frontiers

3 Stages of a Pan African Identity Framework for Establishing Self-Sovereign Identity with Blockchain

S. Solomon Darnell, PhD [1,4,*], **Eddie J. Kago** [2], **Joseph Sevilla** [3]

[1] *Executive Director, Solomon Ventures LLC, Nairobi, Kenya*
[2] *Executive Director, Vibranium ID LLC, Nairobi, Kenya*
[3] *Director @iLabAfrica, Strathmore University, Madaraka Estate, Kenya*
[4] *Research Director @iLabAfrica, Strathmore University, Madaraka Estate, Kenya*

Correspondence*:
S. Solomon Darnell
sdarnell@strathmore.edu

ABSTRACT

The African continent (specifically its overwhelming in(animate) resources) is often referred to as the sleeping giant by magazines, blogs, research presentations and articles, and NGOs (such as World Bank Morris et al. (2009); Cobbing and Hiller (2019)). Reasons for this moniker/title include the continents plentiful natural resources, its large and quickly growing young population, and the young populations quick adoption and acclimatization to technology. Most countries on the continent are known as developing countries due to lack of access to safe drinking water, reliable electricity and roads, sanitation and hygiene, and a high number of people with tropical/infectious diseases. However, due to the usefulness of cellular phones and technology, several countries and companies within them have focused on cell phone proliferation (91% in Kenya). Smart phone usage allows Kenyans access to the world's information and potentially endless innovation. Given a large number of Kenyans with smartphones use social media coupled with the advent of Europe's GDPR (general data protection regulation), African identity and its associated data became an area of great interest. As the world is quickly progressing into a digital economy, a solution must be created that allows us to regain and control our identities, doing our best to ensure losing such is infinitely close to computationally and probabilistically impossible/improbable. Developing a blockchain based identity backbone, using biometrics and historical family information while allowing government based identification documents is the best way forward. Three stages have been identified as necessities to accomplish the development of this system, before opening it further beyond the pan African world-wide community. The three stages are defined by systems that allow for biometric/demographic registration (stage 1), interoperability and security hardening (stage 2), and biometric modality data analysis/organization/association (stage 3).

Keywords: Africa, self-sovereign, identity, blockchain, biometrics

1 INTRODUCTION

For the last 6 years identity in Africa has been put in the spotlight by several countries on the continent and organizations like World Bank, along with other NGOs (non-governmental organizations). Sustainable

development goals defined by the World Bank have helped lead to this focus Bank-ID4D (2017). Aside from external policy makers and institutions, Kenya has Vision 2030 which outlines world class infrastructure facilities and services where "equality is entrenched, irrespective of one's race, ethnicity, religion, gender or socio-economic status" and "nine governance principles shall be adhered to;" one of which is "Decentralization" Kenya (2008). Decentralization is exceptionally important to Kenya, as it is one of the nine governing pillars of Vision 2030. A companion idea supporting decentralization is "upgrading national ICT infrastructure" which includes the implementation of "Public Key Infrastructure (PKI) to authorize and authenticate information systems in the country". Blockchain is a decentralized distributed computing platform that currently uses PKI to maintain security and privacy. Another companion idea, one supported by our proposed system, is "development of a national addressing system project to identify streets, buildings, plots and other infrastructure and allocating them a street address" Kenya (2008). Currently, Kenyans in areas of low infrastructure can only describe where they live. Our system will allow for such a description to be added as demographic data, along with coordinates. This system will be an aide to the street addressing system of Vision 2030, as global coordinates must correspond to physical addresses. Our proposal will serve as a model for African countries with existing citizen data infrastructures and for countries with limited identity systems.

This speaks to the absolute necessity of a self sovereign identity (SSI) system based on a decentralized, incorruptible ledger. As a Pan-African self-sovereign Identity Framework, our proposed system embodies the primary aspects of a foundational identity system.

2 MOTIVATION

Is there still a way to contribute to human digital infrastructure? As identity is one of the most fundamental and primary aspects of physical identity, is there a individual controlled trustworthy digital system that exists outside of governments and not completely controlled by an international conglomerate? How can we design, build and setup such infrastructure to not only last past our generation and be created in such a way that its not exploitative? Can we build such an infrastructure that can be monetized but does not require people with the least resources to pay unless they desire it? Can we build digital infrastructure that can also be used by citizens in post-colonial countries who have so far been close to left out of the fourth industrial revolution? Can we design our addendum to the world's digital infrastructure that is different that what currently exists? Finally, can we build digital infrastructure that holds up in times of national and international tragedy, stress and catastrophe?

2.1 Why Pan-African?

Within AI research, a common technique of calculating a "good enough" solution to an NP complete problem is to solve a similar problem of reduced complexity. In an attempt to create a robust self-sovereign identity system to satisfy all humans on the planet it follows that attempting to create a robust identity system for the Pan-African context Du Bois (1974) is a similarly challenging problem that when solved will be a "good enough" solution to the parent problem. Pan-African's represent a segment of the population that is represented thoroughly throughout the world, often at the extremes of society. It seems when developing an identity system to serve everyone we can design for the population that can approximate the full breadth and depth of humanity.

2.2 Young Mobile Population

Since the year 2000, the population of the African continent has nearly doubled, from around 815 million to 1.34 billion, based on figures from PopulationOf dot net pop (2020). With such a quickly growing population, it follows that the median age is not very high, at 24 years old pop (2020). Mobile device usage

is consistently growing on the continent, specifically in sub-Saharan Africa, and is projected to continue Intelligence (2020). In Kenya alone, mobile phone proliferation surpassed 100% by the end of 2018 Tanui (2018).

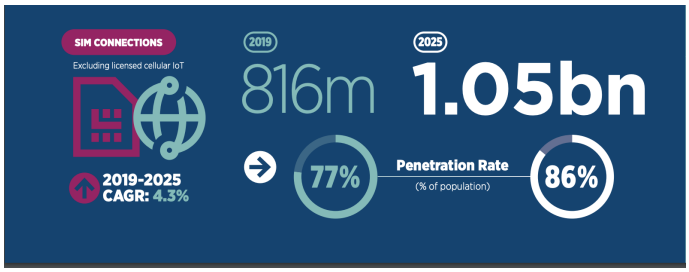

Figure 1. sub-Saharan sim connections (GSMA Intelligence Intelligence (2020))

Figure 1 shows the sim connections in sub-Saharan Africa as a whole, which are at 816 million in 2019, and are projected to be just over 1 billion in 5 years.

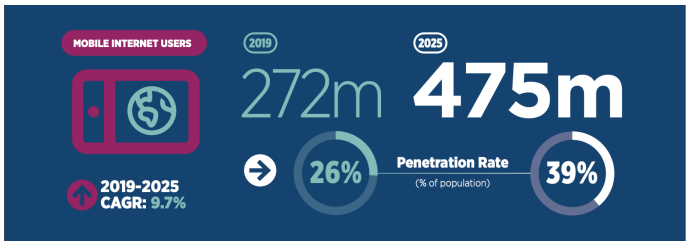

Figure 2. sub-Saharan Mobile Network Users (GSMA IntelligenceIntelligence (2020))

Figure 2 shows that in 2019 approximately 26% of the population of sub-Saharan Africa is using mobile data.

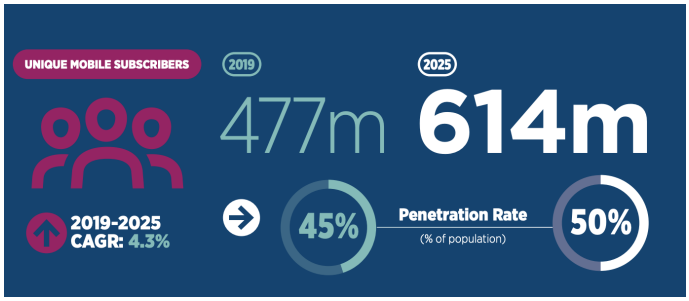

Figure 3. sub-Saharan Mobile Subscribers (GSMA Intelligence Intelligence (2020)

Figure 3 shows that the mobile subscription rate is 45% of the sub-Saharan Africa's population.

With 24 being the median age of the continent, and the projections of sim connections to grow by 9%, mobile data users to grow by 13% and mobile subscribers to grow by 5% in sub-Saharan Africa, it shows us that the youth will be digital denizens. Creating a digital identity that will protect this population as it continues to grow, is our aim. As this population is somewhat new to digital life, they lack an established

mental paradigm for the concept of digital identity; this fact will possibly make adoption of self-sovereign identity paradigm, and all it entails, easier.

2.3 Contributing to Digital Infrastructure

One of the best ways to contribute to global digital infrastructure is to rebuild it from the world wide web technology level. However, such is a monumental undertaking not the subject of the work at hand. There are several other ways to contribute to global digital infrastructure, and one of the most important, that uses existing infrastructure and technology is by way of open-source cryptographic consensus based distributed ledger protocols (blockchains) and applications (DApps).

Going the way of blockchain and DApps we must evaluate the existing technologies in the area of interest. As digital identity is of interest, the different types of digital identity must be at least reviewed, so that we may put forth something we believe is an improvement on that which exists. Digital identity can be divided into three different categories: private provider (platform) controlled, nation controlled, and self-sovereign.

The private provider category has been in place since the establishment of the Internet. This category contains several types of private identity providers, some of which are: dial-up provider identity, AOL identity, free Internet email (e.g. Hotmail, Yahoo, Google), and membership based sites (e.g. MySpace, Amazon, Facebook). Social media sites are including in other membership based sites due to data usage protocols and purpose of identity management Baars (2016).

The second category under consideration includes digital identification initiatives by nation-states, some of the more significant ones are eCitizen (Kenya) Ondego and Moturi (2016), Aadhar (India) Sen (2019), WeChat Plantin and de Seta (2019), and Estonia Identity Suite (eID, Mobile, Smart, Residency) eid (2019); mob (2019); sma (2019); ere (2019). WeChat could be placed in the first category as it is a membership based identity for a social network; however, due to China's "markedly techno-nationalist media regulations and and increasingly overt cyber-sovereignty agenda" it has gone from private provider to a nationally controlled infrastructure service.

The final category is self-sovereign identity, which is currently only possible by way of blockchain technology van Wingerde (2017). Because companies and governments require ownership of data they control, and hold on their servers, there is no way self-sovereign identity is possible through those entities. In fact, with blockchain everyone can hold a copy of the ledger everyone is a co-owner of the system. There is no sovereignty without supreme control of your data within a limited sphere, and that is impossible, by definition, if everything is controlled outside of the individual. Some of the people who need to be served by such a system do not have the resources necessary to maintain a full copy of such a ledger. Thankfully, due to the design of blockchain systems Gatteschi et al. (2018); Hassan et al. (2020); Zheng et al. (2017), at anytime one does obtain such resources one will be able to obtain the full ledger themselves and become a network node. The design of blockchain is meant for inclusiveness and hence is the only technology today that can realistically promise self-sovereign collective infrastructure for individuals in the digital world.

2.4 Pan-Africa SSI Qualifiers

Table 1 contains references as the entry to some of the table elements, in such a case the reference denotes the possibility of that type of identity service having the attribute in question. Establishing a self-sovereign identity system with blockchain will need to have positive attenuation for every attribute listed in Table 1 along with those outlined by Wingerde's master's thesis table 26 "Blockchain-enabled Self-sovereign Identity" van Wingerde (2017). Wingerde outlines a set of constraints in line with the General Data Protection Regulation (GDPR), the Revised Payment Serivces Directive (PSD2), and the electronic Identification, Authentication and Trust Services regulation (eIDAS) van Wingerde (2017).

Table 1. IDENTITY SERVICE COMPARISON

Attribute	Private	Government	Self-Sovereign
Demographics	✓	✓	✓
Biometrics	SOME	✓	SOME
User Owns Data	X	X	✓
Share Data Profits	X	X	SOME
Transparent Data Access	X	X	✓
State System Integration	SOME	✓	SOME
Transparent User Audit	X	X	✓
National Infrastructure	✓	✓	✓
Blockchain Back-end	X	✓	✓
Data Volunteering	X	X	SOME

Concerning being government infrastructure, like WeChat Plantin and de Seta (2019), the system should become so ubiquitous until it is necessary that government uses it as infrastructure.

2.5 Organization

The three stages the framework will now be outlined by exposition of its registration processes, interoperability and security, as well as its biometrics based longitudinal study.

3 STAGE 1: REGISTRATION

The first stage is the same for any identity system, and that is what and how information is stored in the system. What are the privacy tenets? How does one restore a lost or forgotten account? Can an individual register multiple accounts? If so, how are multiple accounts handled?

3.1 Demographics

The basic defining attributes of an individual form the bedrock of foundational identity. Enabling the core attributes to be mapped to an identifier by which an individual is known. Given demographic data is the first basis to individual identification, this information is very important in designing supporting systems for essential services (e.g. financial inclusion/access, healthcare access and education). Who you are varies depending on who asks. Your name may be Muthoni but to your children you are a parent, a resource to your employer, a student to your university, a taxpayer and citizen to your government. Different contexts define who we are over our lifetime and how we identify ourselves. One may end up holding different forms of documentation to prove who they are to access and benefit from available services. Hence functional identity is formed across myriad different contexts.

Some details vary on the different identifying documents but some key details are constant. Common details include ones name, gender, and image on an identifying document. One may hold a national ID card, a driver's license, a student's ID card, an employee card, a club membership card and a health insurance card. Yet in reality, it is still the same person regardless of interactions with differing authoritative bodies. In usage of any of the credentials, one only needs to show it, have its credibility checked before being granted access to a facility or services tied to the credential.

While many mundane tasks like money transfer have been successfully digitized, it has remained a hard task for the same to happen for exchange of identity credentials either due to poorly implemented standards or technology silos that hinder interoperability. Internet standards like the Verifiable Credentials

spec and Decentralized Identifiers (DIDs) by W3C have evolved over time to support a standard version of credentials and credentials exchange when issuing and verifying claims held by an individual w3c (2019). The digital identity revolution has been growing as seen in white papers published by the World Economic Forum highlighting the same Nash (2020); wef (2020).

3.2 Handling Biometric Data

Biometrics is the art and science of measuring life, and in computing practice it uses sensors to record a physiological or behavioral marker to process and use for identifying and/or verifying individuals. Cancelable biometrics Ratha et al. (2001) is a sub-field created by Nalini Ratha, inspired by early one-time passwords (OTP) systems. Cancelable biometrics allows for a digital representation of ones biometric information to be transferred electronically without compromise. Changing ones physical biometrics permanently quite the difficult task; hence, we want a system that safeguards this information most stringently. Following that thought unless special permission is given by the individual, the system will not require biometric templates to be sent directly for any operation. The system will utilize cancelable biometrics that build a key representation from biometric information, similarly to a one-way hash Merkle (1989). When a values/parameters that contribute to a cancelable functions output are compromised, biometric data is not. The aforementioned parameters to the function can be re-generated and updated, with more attention to security.

3.3 Serving Under-served Groups

One of the more meaningful reasons to build a blockchain SSI, starting with Kenyans as the inaugural population for the system is due to the numerous challenges that present themselves with myriad groups in the country. Kenya's arid north is full of groups who are pastorialists, e.g. they have no fixed address. There exists a tribe, the Maasai, who are also pastorialists found throughout the country. Kenya is also home to many groups that live their entire lives on farm land far away from major cities and tech infrastructure. This system takes the needs and lifestyles of all of these different groups into account. Because the system takes such disparate groups into account, it makes for a robust design, not easily envisaged by those without such a country and populace as a backdrop.

4 PHASE 2: INTEROPERABILITY AND SECURITY HARDENING

Today's world is changing rapidly, especially as we enter the fourth industrial revolution, the systems we build must be adaptable. History has shown us that the species that are most adaptable tend to have a higher survival rate than those that must cling to that with which it has always been familiar.

5 INTEROPERABILITY

As the internet and digital identity have progressed, so has interoperability of differing types. New digital identity frameworks are being designed with an aspiration to achieve the efficiency of X-Road from Estonia. The X-Road government infrastructure supports a "once-only" approach to data access whereby no single piece of personal information should be entered twice Saputro et al. (2020). Such an approach is possible due to individual servers being interlinked via end to end encrypted channels creating an X like backbone that supports interoperability with relying systems. Secure access to the data is provided given that a relying service cannot access personal data without approval by the owner of the information.

While backbone identity infrastructures exist in leading African economies, with the Integrated Population Registration Service (IPRS) in Kenya Rading (2019) and the NIMC Verification Service in Nigeria KALU et al. (2018), they should have provision for the use of personal biometrics beyond enrollment of citizens into the systems. An additional layer that allows direct control by use of biometrics, to access of personal

data would preserve information integrity and an API first approach of state registries would be key in supporting interoperability of systems.

Interoperability has been achieved at different levels by some social networks and email providers of most note is WeChat Plantin and de Seta (2019). WeChat is Chinese digital infrastructure and platform for most things that can be accessed online in the country Plantin and de Seta (2019). Interoperability has already been solved by a few different approaches of which X-Road Saputro et al. (2020), and OAuth 2.0 Jones et al. (2015); Hardt et al. (2012) are of most interest. Estonia's X-Road is of interest because it is the trusted Internet infrastructure for government entities Saputro et al. (2020). Estonia's different identity systems and services run on it eid (2019); ere (2019); mob (2019). OAuth 2.0 is of interest because it is the protocol over which javascript web tokens (JWT) operate Jones et al. (2015). The system will utilize OAuth 2.0 and JWT upon authentication to manage access to digital resources.

5.1 Security Hardening

In today's software practice, security patches have become quite the normal occurrence. Security patches apply to operating systems, developed by major companies and organizations, as well as mobile and computer applications. Common software engineering practice lends itself to security from compromise; however, in a world of humans were data is becoming more monetized and precious by the moment, we must design a system such that it keeps data safe from:

- social engineering
- biometric template theft
- general abuse and misuse

Some security hardening topics are not enumerated here as the cryptograhpic consensus based distributed ledger manages to mitigate through its design, such as bad actors on the network (computers attempting to hijack the network), data intercepting (private data will be locked with encryption keys), and identity masquerading (transactions are signed). By using the blockchain we introduce an owner-less distributed ledger that contains all historical system transactions. The distributed nature of the blockchain is such that it allows *every* user of the system to view every transaction at any time. By using a blockchain transactions, once they are submitted to the system can not be modified in any way, including deletion. All of these blockchain attributes do a great job of keeping transactions and data secure.

Biometrics and system notifications will be used to help stymie social engineering approaches. Blockchain systems use private keys to manage data; however, an issue with such is that once a private key is lost the certifications, claims and assets related to that private key are forfeit. The Pan-African system will use biometrics to aide in generation of the private key, so that it can't be lost. Generation of cryptographic keys usually requires a random seed of some sort, and research exists that outlines how to use information from biometric templates to be that random seed. Such systems are referred to as Biometric CryptoSystems Jin et al. (2016).

Template theft was addressed earlier along with the concept of cancelable biometrics Ratha et al. (2001, 2006).

Part of security hardening is ensuring personal data can not be shared without consent of the owner. To this end we have to add smart contracts for the system that allow all personal data be double signed by the owner. Hence, when trying to move the data a smart contract gives notice to the owner of someones attempt to share their data. The smart contract will have to insist on approval by the data owner. If approval isn't received after a certain time period and/or the data owner denies the operation, the network must cancel it

while logging the transaction attempt. The system must automatically encrypt all personal data in personal claim repositories (user wallets). Identity claims must be issued following a specific machine-readable format. The 1st signature is the data owners, the second is for transmission of data and consists of the public key of the recipient.

6 PHASE 3: LONGITUDINAL DATA STUDY

In biometric research longitudinal studies are usually completed to prove assertions and learn more about a specific modality, as in evaluating the validity of a modality's persistence Yoon and Jain (2015). A longitudinal study is one in which the same group of participants are observed over an extended period of time, e.g. 15 years. Such information, gleaned over time, has proven necessary for researchers and end-users when making claims that can have legal ramifications.

In 2014, Yoon and Jain were able to perform such a study by using an "operational fingerprint database" Yoon and Jain (2015). This year, Mundnich et. al. did a psychological and behavioral study utilizing data "from direct clinical providers in a hospital workplace" Mundnich et al. (2020). One the aims of our system is to obtain biometric and behavioral data without negative semblance. In speaking to negative semblances, we mean utilizing "records of repeat offenders apprehended by the MSP" (US Citizen slave prisoners who have lost their human rights) Yoon and Jain (2015), and data sets of people who had to give away rights to certain data as an employment condition Mundnich et al. (2020).

A reason a study is to be made with this system is because of the current state of bias in biometric recognition systems Buolamwini and Gebru (2018). Machine learning models and scientists are majority Caucasian/Asian and the major biometric face databases are of the same demographic. Buolamwini carried out studies and evaluations of face recognition corpi and systems of the largest providers of the technology in the United States. Buolamwini found 'dark-skinned' women to be woefully underrepresented and dramatically mis-classified, in comparison to lighter males Buolamwini and Gebru (2018).

Another reason a study is to be made with this system is to improve the system based on user feedback that will be completely optional. Biometric data is not the only information to be captured by the study, but also various user sentiment, along with platform usefulness, and usability. At each stage of the systems use, users will be able to provide feedback, at a granularity of their choice, which we will use to improve interactions, usability, partnerships and more.

6.1 Participation Protocol

Participation in this study will follow strict guidelines to ensure participant privacy and secure their volunteered biometric data as much as possible. Our participation protocol has three components: fully informed self sovereign volunteering (SSV), data obfuscation and usage, and self sovereign control.

Fully informed self sovereign volunteering (SSV) is the most ethical and responsible way to acquire information from people. SSV requires all data usage is logged to a blockchain network and volunteers are notified as to how their data is being used. If their data is monetized, they will receive monetary reimbursement, using a model similar to that of Steem.com. Steem is a blockchain for the support of "community building and social interaction with cryptocurrency rewards" STEEM (2018). Concerning rewards for the monetization of the data of volunteers, a Steem-like system must be deployed on our network.

6.2 Data Handling

One-way hashing will be used to clean data of personally identifying information, such as names being attached to biometric signatures.

The world is consistently moving forward with biometric research with every publication and new cell phone Gelb and Clark (2013). The data to be used along with registration in this system is multitudinous, and by necessity will grow. As this is a platform intended to provide identity, in a complete sense, in a digital format only controllable by the owner of the identity, an egregious amount of information can be gleaned from its proper study.

7 MOVING FORWARD

The requisite research and planning have been done for the implementation of the system to begin. Unstructured demographic data will be accepted into the system, along with cancelable biometric templates. Hyperledger Indy will be the first blockchain backbone component of the minimum viable product. As noted in research by Wingerde van Wingerde (2017) and Ferdous Ferdous et al. (2019) The Sovrin platform, which uses Hyperledger Indy, is a popular blockchain identity system closer to being truly self-sovereign than others. Though Sovrin is the best system at the moment, it lacks some few features, those specifically outlined in van Wingerde (2017). In order to reach the desired system the blockchain on which Sovrin exists will require addition of several smart contracts. More research is required to figure out the best way to fill in the gaps. Determination and full design of the longitudinal study must also be completed in order to have the study begin upon deployment of the system being built.

The implementation and adoption of the system will lead us to a real conclusion of the efficacy of the ideas put forth.

CONFLICT OF INTEREST STATEMENT

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

AUTHOR CONTRIBUTIONS

S. Solomon Darnell is the main author. Eddie J. Kago aided with ideation and demographics conversation. Joseph Sevilla was the main proof-reader.

REFERENCES

[Dataset] (2019). E-residency - e-estonia

[Dataset] (2019). Id-card - e-estonia

[Dataset] (2019). Mobile-id - e-estonia

[Dataset] (2019). A primer for decentralized identifiers

[Dataset] (2019). Smart-id - e-estonia

[Dataset] (2020). Africa population (live)

[Dataset] (2020). Reimagining digital identity: A strategic imperative

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

[Dataset] Bank-ID4D, W. (2017). Principles on identification for sustainable development : Toward the digital age

Buolamwini, J. and Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of Machine Learning Research*. vol. 81, 1–15

Cobbing, J. and Hiller, B. (2019). Waking a sleeping giant: Realizing the potential of groundwater in sub-saharan africa. *World Development* 122, 597–613

Du Bois, W. E. B. (1974). The pan-african movement (Pan African Congress)

Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* 7, 103059–103079

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., and Santamaria, V. (2018). To blockchain or not to blockchain: That is the question. *IT Professional* 20, 62–74

Gelb, A. and Clark, J. (2013). Identification for development: the biometrics revolution. *Center for Global Development Working Paper*

Hardt, D. et al. (2012). *The OAuth 2.0 authorization framework*. Tech. rep., RFC 6749, October

Hassan, M. U., Rehmani, M. H., and Chen, J. (2020). Differential privacy in blockchain technology: A futuristic approach. *Journal of Parallel and Distributed Computing* 145, 50–74

[Dataset] Intelligence, G. (2020). The mobile economy sub-saharan africa 2020

Jin, Z., Teoh, A. B. J., Goi, B.-M., and Tay, Y.-H. (2016). Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition* 56, 50–62

Jones, M., Campbell, B., and Mortimore, C. (2015). Json web token (jwt) profile for oauth 2.0 client authentication and authorization grants. *May-2015.[Online]. Available: https://tools. ietf. org/html/rfc7523*

KALU, M. I., DAVID, N., and NNAJI, F. (2018). The philosophy and politics of national identity management in nigeria: A case for nation-building. *African Journal of Politics and Administrative Studies* 11, 1

Kenya, D. (2008). *Deploying World Class Infrastructure Facilities & Services* (Kenya Vision 2030)

Merkle, R. C. (1989). One way hash functions and des. In *Conference on the Theory and Application of Cryptology* (Springer), 428–446

Morris, M., Binswanger-Mkhize, H. P., and Byerlee, D. (2009). *Awakening Africa's sleeping giant: prospects for commercial agriculture in the Guinea Savannah Zone and beyond* (The World Bank)

[Dataset] Mundnich, K., Booth, B. M., L'Hommedieu, M., Feng, T., Girault, B., L'Hommedieu, J., et al. (2020). Tiles-2018: A longitudinal physiologic and behavioral data set of hospital workers

[Dataset] Nash, J. (2020). World economic forum spells out its decentralized biometric travel id project

Ondego, B. and Moturi, C. (2016). Evaluation of the implementation of the e-citizen in kenya. *International Journal of Applied Information Systems (IJAIS)* 10

Plantin, J.-C. and de Seta, G. (2019). Wechat as infrastructure: The techno-nationalist shaping of chinese digital platforms. *Chinese Journal of Communication* 12, 257–273

Rading, M. O. (2019). *Interoperability Framework for National Population Register A Case Study of IPRS*. Ph.D. thesis, University of Nairobi

Ratha, N., Connell, J., Bolle, R. M., and Chikkerur, S. (2006). Cancelable biometrics: A case study in fingerprints. In *18th International Conference on Pattern Recognition (ICPR'06)* (IEEE), vol. 4, 370–373

Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal* 40, 614–634

Saputro, R., Pappel, I., Vainsalu, H., Lips, S., and Draheim, D. (2020). Prerequisites for the adoption of the x - road interoperability and data exchange framework: A comparative study. In *2020 Seventh International Conference on eDemocracy eGovernment (ICEDEG)*. 216–222. doi:10.1109/ICEDEG48599.2020.9096704

Sen, S. (2019). A decade of aadhaar: Lessons in implementing a foundational id system. *ORF Issue Brief* 292

[Dataset] STEEM (2018). Steem: An incentivized, blockchain-based, public content platform

[Dataset] Tanui, C. (2018). Kenya's mobile phone penetration surpasses 100% mark

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

Yoon, S. and Jain, A. K. (2015). Longitudinal study of fingerprint recognition. *Proceedings of the National Academy of Sciences* 112, 8555–8560. doi:10.1073/pnas.1410272112

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (IEEE), 557–564