Original Research

Volume 5, Issue 2, pp 211-219, September, 2023

ACHIEVERS JOURNAL OF SCIENTIFIC RESEARCH

Open Access Publications of Achievers University, Owo

Available Online at *www.achieversjournalofscience.org*

Blockchain Technology: A Smart System Framework Towards Providing Human Immunodeficiency Virus (HIV) Patients in Nigeria, the Required Confidentiality

Olutayo, V.A.[1*] and Obamehinti, A.S.[2]

[1]Department of computer science School of Natural Science Joseph Ayodele Babalola University

[2]Department of Computer Science School of Science Olusegun Agagu University of Science and Technology

Corresponding Author E-mail: vaolutayo@jabu.edu.ng

Submitted: July 12, 2023, Revised: August 25, 2023, Accepted: September 02, 2023, Published: September 28, 2023

Abstract

Stigmatization in Nigeria has been for a long time. Over the years, patients living with HIV are often stigmatized and tend not to attend to their health condition due to the fear of further stigmatization. Every citizen living with ailment deserves to be treated as humans and do not have to go through the horrible face of being judged and secluded unnecessarily. Patient confidentiality is an integral part of the medical code of conduct and should be emphasized more due to the prevailing challenges caused by the existing medical system, hence the need for Blockchain technology. This research proposes a Blockchain technology, that will provide, anonymity, confidentiality of information's, high level security of HIV patient records and would prevent any form of tamperproof by health personnel.

Keywords: Patient confidentiality, Blockchain, Smart contract, Interaction, Block, Patients, Doctor.

1.0 Introduction

A smart system is a proposed application built for the purpose of protecting HIV patients records and give room for patients to interact with their physicians without the fear of a third party interference. The existing means by which HIV patients are attended is through physical means where a patient will have to come in to the hospital for regular checkup and administer medicine regularly. The list of medicine is sent to the pharmacy departments where the medicines are given to such patients. Also, the nurse in the hospital on duty have access to the file of such patients. There are cases where this patients face becomes familiar and certain health practitioners find it easy to place a face on the HIV patients there by discussing about such patients record to outsiders as against being strictly confidential.

According to Bulent Turan, *et al.* (2022) suggested that the association between perceived community stigma and affective, cognitive, and mental health outcomes self-esteem, depressive symptoms, avoidance coping, self-blame are mediated by internalized stigma. Furthermore, a serial mediation model suggested that perceived community stigma leads to internalized stigma, which leads to anticipated community stigma, which in turn leads to lower medication adherence. The associations between perceived

community stigma and interpersonal outcomes social support, trust in physicians. were mediated by internalized stigma and anticipated stigma, again in a serial fashion perceived community stigma leads to internalized stigma, which leads to anticipated stigma, which in turn leads to interpersonal outcomes.

Furthermore, Nelsensius Klau Fauk *et al.* (2021) researched using qualitative framework analysis was used to guide data analysis. Health stigma and discrimination framework guided the conceptualization and discussion of the findings. The findings presented the views and perspectives of healthcare providers that HIV stigma and discrimination toward PLWHA still occurred within families, communities and healthcare settings. These were reflected in negative labelling, separation of personal belongings, avoidance, denial of treatment and rejection of PLWHA by healthcare providers, family and community members (Waltering *et al*., 2015). This calls for an increased unification of existing analog and digital systems and for the development of a less error-prone model. As the digitization of public and private organizations evolves, customers and citizens are exposed to new kinds of vulnerabilities. Instead of passport theft or bank robbery, we are now worrying about hackers stealing identities or personal information, ("JPMorgan Chase Hacking Affects 76 Million Households," 2020). In such systems there is a large need of immutability, identification and redundancy; e.g. no one should be able to alter the prescriptions of a patient except for a doctor, there should be no doubt about the identification of all participants in the system, and there should not be a single point of failure. A traditional database system does only partly fulfill these requirements and alternative technologies should therefore be explored. In 2008 the basis for an immutable, cryptographically secured and distributed database system was laid with the introduction of Bitcoin and blockchain technology (Nakamoto, 2008). Since the implementation of Bitcoin in 2009, other applications of blockchain technology have emerged, mainly in the financial sector but also with non-cryptocurrency related use cases. Blockchain as a stand-alone technology, along with recent advances in computer science regarding secure multiparty computation, was proposed by Zyskind *et al.* (2021) as a method for access-control and the removal of trusted third parties when dealing with personal data. There has already been some exploration into the subject of using blockchain technology for digitalizing existing processes in the health care industry (Krawiec *et al..*, 2020).

Many high-level advantages to using blockchain for electronic patient records (EPRs), without any deeper technical analysis, are put forth in Braxendale (2016) and Nugent *et al*. (2020). It seems however that the current solutions available are either inefficient because of how the consensus mechanism is used in the blockchains, or that they are not secure and rely on the trust of a third part (e.g. government, company etc.).." Medication errors or adverse drug events are the most common cause of injury to hospitalized patients and are often preventable (Bobb, *et al.* 2014). Of adverse drug events, prescribing errors are the most common form of avoidable medication errors (Hamid *et al..*, 2016). There is however, a better approach, in USA as of April 2014, over 50 percent of the medical doctors were using electronic means for medical diagnosis and recommendation. Notably, the usage of so-called e-prescriptions has increased by at least 50 percentage points in 48 states from December 2008 until April 2014 (Gabriel, 2014). The change is also happening in Germany with the introduction of the E-Health Act in January 2015. Among other things that the act encompasses, is an electronic medication plan to be put to use by 2018 for all patients having three or more prescriptions. This is meant to lower harmful interactions between medications by informing doctors of what medications a patient is taking. In such systems there is a large need of immutability, identification and redundancy; e.g. no one should be able to alter the prescriptions of a patient except for a doctor, there should be no doubt about the

identification of all participants in the system, and there should not be a single point of failure. A traditional database system does only partly fulfil these requirements and alternative technologies should therefore be explored. In 2008 the basis for an immutable, cryptographically secured and distributed database system was laid with the introduction. The uniqueness in the characteristics of Blockchain technology, has given it the right solution to the existing system of lack of patient confidentiality which has led to stigmatization over the years.

2.0 Unique characteristics to aid the required confidence needed by the HIV patients

1. Persistency: Blockchain is persistent has such that it easily discovers blocks that contain invalid patient documentation\transactions.

2. Confidentiality/Anonymity: Blockchain has given a pace for each user to interact with a different address that does not reveal the real identity of the patient/client

3. Auditability: Blockchain stores data based on the user attended output by physician. Any patient already attended to would be switched to has pull of blocks to confirm such patients have been attended to and medical record securely kept.

4.Tamperproof: patients record in Blockchain technology cannot be tampered with due the its high level security system that often require two digital signature of primary and secondary key before access can be gained into the system.

3.0 Blockchain Design Methodology

The proposed method for protecting human right, is adopted from Karamitsos *et al.* (2018). The design methodology for human right protection is composed of the following steps, first for any user the setup of the Ethereum node is required. Second, the functions is defined and finally, the process between the government, law enforcement agencies and citizens are described in the following sections. The figure in 4.1 shows the structure of the Blockchain and how it helps the citizens interact with the government and also have access to the constitution without the citizen identity being identified.

3.1 Smart Contract Structure

The principle parts of the smart contract are a lot of executable capacities and state factors. Every exchange has input parameters which are required a capacity in the agreement. Amid the execution of a capacity, the status of the state factors is changed relying upon the rationale usage. The smart contract code is written in abnormal state dialects, for example, Solidity and Python for Ethereum applications. The code is aggregated into bytecode utilizing compilers as Solidity or Serpent. The agreement code will be transferred into the Blockchain once the compiler is executed with no mistakes. Each agreement will be allotted a one of a kind location by the Blockchain organize. Ethereum is one of the favored advances for the improvement of the keen contracts. The fundamental segments for the exchanges depend on state machine and capacities. It is a Turing-complete contract handling and execution stage based of a Blockchain decentralized shared record. The plan and the usage of the Ethereum are absolutely autonomously from the digital money Bitcoin. An abnormal state programming language called Solidity is utilized to compose brilliant contracts and decentralized applications (Dapp). The software engineer can make their exchanges groups, state changes and occasions capacities, and guidelines for proprietorship.

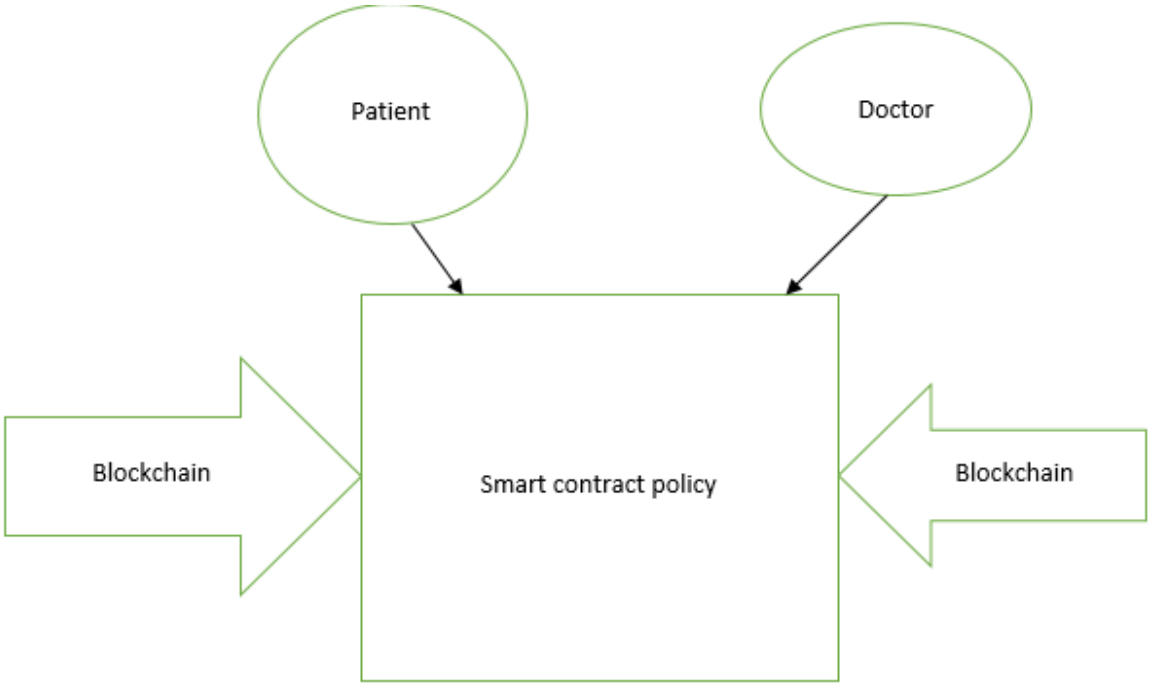

Figure 2.1 use case of the proposed HIV patient confidentiality application

Patients are assumed to be private persons, seeking medical care at one of many healthcare providers, in this thesis simply called Doctors. Doctors are assumed to be certified, medical professionals, in possession of a state-issued license and authorization to practice medicine. Pharmacies are defined as only those commercial or state-owned outlets possessing the legal right to sell prescription medications to patients. The requirements are described in a less formal way in Figure 2, where the different users are shown interacting with the Blockchain, on which the smart contracts reside. In bullets next to them are the actions they need to be able to perform. There are some requirements that apply to the general system and not just to one user specifically. Some of them are described in part by the user stories, but for the sake of exhaustiveness and application to users not in the system, they are explicitly written below.

1. It must be impossible, for a non-admin account, to connect prescriptions to the identity of a patient, doctor or pharmacy without the consent of the user in question.

2. Only those permitted to should be allowed to connect to the network.

3. There must be an immutable traceability built into the system, where it is possible to see:

1. Who prescribed a certain medication?

2. If a medication was sold after it having been prescribed

3. Where it was sold Immutable traceability means that there must be a history of changes made to prescriptions and that it must be made very difficult, if not impossible, to alter it post ex.

4. Smart contracts must be exchangeable without needing to re-move the entire system

or change addresses to contracts with which humans interact.

4.0. Testing and Results

In the testing of application, metamask is used to test the result of interaction that depicts patients confidentiality using a smart contract as the policy guide for interaction. A solidity programming language is use to write the codes on a remix ide compiler.

- Remix ide: the compiler used as indicated in figure 4.1 is a remix ide.
- Solidity language: the smart contract as it is indicated in figure 4.1 is written in solidity high level programming language.
- Environment: the environment where an ethereum smart contract can be executed is on an ethereum virtual machine environment. For the purposed of this research, an injected web3 environment is used to execute the smart contract code.
- Account: the account as it is indicated in figure 4.1 is the ethereum wallet account where the ether which is the money spent in an ethereum blockchain for the purpose of land transaction is saved.

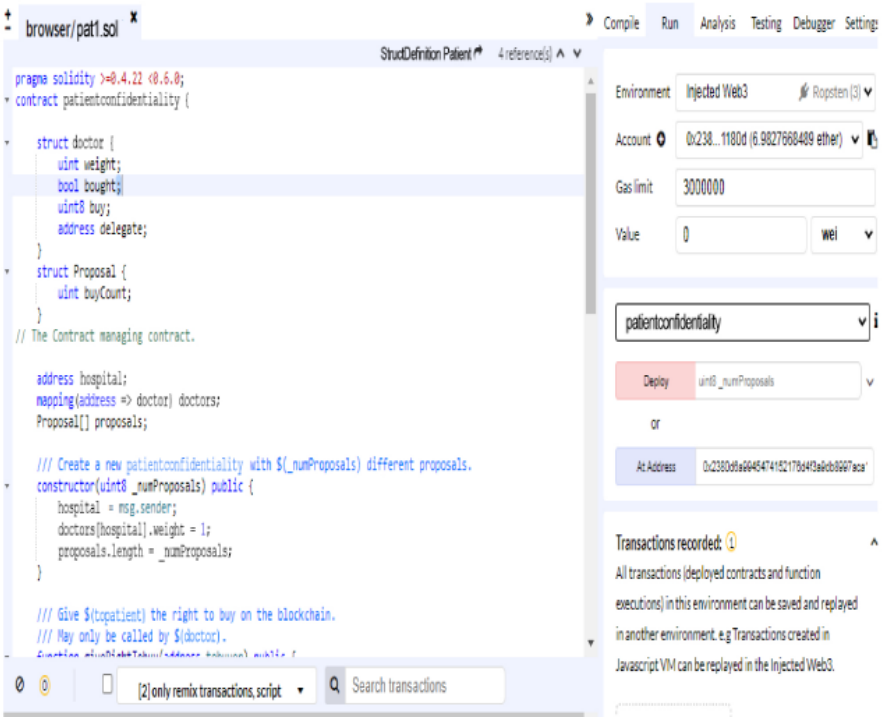

Figure 4.1. Patient's confidentiality Smart contract

4.1 Transaction Confirmation

Using rospten test network where MetaMask is the bridge between the test network and the patientconfidentiality smart contract. This is done to indicate that every participant of the blockchain has verified the contract deployed by the patient and can be transacted to the doctor to initiate confidential conversation. Figure 4.2 and 4.3 indicate the patient interaction between the doctor and the owner of the account which happens to be the patients is established and secured. Furthermore, in this section a comparison is drawn between two confirmed interaction/contracts to indicate the authencity, transparency and avoidance of information leakage of patient files to a third party. of land transaction in the landtransaction blockchain network.

Ropsten Network Setup

- Interaction/Transaction hash**:** is a unique id that is generated for every interaction/transaction that is performed in the blockchain network. For every transaction confirmed, there is a different id and with this it has avoided the problem of double spending in the land title management and transaction. The status shows it was succesful, this indicate that the transaction is genuine and the nodes have used their public key to verify the genuineness of the interaction/transaction.
- Block: there is a unique block number for every node(participant) in the ethereum blockchain, the blockc number indicates a block was successfully mined by the miner also it indicates that the transaction was confirmed by 53503 nodes in the blockchain, this in a way has created a transparent system of transaction where it is decentralized and cant be tampered with by anyone. This has defeated the use of third party and patient file leakage.
- From and To: the from is the patient/owner of the transaction and to is the doctor . A unique id is also given to the patient and doctor for the purpose of anonymity when doing an interaction. This as also fulfilled another purpose of making the patient anonymous.
- Nonce: the nonce for this blockchain application is the arbitrary number that is used just once for the purpose of crytopraphic communication the blockchain network. It a random number that is used for the authentication protocol of this transaction in the block so as to make attack or replay of the same interaction/transaction impossible.
- Time stamp: The server for time stamp works by taking a hash of a block of item to be time stamped and widely publishing the hash. Time stamp prove the data must have existed at a time.

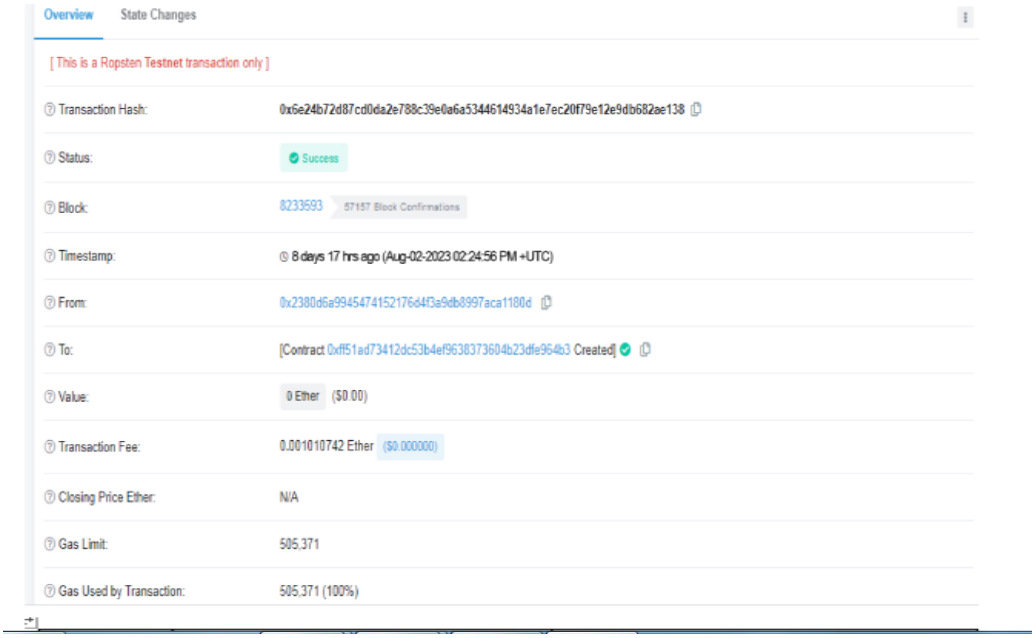

Figure 4.2 Patient confidentiality 1 interaction results.

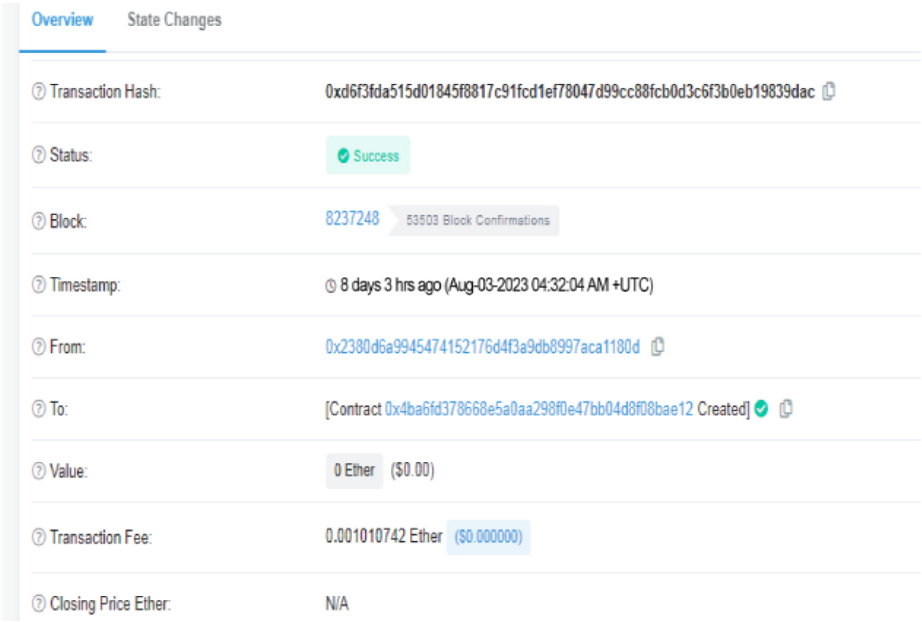

Figure 4.3 Patient confidentiality 2 interaction results

Table 4.1 unique difference between interaction in figure 4.2 and figure 4.3

functions	Patientconfidentiality 1	Patientconfidentiality 2
Transaction hash	0xd6f3fda515d01845f8817c91fcd1ef78047d99cc88fcb0d3c6f3b0eb19839dac	0x6e24b72d87cd0da2e788c39e0a6a5344614934a1e7ec20f79e12e9db682ae138
Block	8237248	8233593
Block confirmation	53503	57157
Time stamp	8 days 3 hrs ago (Aug-03-2023 04:32:04 AM +UTC)	8 days 17 hrs ago (Aug-02-2023 02:24:56 PM +UTC)

5.0 Conclusion and Contributions

At the end of this research, it would change the modus operandi of how HIV patients are being attended to and other related health care is carried out in Nigeria. The Blockchain system if adopted, will contribute tremendously to economic development of the country. The following are the areas in which Blockchain used to manage health care has contributed to the country:

- Promoted patient confidentiality in hospitals
- Durability of patient's record
- Promote better health care system
- Reduce congestion in hospitals

References

Nelsensius, K.F., Paul, R.W., Karen, H. and Mwanri, L. (2021). HIV Stigma and Discrimination: Perspectives and Personal Experiences of Healthcare Providers in Yogyakarta and Belu, Indonesia. https://doi.org/10.3389/fmed.2021.625787

Turan, B., Budhwani, H., Fazeli, P.L., Browning, W.R. and Raper, J.L. (2022). How Does Stigma Affect People Living with HIV? The Mediating Roles of Internalized and Anticipated HIV Stigma in the Effects of Perceived Community Stigma on Health and Psychosocial Outcomes https://doi.org/10.1007%2Fs10461-016-1451-5

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

Tschorsch, F. and Scheuermann, B. (2018). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communication Survey Tutorial*, 18, 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

Karamitsos, I., Papadaki, M. and Al Barghuthi, N.B. (2018). Design of the Blockchain Smart Contract: A Use Case for Real Estate. *Journal of In-formation Security*, 9, 177-190.

Kraft, D. (2020). Difficulty control for Blockchain-based consensus systems, *Peer-to-Peer Networking and Applications*, 9(2):397–413.

Jpmorgan chase hacking affects 76 million households. (2014). The New York Times, http://nyti.ms/1rQi4vG

Zyskind, G., Nathan, O. and Pentland, A.S. (2021). Decentralizing privacy: Using blockchain

Krawiec, R., Housman, D., White, M., Filipova, M., Quarre, F., Barr, D., Tsai, L. (2020). Blockchain technology: Opportunities for healthcare. This white paper was developed in response to the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) ideation challenge.

Nugent, T., Upton, D., and Cimpoesu, M. (2020). Improving data transparency in clinical trials using blockchain smart contracts doi:10.12688/f1000research.9756.