The Use of Blockchain Technology in Identity Storage and Management

Gideon Simon Ghajiga
Dikeledi Jacobeth Warlimont
Mzansi Youth Leadership Academy, Johannesburg, South Africa
gghajiga@gmail.com
djwarlimont@gmail.com

Abstract

Evolvement of Blockchain following the introduction of the internet has thrown up many issues and its application across the broad spectrum of human activities, among which is full-proof identity management system. The current centralized data system of national identity services is replete with a whole gamut of operational risks for parties involved due to the issue of trust and lack of safeguards to protect the system from being compromised or hacked. Decentralized identity management system is a solution to the challenges, adopting a user-focused approach that gives full control of an identity back to the individual; and using Nigerian's National Identity Management System as a case study, a blockchain technology-based identity management system is proposed. Prototypes for identity construction, alteration, certification and reporting are presented. Cyber-attackdeterrence and developing of smart contract protocol model for identity management, as well as attribute disclosure are other contributions to the use of blockchain.

Key words: Blockchain, Identity Management, Decentralized Identity Management system, Nigeria's National Identity Management System
J.E.L. classification: C8, O33

1. Introduction

With the emergence of the internet and increasing cases of identity fraud, email breaches, the security of information and data online has become a recurring decimal in the quest for optimization, deployment and use of technology for storage, management and retrieval of information. (Bambara et al, 2018). This has call to question the present technological architecture and infrastructure in the deployment and use of technology in the documentation, collation and storage of personal data, as well as management of peoples' identity; both at national and international level. It is therefore imperative that these pressing issues will require a paradigm shift towards the use of Blockchain a dispersed record innovation in the execution of national identity for all citizens, with far reaching positive implications.

Every day that we are being inundated with news of data breaches which culminated in millions of emails, credit card information of websites of banks, International hotels, government institutions being breached, causing them to lose billions of dollars to various fraud. A case in question is the hacking of 500million emails of Yahoo members, 5.2 million Bonvoy loyalty program of Marriot Hotel International, and many more of such incidences. Trending technological tools are not only outdated, insecure, but are bereft of appropriate privacy protections, while personal data of people are monetized and commoditized; at the expense of owners. **(www.wired.com/story)**. This was also collaborated by a real-life scenario where clients' information in a big law firm were breached; and it was decided that blockchain technology could offer a more plausible alternative to securing customers data, particularly contracts and highly sensitive information(Bambara et al, 2018).

In the quest to bridge such a security gap and cover such lapses that technology expert, software engineers and developers are looking towards the direct of Blockchain technology for solution.

2. Literature review

Before the introduction of Blockchain technology, Government establishments, companies, businesses, banks, airlines, and hotels data base have been at the receiving end of hackers; and of course internet experts and web developers have been battling with the issues bordering on security breaches and compromise of their data bases and emails; aside from identity and credit card frauds, with malicious intent (Drescher, 2017, P.580). This was increasing in quantum leaps and assuming an alarming proportion and something needed to be done.

The state of affair was aptly captured Tapscott and Tapscott (2016) when they stated that inspite of ubiquitous presence on the world wide web and new technological security inventions, we can't dependably build up each other's characters or trust each other to execute and trade cash without approval from an outsider like a bank or a legislature. These equivalent mediators gather our information and attack our protection for business addition and national security. It was within this milieu, enters the blockchain technology.

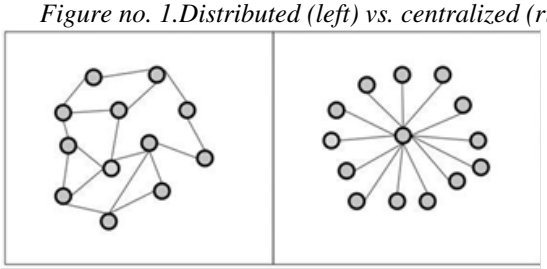
Based on this trajectory, it was therefore logical that the advent of the blockchain technology and its development was inevitably out of necessity on the part of software engineers, internet security experts; in their quest in mitigating the ubiquitous and pervasiveness of Internet's problems of privacy, security, and inclusion with cryptography. Under the prevailing circumstances before the emergence of blockchain technology, every ingenuity on the part of experts to think with process always leaves an opening for compromise. This was as a result of contribution of an outsider, performing an intermediation role to engender trust between parties. This was succinctly amplified by use of credit cards for payments over the Internet, which at best is not secure because users had to relinquish too much of their personal data, and the accompanying transaction fees were prohibitively high for small payments.

Recently, MasterCard International has been reported to have joined the blockchain digital identity alliance ID2020. The ID2020 Alliance was founded by a consortium made of Accenture, Microsoft, Gavi, Rockefeller Foundation and IDEO. Partners include Non-Governmental Organizations, private companies and United Nations agencies (Ledger Insight 2020).

2.1 The Blockchain Phenomenon

Blockchain technology, like the internet before it which is billed to tsunamically alter transactional relationships is strategically positioned to become the next prime disruptor, tipping the technological scale for good or for bad; or both. They are an emerging digital technology that synthesizes cryptography, data processing and management, networking, and stimulus mechanisms to bolster the verification, implementation, and documentation of transactions between parties. According to (Xewei et al 2018), blockchain ledger is a list ('chain') of groups ('blocks') of transactions. Parties proposing a transaction may add it to a pool of transactions intended to be recorded on the ledger. Processing nodes within the blockchain system take some of those transactions, check their integrity, and record them in new blocks on the ledger. The substance of the blockchain records are replicated across many geographically-distributed processing nodes

Figure no. 1.Distributed (left) vs. centralized (right) systemarchitecture



Source: Blockchain Basic: A Non-Technical Introduction in 25 Steps, Daniel Drescher (2017)

Therefore, the use of blockchain will usher a gargantuan shift which will displace the historically intermediation roles of intermediaries upon whom national institutions, have; over the years comes to relied on to implement administrative and security safeguards against document fabrication, unlawful relocation, tax evasion, money laundering and the 'underground' market activities in the hard-drug trade, human and sex trafficking, as well as cybercrime.

There was asserted in (Xewei et al, 2018), that generally speaking, these exchanges are bolstered by confiding in outsiders, particularly government organizations, banks, lawful firms, bookkeeping firms, and specialist co-ops in explicit enterprises. Blockchain technology therefore gives acredible alternate method to build confidences in such exchanges.

More so, when a quantum leaps in online communication in a 'wired' world is throwing up more opportunities for these types of crime; namely : spammers, identity thieves, phishers, spies, zombie farmers, hackers, cyberbullies, and data nappers –criminals who activate ransomware to hold data captive.(Tapscott and Tapscott 2016). As pointed out by Andre Boysen (2019) on Cyber security, it is practically difficult to peruse the news without going over a lead story indexing the most recent digital break or abuse of information. Licensed innovation is being taken from organizations at a disturbing rate. Remote hackers are intruding and muddling decisions. Crooks utilize the dull openings of the web to sell medications, weapons and even individuals.

The American Bar Association Cyberspace Law Committee in Fort Lauderdale, Florida, USA Report of January 29-30, 2016 defined blockchain as akin to a computerized, circulated exchange record database with indistinguishable duplicates kept up on a system of numerous PC frameworks constrained by various substances. It records and stores each exchange that happens in the system.

2.2 Imperative of Blockchain

We are daily inundated with reports and news of stolen identity, hacking of passwords and theft of personal data of internet users which has rendered current security safeguards unsecured.This was collaborated by Bambara *et al.,* 2018) when they said in the present world wide web, we are inundated with security issues that are recognizable to everybody. More often than not we depend on our usernames and secret codes to get to access our benefits.

These security features are susceptible to breaches inspite of the attendant safeguards put in place; there have been tremendous increase in data theft, internet fraud, identity theft, hacking and so many other vices. As a result of these mitigating issues, blockchain technology offers a more verifiable and decentralized system without an intermediary and which is a shade head in terms of trust issue called the 'trust protocol' which hitherto requires and necessitates a third party to verify the authenticity of a transaction or documents.Bambara et.al., (2018)work supports this fact. Blockchain utilizes encryption innovation to enhance security. By permitting information and data to be generally conveyed, blockchain innovation has laid the foundation of the new world wide web version 3. In spite of the fact that it was initially conceived for the cryptocurrency, the business and innovation networks are finding numerous utilizations for it. Information on this new innovation will be required by developers as well as by all organizations. It is envisioned that in the next five to ten years, blockchain will alter the plans of action in a wide range of businesses—and probably change our daily existence.

In a White Paper authored *by* Skip Slone & the Open Group Identity Management Work Area March 2004, sees trust as akin to a firm confidence in authenticity, integrity, truthfulness, fairness, in the intent of another party to conduct a deal, transaction, pledge, contract, etc. in accordance with agreed principles, rules, laws, expectations and undertakings.

In so many ways, blockchain technology which combines myriads of mathematical formulae, algorithm, computer codes and cryptography, offers in terms of integrity; a better but verifiable, secure, reliable and hack-free architecture that can host data and information which can be accessed seamlessly.This fact was amplified by (Daniel Drescher 2017). The choice of blockchain is to accomplish and keep up trustworthiness in appropriated frameworks. The enthusiasm aboutthe technology hinges on its capacity to stand as an instrument for accomplishing and keeping unaltered records in shared frameworks that can possibly change entire businesses bypassing middlemen. This is particularly true of blockchain's transparent and open approach in keeping tab on transactions; revolutionizing the way information and data are seamlessly stored and can be retrieved and managed. The Blockchain Technology has opened a whole new vista and possibilities

for sovereign nations, particularly Nigeria who desire a uniform system of identification that will aid government agencies, especially the police in the discharge of the statutory responsibilities(NIMC 2010).It offers Nigeria a unique opportunity to institute and establish a robust, and an all-encompassing but enduring identity management systems that can hosts citizen's identities whichcan incorporate and host their personal data such as birth authentication, marriage endorsement, common enlistment and driver's license (ITU-T FGDFS, 2016).

The salient features of the blockchain technology which makes it natural choice for deploymentin the management of Nigeria's National Identity card is, being a decentralized system, anybody can review the entries in it, due largely the fact that blockchain is based on consensus of the majority of parties involved. It is also an establish fact that information or data imputed into the blockchain cannot be effaced, because it contains a precise, verifiable documentation of every single record of contract entered into.

A very important feature of blockchain technology is the fact that any transaction or record imputed cannot be altered without being detected. Blockchain offers transparency system which is open to all parties which ultimately enhance trust.

2.3 Nigeria's Current National Identification Card Management

The Nigerian National Identity Card Scheme under the tutelage of National Identity management Commission(NIMC) as it presently constituted is bedeviled with so many issues compounded by serial allegation of corruption and fraud in the implementation actualization of Government objectives of having an accurate data on its citizens for planning, health care, election voting and a host of other benefits.

Preceding the setting up of the National Identity Card scheme, there has been a dearth of adequate report on consumer credit market, coupled with the fact that there was non-existence of consistent but uniform form of identification system which will form the bedrock in helping the Law Enforcement Agencies in Nigeria in the discharge of their statutory functions (NIMC, p.4, 2010)

The Nigerian Identity Management System is presently functioning as centralized server system as oppose to the decentralized which the blockchain technology offers.

The current National Identity Card Scheme, which is being statutorily managed by the National Identity Management Commission (NIMC); is to perform the following functions:

a. Registration and biometric enrollment of residents and legitimate inhabitants, with the objective of generating and storing National Identity database on a sustainable basis;
b. Toissue to every citizen a unique number code which is called the National Identification Number (NIN).
c. Issuance of what is called the General Multi-purpose Cards (GMPCs) (as provided for in the NIMC Act);
d. Provide for identity verification and authentication services;
e. Provide for access and connectivity infrastructure between registration centers, central data processing center, identity verification system and backend systems;
f. Provide for standardization and consolidation of identity databases in government organizations, which of course including providing the regulatory and institutional framework for an orderly development of the Nigerian National Identity Scheme.

The exiting system currently in operation provides for citizen identitycertification and affirmation through the appropriation of safe entry to a National Identity Card Database (NIDB). It is required by law for the National Identity Management Commission (NIMC) to from time to time enhance the identity card to chip-embedded cards. The current system has been fraught with many pitfalls, among which are: inherent danger and threat of the database, being compromised through hacking, identity theft; and at best the central server crashing and loss of the entire information; and the capabilities for manipulation and stealing of information. No to mention also attack from malware and ransomware is also eminent in this regard. (NIMC, 2010)

A good example of the deployment of blockchain technology is in the tiny nation of Estonia, a one of the Baltic nations with a population size of 1.3million people, has demonstrated the political will in pioneering the adoption and use of blockchain technology in service delivery to its citizens. This was succinctly captured by Tapacott and Tapscott (2017).

Estonia's pioneering political leaders have structured their e-government course of action, anchored on disperses administration, interconnectedness, responsiveness, and network security. Their objective is to establish and sustain a system where new innovation and technological advancement can be seamlessly integrated and citizens can access government services and information online, using their unique identity code. It will also enable citizens to also update their personal information with government as at when desirable.

For a meaningful economic planning, robust, adequate and timely intelligence gathering, which is a sin quo to functional security architecture, Nigeria needs a technologically driven national identity system, and not the present system where there is no coordinator system to harmonize the various approach between the government and the private sector. While the banks and financial institutions are enrolling their customers in their database, government is issuing the chip-based identification code to each citizen after enrollment. Data required from each citizen for enlistment are date of birth, gender, education qualification, ethnicity and a host of related information. Fingerprinting, and facial picture of the enrollee from head shoulder length is also incorporated, aside from digitizing individual signatures into the data base. Such information provides the basis for comparison and authentication of previous enrollment, if any.

These data are ultimately stored in the database of National Identity Management Center Numb*e*r **(**Omoniyi, 2012**).** The purpose for the unique number is differentiating individuals bearing similar names. Extra data like resident personal residence, local council, telephone number, date of birth, information of parents, DNA data, criminal record, driving record, marital status, as well as job placement history is also inclusive. Ultimately, this distinctive identification holds the complete life cycle of the owner**. (**Omoniyi, 2012).

Estonia, a small Baltic nation with a population of 1.3million people has demonstrated the political will in pioneering the adoption and use of blockchain technology in service delivery to its citizens. This was succinctly captured by Tapacott and Tapscott (2017) when the said **"**Estonia's leaders have designed their e-government strategy around decentralization, interconnectivity, openness, and cybersecurity. Their goal has been to future-proof infrastructure to accommodate the new. All residents can access information and services online, use their digital identity to conduct business, and update or correct their government records.

While these lofty objectives in achieving a universal coverage for all citizens to have a permanent identification, technological innovations present a whole new opportunity for a comprehensive, trustworthy, hack-proof national identification system; built on an open and transparent architecture; unlike the centralized system.

According to (Ji et.al. 2009) the concentrated database structure constitutes a great impediment to an innovative identity management system; subject to the whims and caprice of professional hackers, intermittent downtime; with its attendant legalism of license fees and frequent upgrade of new versions. Occasional compatibility of hardware to be for integration with existing ones is also another drawback.

Hence, the imperative of the use of blockchain, which is the act as a distributed ledgerwill bring a whole new perspective to the way data and information are stored and transactions executed. This comes with the unique and novel advantage of speed, lower cost, full-proof security, fewer errors, and the elimination of central points of cyberattack; and of course, system failure. (Tapscott and Tapscott 2016) affirmed this unique feature of the blockchain when they said eachblock (database) similar to the one that utilizes bitcoin, is dispersedlyconnected across many PCs offered voluntarily by parties. This removes the chances of being breached by anybody. It is available and anybody can have access to it since it is not quarantined in stationery hardware that can be tempered with.

In (Tapscott and Tapscott 2016) this new advanced record of monetary exchanges can be customized to record for all intents and purposes everything of significant worth and significance to mankind: birth and passing endorsements, marital documents of note, deeds and titles of possession, educational certificates, money related records, clinical history, protection claims, votes, and whatever else that can be transmitted in code.

The Blockchain therefore offers an unimaginable vista in the technological world of not only financial services but also in the Identity Management (IdM). Melane Swan (2015) supports the fact that the prospective edge that the blockchain are something other than monetary. Its applicability transcendent all human endeavors, across the wide spectrum of human existence.

3. Research methodology

In this undertaking, this research for the adaptation and use of Blockchain in national identity management, conscious and deliberate efforts will be geared towards exploring the unique security and trust-proof features of the blockchain technology which will, ultimately be deployed in the administration of the country's National Identity Scheme within the context of the existing technologies. This will involve the review of existing literature on blockchain technology and its application in identity management, in terms of architectural infrastructural system which will meet the requirements of the project for adoption and implementation.

4. Conclusions

The advent of Blockchain has ushered in a new phase and has challenged exiting technology in data security and digital identity. Given several reasons, Michael (2017) justified people's prediction that blockchain will transcend bitcoin and will fundamentally and irreversibly trigger a shift in our universe, technologically. Its applicability is envisaged to cover wide and diverse areas. Aside from finance, it will cover digitization of property rights, computerized ballot system, legal agreements, logistic networks, e-government in all ramifications, decentralized autonomous organizations, our tax system and tax administration.

It is pertinent to mention here that already blockchain technology has being deployed and put in used in the following countries in the management of land in Sweden, Brazil, Dubai; and in addition, China has already led the pack by blazing the trail in the test of its country central-bank midwifed national cryptocurrency, and currently undergoing a trial run within the context of its country-wide financial infrastructures.

Blockchain Technology offers a very credible and pen system which eliminates trust issues by offering an infrastructure that decentralizes the ownership of credentials and offering a universally available protocol for verifying one's record in an immutable chain of data, that is once imputed, it cannot be changed. This data rather than being stored on as per application- basis, is stored in distributed database, which featured a de-centered, traceable, non-tampering, security-proof and reliable; thereby, integrating the Peer-to-peer (p2p) protocol, fortified by digital encryption technology. It can also be called a shared ledger. This shared ledger is downloaded by each individual user of the blockchain and is a record of each exchange made at any point in time.

However, this topic may require further study because of some challenges of blockchain, which is principally a collection of nodes which are linked by peer-to-peer networks, with exclusively its own layer of protocol messaging communication signals. These challenges among others include performance appraisal, scalability, and privacy; which need to be taken into account when considering its deployment.

5. References

- Bambara, J., Allen, P.R., 2018. Blockchain*, A Practical Guide to Developing Business, Law, and Technology Solutions*: McGraw-Hill Education
- Brian, B., 2020. Hack Brief, 2020. *Marriott Got Hacked. Yes, Again,* [online]. Available at*:* https://www.wired.com/story/marriott-hacked-yes-again-2020/ [Accessed March, 2020].
- Daniel, D., 2017. *Blockchain Basics. A Non-Technical Introduction in 25 Steps*, Apress Publishers
- Don, T., Alex T., 2016. Blockchain Revolution, *How the Technology Behind Bitcoin is Changing Money, Business and the World,* Penguin Publishing Group
- ITU. 2016. *International Telecommunication Union (ITU) Workshop Publications,* [online]. Available at: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-CAT.OL-2016-PDF-E.pdf [Accessed May, 2020].
- Ji, L., Liang, H., Song, Y., & Niu, X., 2009. *A Normal-Traffic Network Covert Channel*. 499-503. 10.1109/CIS.2009.156.
- Melanie, S., 2015. *BluePrint for a New economy*, O'Reilly Media, Inc. Sebastopol.
- NIMC. 2010. National Identity Management Commission Report, *NIMC annual Report 2010*, [online]. Available at: https://www.nimc.gov.ng/docs/reports/annual_report_2010.pdf

- Nicky, M., 2018. Mayo Clinic exploring blockchain*, Enterprise blockchain news*, [online]. Available at: https://www.ledgerinsights.com/about-us/May
- Omoniyi, T. 2012. National Identity Number. *A rainbow of views. Monday*, 02 April. Daily Trust online
- Xiwei X., Ingo W., and Mark S., 2019. *Architecture for Blockchain Applications*, Springer Nature
- Yahoo,. 2016. Yahoo, *'state' hackers stole data from 500 million users,* [online]. Available at: **https://www.bbc.com/news/world-us-canada-37447016 /** [Accessed March, 2020]