Blockchain Technology as an Antidote to Nigerians' continuous involvement in certificates forgery

Conference Paper · June 2019

1 author:

Adegboye James
The Federal Polytechnic, Ilaro
14 PUBLICATIONS   **1** CITATION

Some of the authors of this publication are also working on these related projects:

Current Innovation View project

Measles Research View project

Proceedings of the 16th iSTEAMS Multidisciplinary Research Nexus Conference
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

Block Chain Technology as an Antidote to Nigerians' Continuous Involvement in Certificates Forgery

Buoye P. A.[1] & Adegboye O.J.[2]
Computer Science Department
The Federal Polytechnic
Ilaro, Ogun State, Nigeria
Email: [1] adewuyi.buoye@federalpolyilaro.edu.ng, [2] olujoba.adegboye@federalpolyilaro.edu.ng
Phone: +2348030640850, +2347038195169

ABSTRACT

It is shocking and disappointing that even when it is a public knowledge that forgery of certificates and official documents is a criminal offence that attracts severe punishment, many Nigerians have continued to engage in the illicit activities unabated. The number of persons involved in certificate scandals in Nigeria in recent times is on the high side and the caliber of people involved is disgraceful and embarrassing. So worrisome is the fact that in most cases, forged documents passed through government agencies, including security agents unidentified. The **blockchain** is an open, decentralized, distributed and public digital ledger where transactions are recorded between people across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the Consensus of the network. Based on the blockchain property of serving as a decentralized permanent unalterable store of all types of information or assets, certificate awarding institution can start awarding digital certificates.

Keywords: Blockchain Technology, Certificate Forgery, Consensus Algorithms, Digital Certificate Decentralized Distribution

1. INTRODUCTION

The number of persons involved in certificate scandals in Nigeria in recent times is on the high side and the caliber of people involved is disgraceful and embarrassing. Abati (2018) said, One US report indicates that Nigerians are among the most educated immigrants in the United States, vertically and horizontally. During Obasanjo's civilian administration, a member of national house of representative claimed to have graduated from Toronto University, so also is the Chicago scandal. What is worrisome for me is the caliber of people involved on daily bases. If, according to Abati (2018) Nigerians are considered as the best educated black persons in the world, it is now shameful that Nigerians today are also ironically poster-characters for fake certificates, 419 qualifications, and dubious academic affiliations. It is shocking and disappointing that even when it is a public knowledge that forgery of certificates and official/government documents is a criminal offence that attracts capital punishment, many Nigerians have continued to engage in the illicit activities unabated. Before the ex-minister of finance, Mrs Kemi Adeosun's NYSC certificate forgery scandal became an issue of public discourse, she has used the certificate to pass a screening test for her appointment as commissioner of finance in Ogun State (Abati, 2018). It is my believe that there are so many people in both private and public sector that are involved in certificate scam which have not been identified.

Proceedings of the 16th iSTEAMS Multidisciplinary
Research Nexus Conference
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

This is as a result of increasing rate of certificate/document forgery and the inability or failure of the relevant authorities, including security agents to identify it in time. So worrisome is the fact that in most cases, forged documents passed through government agencies, including security agents unidentified. This has once more raised question on the integrity and credibility of the country's security agencies in curbing the menace. It is possible for Nigerians to fake medical reports from non-existing hospitals. This is done either to travel abroad, get good job, absent from work or at times when an employee does not want to go to a particular location for his/her primary assignment. On several occasions, the former Director General of the NYSC, Johnson Olawuni had vowed to punish corps members falsifying medical reports to secure deployment to new stations as it was discovered that most reports presented were fake. Years after this fire and brimstone pronouncement, nothing seems to have happened as fake medical reports has grown to become big business for many health practitioners." (Ezea, Awodipe, Atueyi, Salau, Alade, Thomas-Odia and Jeremiah, 2018).

Falsification of documents at the Sea ports in Nigeria either by the Importers or Clearing Agents is giving the Nigerian Customs Service (NCS) much trouble every year. False declaration of goods is the act of giving false description about the nature, type, quantity of goods imported into the country (Ezea, et.al 2018). Falsification of documents at the port helps to smuggle banned items into the country, reduces the amount of duty payable on such goods, hence, reduce the revenue generation and put the nation on danger of arms and ammunition proliferation.

2. LITERATURE REVIEW

Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer (P2P) basis (Adam-Kalfon and El Moutaouakil, 2017). Blockchain is a distributed network performing certain actions programmed into it. Blockchain seems to be the driving technology behind the next generation Internet, also referred to the Decentralized Web, or the Web3. The blockchain is a novel solution to the age-old human problem of trust (Shemin and Valentin, 2017), It provides an architecture for so-called trustless trust. It allows us to trust the outputs of the system without trusting any actor within it. Blockchain is a shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls (Shemin and Valentin, 2017). It is a distributed database that maintains a continuously growing list of transaction data records, cryptographically secured from tampering and revision.

Blockchain owes its name to the way it stores transaction data —in blocks that are linked together to form a chain. As the number of transactions grows, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain within a discrete network governed by rules agreed on by the network participants (Gupta, 2018). A Blockchain protocol operates on top of the Internet, on a P2P Network of computers that all run the protocol and hold an identical copy of the ledger of transactions, enabling P2P value transactions without a middleman though machine consensus. Blockchain itself is a file, a shared and public ledger of transactions that records all transactions from the first block until today. The ledger is built using a linked list, or chain of blocks, where each block contains a certain number of transactions that were validated by the network in a given time span.

Mahalingam (2018) called each computer in the chain as a node and each node has a copy of the digital data or Blockchain. Each node checks the validity of each data transmitted. If a majority of nodes say that a transaction is valid then it is written into a block. Communication is always happening directly between peers, rather than through some central node. Information about what is happening on the Blockchain is stored on each node then passed to adjacent nodes. In this way information spreads through the whole network. A node here revers to a computer and a block is a growing list of records (Mahalingam, 2018).

Proceedings of the 16th iSTEAMS Multidisciplinary
Research Nexus Conference
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

If a block is revered to as the list of records, then a blockchain can be rightly said to be a database that is distributed among all nodes, (computers). Although Traditional online databases usually use a client-server network architecture, which allows users with access rights to change entries stored in the database, but the overall control remains with administrators. When it comes to a Blockchain database, each user is in charge of maintaining, calculating and updating every new entry. Every single node must work together to make sure that they are coming to the same conclusions. Gupta (2018) stated, to be clear while the blockchain contains transaction data, it's not a replacement for databases, messaging technology, transaction processing, or business processes. Instead, the blockchain contains verified proof of transactions. However, while blockchain essentially serves as a database for recording transactions, its benefits extend far beyond those of a traditional database. Most notably, it removes the possibility of tampering by a malicious actor (for example, a database administrator). Blockchain can be likening to an operating system, such as Microsoft Windows or Mac O.S. (Gupta, 2018). Mohamed, Makhlouf, Mithun, Abdelouahid, Leandros and Helge, (2018) classified blockchain as either a private (permission) or public (permission-less). Both classes are decentralized and provide a certain level of immunity against faulty or malicious users for the ledger. The main differences between private and public blockchains lie in the execution of the consensus protocol, the maintenance of the ledger, and the authorization to join to the P2P network.

2.1. Major Characteristics of Blockchain
According to Zibin, Shaoan, Hongning, Xiangping, and Huaimin, (2017), blockchain has following major characteristics:

1. Decentralization: Contrast to the centralized mode used in conventional centralized transaction systems, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.
2. Persistency: Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.
3. Anonymity: Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user.
4. Auditability. Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent transaction. So transactions could be easily verified and tracked.

2.2 Types of Blockchain
Zibin et.al (2017) and shermin and valentine, (2017) categorized blockchain into three which are:
Public Blockchain
Private Blockchain
Hybrid /consortium/ federated Blockchain

2.3. Features of Blockchain
Public Blockchain

1. Anyone can download the code and start running a public node on their local device, validating transactions in the network, thus participating in the consensus process.
2. Anyone in the world can send transactions through the network and expect to see them included in the blockchain if they are valid.
3. Anyone can read transaction on the public block explorer. Transactions are transparent, but anonymous/pseudonymous (shermin and valentine, 2017).

Proceedings of the 16th iSTEAMS Multidisciplinary
Research Nexus Conference
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

Private Blockchain
Write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Private blockchains are a way of taking advantage of blockchain technology by setting up groups and participants who can verify transactions internally. This puts you at the risk of security breaches just like in a centralized system, as opposed to public blockchain secured by game theoretic incentive mechanisms.

Hybrid or Consortium Blockchain
- Federated Blockchains operate under the leadership of a group. As opposed to public Blockchains, they don't allow any person with access to the Internet to participate in the process of verifying transactions.
- Federated Blockchains are faster (higher scalability) and provide more transaction privacy.
- Consortium blockchains are mostly used in the banking sector. The consensus process is controlled by a pre-selected set of nodes.
- The right to read the blockchain may be public or restricted to the participants.

Table 1: Summary of the properties of the three types of Blockchain Technology

Feature	Consensus determination	Read permission	Immutability	Efficiency	Centralized	Consensus process
Public blockchain	All miners	Public	almost impossible to tamper	Low	No	Permission-less
Consortium blockchain	Selected set of nodes	Public or restricted	May be tampered	High	Partial	Permission
Private blockchain	One organization	Public or restricted	May be tampered	High	Yes	Permission

2.4 TYPES OF ALGORITHMS
Zibin, et. al. (2017) and Karim, Umar and Rubina, (2018) talked about consensus algorithm and group it into the following;
i. Proof-of-Work (PoW)
ii. Proof of stake (PoS)
iii. Stellar Consensus Protocol
iv. Delegated proof of stake
v. Ripple
vi. Tender mint

Ali (2018), in her article, stated that apart from existing consensus algorithms, many more algorithms have been established which aim to solve the faults of the first ever, Proof-of-Work (PoW) algorithm system. There are other algorithms that are applicable to solving the limitations of consensus algorithm.

Mining algorithms: Data mining has three major components: Clustering or Classification, Association Rules and Sequence Analysis.

Traceability chain algorithms: Traceability proves the origin and practices behind a transaction while collecting additional data to improve internal process performances and planning activity of each node in a supply chain

Proceedings of the 16th iSTEAMS Multidisciplinary
Research Nexus Conference
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

Byzantine fault tolerance (BFT): This algorithm defines the dependability of distributed computing systems where components may fail and result in imperfect information.

An **algorithm** is a set of instructions that produces an output or a result. It can be a simple script, or a complicated program. The order of the instructions is important and the algorithm specifies the order. It tells the system what to do in order to achieve the desired result. It may not know what the result is beforehand, but it knows that it must have results (Ali, 2018). Algorithms tell the miners how to go about validating a block. They establish conditions, like protocols do, but the instructions are fundamental, and there is a desired outcome: to process transactions, to determine which blocks enter the chain, and to provide a consensus as to which chain is correct. Algorithms use the underlying protocol to achieve these goals (Ali, 2018).

Table 2: Source: A Simple Introduction to Blockchain Algorithms (Zee Ali)

COMPARISON OF THE FIVE CONSENSUS ALGORITHMS

characteristics	consensus algorithms				
	PoW	*PoS*	*DPoS*	*PBFT*	*RAFT*
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak

3. BLOCKCHAIN AS A HOST FOR DIGITAL CERTIFICATE

Academic credentials must be universally recognized and verifiable. In Nigeria today, verifying academic credentials remains largely a manual process, heavy on paper documentation. Distributed ledger technology (DLT) solutions could streamline verification procedures and reduce fraudulent claims of unearned educational credits. Employing blockchain security protocols will help in defending employers against people who claim to have a degree, but really don't. Unfortunately, people have been known to lie about their degree and qualifications to employers, claims that are difficult (if not impossible) to verify under the current systems. When a person enters the workforce, blockchain could be used to help assure employers that potential candidate have the qualifications that they claim on their resume, by storing that information in a secure ledger The diagram below illustrates the distribution of certificate (data) between schools, students, agency and employer in a blockchain system. No singular individual or agency can change or alter any data sent into the blockchain network. Any alteration must be by a consensus and the previous document cannot be removed which made it difficult for an individual to forge a document on the blockchain network.
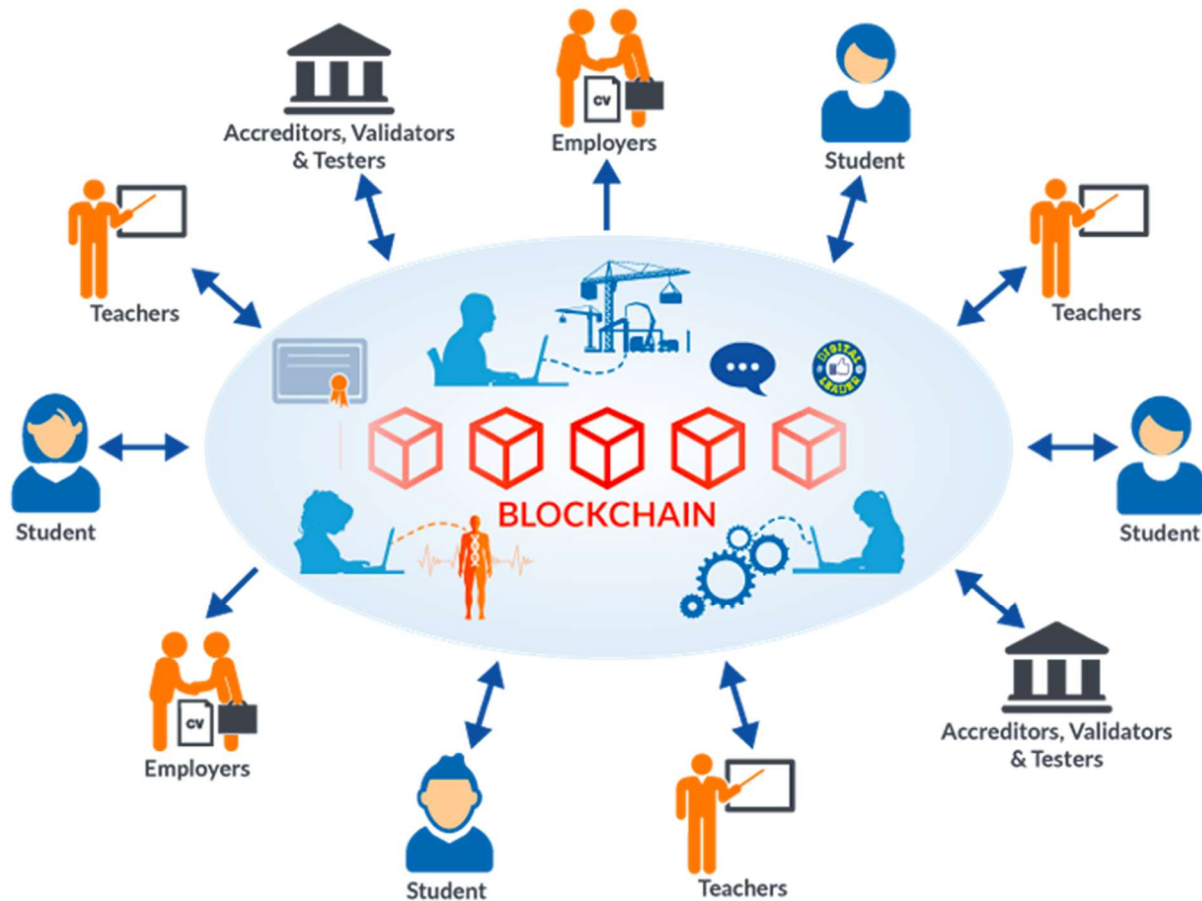
Proceedings of the 16th iSTEAMS Multidisciplinary
Research Nexus Conference
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

Fig 1: Source: Blockchain in Education. (2018)
https://medium.com/universal_blockchain.

3.1 Certificate in Blockchain Vs Paper certificate

If incontestable advantage of blockchain technology is that it will make the dematerialization of documents possible, it is also expected to aid in avoiding the risk of losing or falsifying paper documents. Paper-based higher education certificate, school certificates and extra training course certificates get lost and the original can be lost over time. Once put in blockchain, the information about a student's grades and the courses that have been undertaken will not get lost, and it is impossible to change or falsify the information. At the same time, one can easily access this information with the owner's consent.

Proceedings of the 16th iSTEAMS Multidisciplinary Research Nexus Conference
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

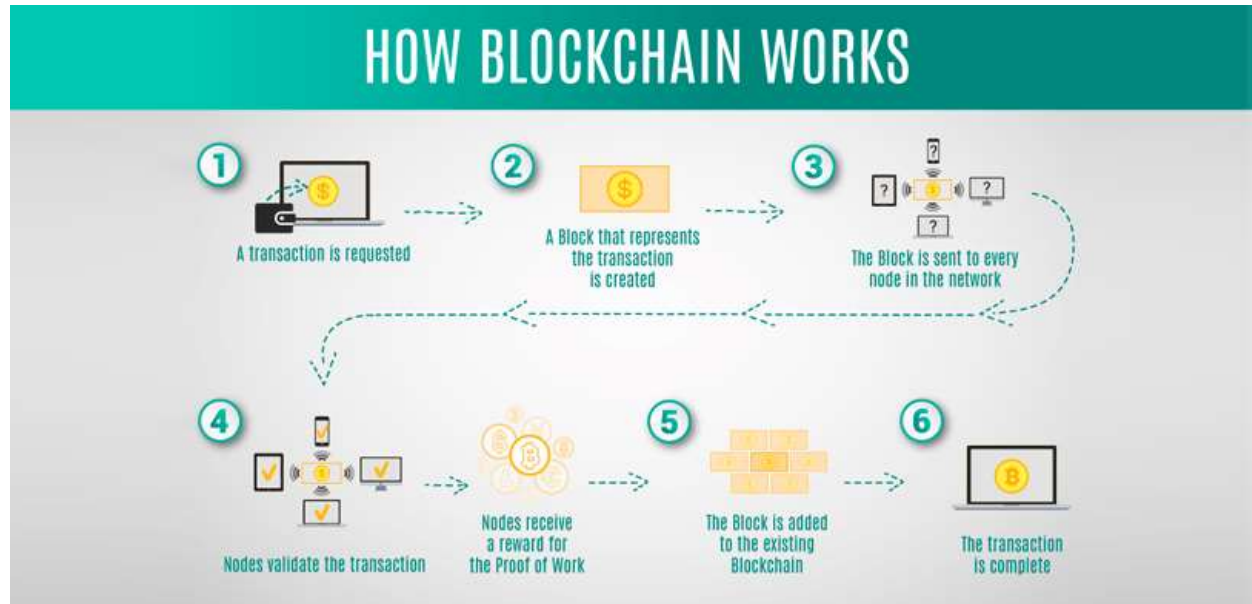## 3.2 How Blockchain works

Fig 2: Source: Blockchain in Education (2018) https://medium.com/universal_blockchain.

4. CONCLUSION

Putting information about education into blockchain will remove doubt for employers about an employee's level of knowledge. Using blockchain technology for storing information about one's level of education will make faking a certificate impossible. It is effective because it will solve the problem of low qualification levels of doctors, lawyers, engineers, economists and other occupations for which a formal education is required. Nowadays, recruitment for specific positions is a time-consuming and complex process. There is no single algorithm able to narrow the search down to only those applicants with the required knowledge. Rather than accumulating papers and certificates in education over their lifetime, people will be able to record information in blockchain, which will make it available to employers anywhere in the world. In addition to the issuance of certificates, educational institutions have to keep a paper record of students' progress for the entire duration of their study, thus creating a burden on the teaching and administrative personnel as well as a lot of bureaucratic impediments.

**Proceedings of the 16th iSTEAMS Multidisciplinary
Research Nexus Conference**
The Federal Polytechnic, Ilaro, Nigeria -
www.isteams.net

REFERENCES

1. Abati R. (0ct 02, 2018). Nigeria's Certificate Scandals. Retrieved from www.saharareporters.com/
2. Adam-Kalfon P. & El Moutaouakil. S. (2017). Blockchain, a catalyst for new approaches in insurance. Published by pricewaterhousecoopers advisory.
3. Ali Z. (2018). A Simple Introduction to Blockchain Algorithms. Retrieved from https://blog.goodaudience.com
4. Bisad A. (2018). Blockchain Consensus Algorithms Explained. Retrieved from https://www.mycryptopedia.com
5. Blockchain in Education. (2018). Retrieved from https://medium.com/universablockchain/
6. Carmen. H. (2010). Understanding blockchain technology and how to get involved. The 14th international scientific conference eLearning software for education, Bucharest, April 19-20, 2018 10.12753/2066-026X-18-000
7. Karim S, Umar R. & Rubina L. (2018). Conceptualizing Blockchains: characteristics & applications. 11th IADIS International Conference Information Systems Page 49-57. ISBN: 978-989-8533-74-6.
8. Manav G. (2018). Blockchain for Dummies, 2ndIBM Limited Edition. 111 River St.Hoboken, John Wiley & Sons, Inc, , NJ 07030-5774
9. Mohamed A.F, Makhlouf D, Mithun M, Abdelouahid D, Leandros M,& Helge J (24 Jun 2018). Blockchain Technologies for the Internet of Things: Research Issues and Challenges Retrieved from www.arxiv.org/abs/
10. RYAN A. (2009). Dataconomy. Retrieved from https://dataconomy.com
11. Samson Ezea, Tobi Awodipe, Ujunwa Atueyi, Sulaimon Salau, Benjamin Alade, Thomas-Odia I, & Jeremiah K. (2018). Discomfort over Nigerians' continuous involvement in certificates/documents forgery. Retrieved From https://tv.guardian.ng
12. Shermin V. & Valentine K. (2017). Blockchain:A Beginners Guide Retrieved from https://blockchainhub.net/
13. Tom V.A (2019). 20 Ways Blockchain Will Transform (Okay, May Improve) Education.Retrieved from
14. www.forbes.com/sites/tomvanderark.
15. Zibin Z, Shaoan X, Hongning D, Xiangping C & Huaimin W. (2017). An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends. IEEE 6th International Congress on Big Data. Page 557-564. 978-1-5386-1996-4/17