as the example of the Rohingya refugees[41]. The security of Aadhaar, the Ugandan national ID system, humanitarian organizations, Nigerian national IDM and, Thai national ID cards suffer from lackluster security[33][38][30][17][51]. Aadhaar suffers from challenges of data privacy, ghost accounts, exclusion of genuine beneficiaries, and government surveillance issues[16]. Storage of a whole nation's biometric identifiers is often done via a central database, creating a single point of interest for external attacks and a prime target for corporations[53]. These databases often lacked independent IT-audits to ensure reliability and security of the software as well as database integrity[53]. Another obstacle is political backing in developing countries. IDM projects lack the necessary structure of legal and political aspects often as much as they lack technological infrastructure[30]. Improvements are observable for the nation's citizenry; however, they did not lack formal identification before the integration of IDM projects, hence improvements were made in speed and efficiency instead of creating new identities and inclusion.

Regarding the **second question:** "How do they contribute to the socio-economic inclusion of marginalized groups?" examples from the literature review and SWOT-matrix have been chosen to deal with marginalized groups.

The herculean task of granting every citizen in India a legal form of identity and integrating them into financial institutions still stands unaccomplished. In India Aadhaar, however successful, relies on government propaganda for its legitimacy and "accomplishments"[38]. Nevertheless, it represents a first step towards digital identity solutions on a major national scale. The Indian government failed to consider the minority which indulges in corrupt practices and has instead deployed an untested and fragile technology[38]. The one's paying the price are the victims of corruption[38]. In the humanitarian sector, refugees suffer from a myriad of mismanagement issues[51]. This has led to fear and misconception of the technology, creating negative knock-off effects such as domestic violence and fraudulent identity enrollment[51]. A lack of transparency in the process created fear of racial profiling[51]. Identity updates were very slow and inefficient[51]. Often documents lost their credibility before refugees had the chance to renew them[51]. This, in turn, created further hurdles for refugees and made them vulnerable. The systems in use lacked conformity to the situation as they were designed for general purposes and lacked necessary aspects for refugee enrollment, identification and authentication[51]. Central databases provide a security weakness; however, they also provide a potential tool for easier integration of refugees and creating upwards mobility in the host country. In large national states, such as India, Aadhaar has made it possible to easier integrate from city to city as government benefits could be claimed via any valid service stations, making migration from poverty-stricken regions more possible and less bureaucratic[38][53]. Another strength of centralized solutions over decentralized solutions is their ease of implementation[20], which plays a major role in developing countries. Marginalized groups are often cited as the prime beneficiaries of IDM projects[54]. However, this is not always the case. Biometric inaccuracies in Aadhaar create further challenges for marginalized people[38]. Evidence does not support a substantial gain from Aadhaar-integration into welfare programs[38]. The program has led to higher monthly transaction costs and cases of exclusion and denials, which has led to suffering of considerable indignities[38]. Inclusionary benefits from marginalized groups are observable, however, they often seem to be just side-effects of IDM programs rather than one of their primary goals. Technological penetration in developing countries varies strongly between regions. The most significant ease to help these countries implement any kind of identity management solution would be to assisting with the provision of necessary technology and knowledge and infrastructure[7]. The **final research question:** "How can Self-Sovereign Identity management systems impact this status quo?" was analyzed with use-cases developed in the thesis and compared with the status quo from the first research question. The impact of the technology has been weighted against the results of the second research question, thus creating a concise overview of which use-cases could benefit or suffer from an IDM implementation with SSI and blockchain as its foundation. SSI attempts to address inherent issues in existing identity models in which user's data are scattered among multiple SPs and where users have limited control over their identity[3]. SSI tries to reduce the likelihood of data breaches and identity fraud as identity providers no longer have to store users' data[56]. The digital nature of registration systems and the promise of technologies such as blockchain, have led to aspirations that individuals may have greater control over their digital identities[3].

Digital technologies have great potential for strengthening user access to registration systems, but this has not been prioritized. Compared to developed countries, developing countries often lack the technological infrastructure for DLT solutions[64]. DLT identity management solutions, same as a citizenship right now, will come with rights and sought-after statuses, while others will predominantly represent liabilities[29]. Digital identity can therefore make segregation more effective[29]. Hence, reducing the social and economic inclusion of marginalized groups.[29]. The issue of integrating marginalized groups into identity management schemes comes from already existing real-world inequalities between identities and citizenship[29]. It is unclear at this moment, how a digital identity such as SSI would affect and interact with this reality. Before creating national ID schemes, it is necessary to consider what citizenship in the "real world" contains and means[29]. Nevertheless, digital identity based on DLT carries a huge potential if designed correctly[29]. The creation of SSI solutions without blockchain is possible, yet the combination ensures that the key concepts of SSI remain uphold[11]. KYC2 with decentralized trust anchors is currently being developed with privacy by design and linkage to possible blockchain solutions[56]. Possibly elevating the difficulties of marginalized groups when going through KYC and CDD. In specific cases, such as when refugees get their identity documents confiscated by human traffickers in the Mediterranean[17], SSI could create a persistent identity. However, SSI solutions often rely on mobile phones as storage for private keys, which in such a scenario would be just as vulnerable as documents. The two major issues of SSI are its lack of a key recovery mechanism and the apolitical views of its proponents[47][17][64]. Key recovery on SSI with blockchain is currently being formulated[47]. Nevertheless, a safe, user-friendly and standardized method does not exist. This created a higher risk of loss of private keys and the user's identity. This links to another uncertainty, whether users will be able to keep their keys safe and avoid losing them[17]. Creating a fundamental understanding of SSI for users is required as it puts the user at the center of the concept. These onboarding costs are still to be determined[47]. SSI with blockchain offers a solution to these problems, however in turn, they create new problems[47]. SSI is plagued by technological uncertainty[47][64][29]. Research is done to improve technological functionality, yet it often fails to address the "real world" situation of identity. It fails to resolve root problems and challenges of accessing official and valid identity[17]. In the context of refugees experimental digital solutions have amplified existing patterns of control structures[44]. SSI can be seen as an apolitical technology, yet fundamentally addresses a political issue[17]. Hence, this apolitical lens paints the technology as neutral[17]. However, it has the risk, like all prior identity management models, to become a tool for surveillance and further business instead of socio-economic goals[17][3]. There is a risk that the benefits and visions of SSI will be subverted and the schemes will be incorporated into existing power mechanisms[17]. SSI has greater potential to be a tool for socio-economic inclusion[64]. Yet, if it is to have a pro-social impact and enhance the well being of marginalized groups, it must avoid these pitfalls of outside control. Contrary to the concept of SSI, before its adaptation, it would benefit from a centralized approach to develop the concept and technological foundation. The W3C consortium is already creating standards for DIDs[64]. If proponents of SSI were to combine the central idea of SSI

and standardize it, they would have higher chances of adaptation. Several SSI providers and prototypes have sprung up, yet there is no consensus on the type of blockchain to be used. This puts SSI at high risks of being hijacked and subverted and creating a concept which is doomed to be centralized like the user-centric approach[3][20]. Lessons from past identity models should play a crucial role in the developing SSI. Fixing technological issues is important, yet historical development and case-studies should play a broader role in development of a functioning SSI concept. Weaknesses from past IDM projects should be considered more strongly in current SSI incentives. There is only one shot at getting SSI right, and proponents of SSI are dreaming of a decentralized utopia with revolutionary market mechanisms, yet fail to conceive past experiences of similar projects and build upon them. SSI can offer a few solutions in different scenarios; it should be prototyped in virtual spaces such as social media and web applications before making its step towards national identity management. Clear requirements for technical and political foundations should be established for developing countries that wish to implement IDM projects based on SSI. While SSI needs to stay true to its core values of decentralization, privacy and user-centric approach, the concept's development would benefit from a centralized approach under a free software license such as GNU.

Lastly, a research agenda regarding identity management systems based on SSI and blockchain has been presented, revealing technological uncertainties and the political realities of the technology, which still require further academic attention. SSI with blockchain does have untapped potential, however like all identity managements before it runs the risk of being co-opted and hijacked by the power structures it seeks to undermine, thus strengthening existing inequalities and fostering exclusion rather than inclusion of marginalized people.