Journal of Multidisciplinary Engineering Science Studies (JMESS)
ISSN: 2458-925X
Vol. 6 Issue 5, May - 2020

Application Of Computational Tri-Nodal Blockchain Technology In Medical Diagnosis Of Out-Patient Treatment And Management

E. E. Jumbo
Dept. of Mechanical Engineering, Niger Delta University, Bayelsa State, Nigeria

V. Zalizko
Faculty of Economics, Taras Shevchenko National University of Kyiv,
Kyiv, Ukraine

E. Rove-Steiner
Dept. of Medical Microbiology, Poma Int'l Business University, Rep. du Benin

***Abstract*—Technology driven solutions are required in response to growing need for better global health care delivery, especially where patients' medical histories are undocumented for referencing. At certain times, patients are unable to access their health care providers or medical facilities for diagnosis and treatment due to their remote distance or location, thus resulting medically related emergencies which sometimes could be fatal or leading to irreversible damage to body tissues or vital organs. The study thus aims at the development and deployment of appropriate blockchain technology with integrated capacity for the processing and storage of medical data for out-patient diagnosis and treatment. In order to achieve this, a blockchain oriented mathematical proof of work was developed; the basis of which an analysis of tri-nodal inter-relationship was performed to show how all members of the proposed blockchain scheme can interact with each other to achieve the common objective of medical diagnosis and drug dispensing on a general consensus basis required of trustless systems. The foreseeable result of the model when implemented is the successful diagnosis and treatment of out-patients on the basis of medical data transmission on a blockchain and subsequent inter-related activities using mobile phones as nodal entry points. The result would further affirm the applicability of blockchain technology in medical diagnosis, logistics, financial management and data storage on the basis of tri-nodal consensus and immutability of originated transaction records.**

Keywords—decentralization, distributive, proof of concept, Byzantine faults, informationization, fault tolerance, internal sub-structures, data encryption

I. INTRODUCTION

Blockchain technology has been variously described as possessing disruptive potentials capable of restructuring the *modus operandi* of most aspects of modern industrialization; on the basis of structured "proofs of concept" particularized for the respective application.

Consequently, Gartner originated a technology hype cycle graph, which indicated that as at, July 2016 blockchain technology among other technologies such as, machine learning, smart robots, connected homes, cognitive expert advisors, autonomous vehicles etc., started taking center stage of manufacturing enterprise.

As could be seen from Fig. 1 below, the *peak of inflated expectations* implies that these identified technologies are significantly impacting on the

way or approach to most industrial and domestic activities and the results on the human development index in the areas of human life that they impact on. In view of the foregoing, most industries are currently researching and leveraging on blockchain technology and adopting same with specialized applications for the particular industry [1].

Thus, the blockchain is a decentralized distributed system; and in this distributed system, two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome where all entrants interact on the basis of a single logical platform. Thus, a *node* can be defined as an individual entrant or player in a logically distributed system or network.

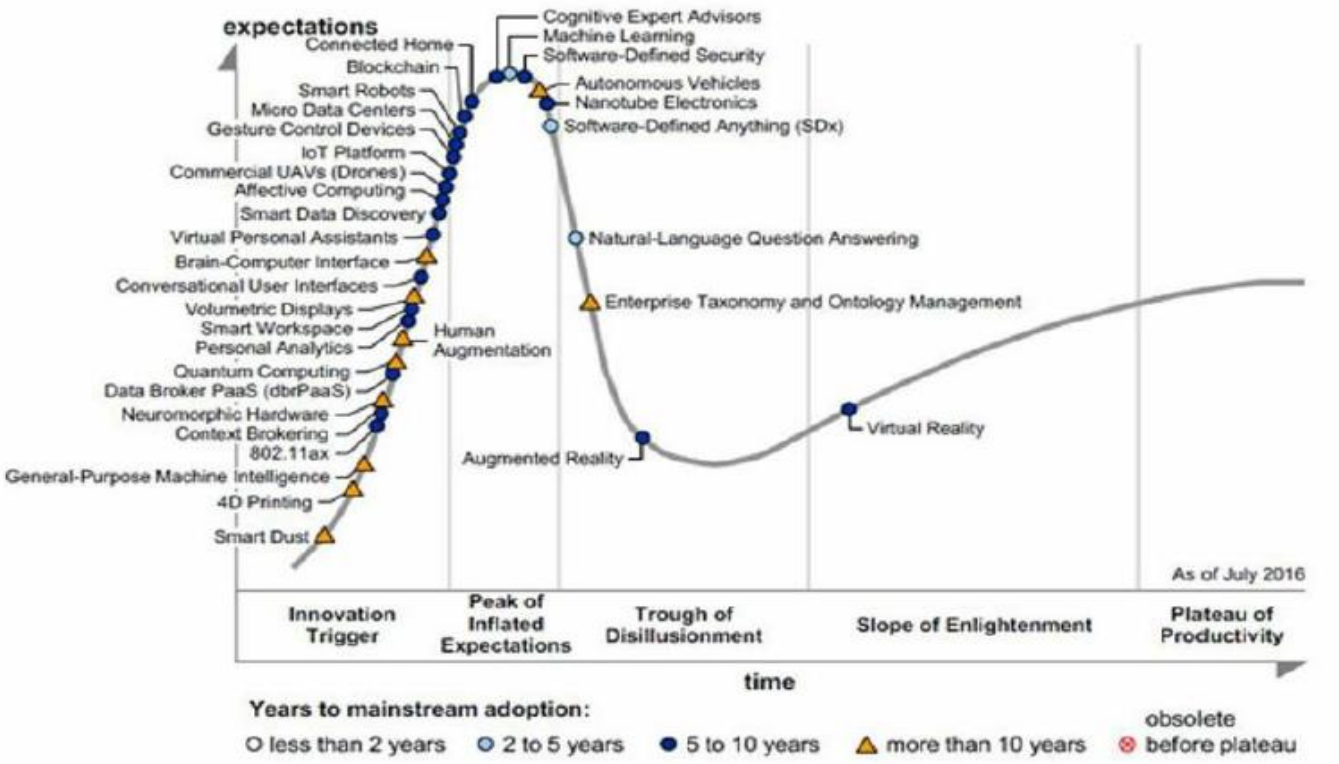

Fig. 1: Gartner Hyper Cycle for Emerging Technologies, 2016.
Source: Imran Bashir, Mastering Blockchain, 2017 [1].

Consequently, all nodes in a network are capable of sending and receiving signals and messages from each other. And due to the transparency and immutability of the system, the integrity of the system is the major driving force, while keeping *Byzantine faults* under checks, thereby eliminating or reducing the impact of arbitrary nodal behaviors that are malicious in nature and detrimental to the operationalization of the strategy.

The purpose of this work therefore is to propose a network of tri-nodal distributed ledger system that can be supported by a condensed computational structure that is capable of segmenting the individual nodes into particular, inter-related and combinatorically analyzable components. In this regard, such nodal interplay, has the ability to create and sustain operational balance between sending and receiving of messages and subsequent anticipated response.

The proposed model therefore relies on the integrity of the nodes and the flow of information through their interconnecting links. Further, since blockchain technology abhors centralization of the controls, it is important to state that under a nodal management of information, each node create its strategy for data generation, analysis and implementation in a transparent manner, validated by the other nodes under a set of rules acceptable to all.

II. SUPPORT STRUCTURES OF AN EXECUTABLE BLOCKCHAIN STRATEGY

It should be noted that while blockchain technology is directly deployable to virtually all facets of human endeavor, the main challenge incidental to its multi-capability under a trustless distributed system is the efficiency of coordination between nodes, fault tolerances and bias limits. This implies that, enabling structures should be able to withstand inadvertent attacks or malfunctioning of nodes and network links, and continue to deliver efficient services, within defined performance parameters.

In response to the foregoing, applications of blockchain technology in medical fields, with respect to Electronic Medical Records (EMRs) documentation; there are reports of the development of specialized blockchain applications to aid the reform of *informationization* processes, especially in the handling of records in medical facilities [2]. These records are mainly data generated from patient's medical history, physical conditions and known drug interactions with patient's medical situations.

Although these records have been shown not to be reliable when taken directly from the patient each time he presents for treatment; it was reasoned to be due to patient's inability to accurately remember quantitative values of historical conditions, such as blood pressure history, blood sugar, and other vital body signs. The second observed difficulty, borders on the patient's inability to use proper medical terms to describe his condition. This has often been

observed to affect the medical personnel assessment and understanding of the patient's conditions [3]. Hence, a crucial support structure to the deployment and application of the proposed model in this paper is the patient's medical records.

Thirdly, the study found that a crucial support structure is the theoretical framework that establishes all possible interaction pathways. During design of this framework, the weak points of the model were identified and solutions were generated and incorporated into the structural templates. Further, this theoretical sub-structure also serves as the basis for efficiency, structural consistency, availability and position tolerance.

In addition, the fourth support structure deals with machine state replication, which is a central feature of blockchain design, where fault tolerance is modeled into the design to take care of situations where a faulty node crashes without any signal or initial indication. In another situation, fault tolerance also takes care of faulty nodes that exhibit malicious or inconsistent arbitrary behaviors [1]. The fifth support structure is the enabling programming language and software that captures all the identified substructures and integrates them into an executable program scheme where resources, targets and instructions are resolved in the desired directions, with all the necessary feedback mechanisms.

The sixth support structure is the nature of data protection that must be incorporated into the program to prevent data or patient information leakage. This is due to the fact that the harm that can be occasioned by the leakage of medical records is enormous [3] and traces for such internal leakage have been reported to be difficult [4] due to the intricacies and attraction of financial benefits of the syndicacy network or chain of involvements.

Accordingly, it has been reported that in 2018 an employee of Med Association (a medical billing company) had his computer invaded by an unauthorized person who may have stolen medical information of over 270,000 patients. In
view of the negative impact of data theft in healthcare administration, it has been reported

that the protection of EMR sensitive data is not only a crucial support structure but also an emerging research trend, capable of large scale investigation and investment [5].

The seventh support structure is the need for patients to be involved in the management of their medical records. This crucial support structure which necessitates our proposed model also draws attention to the possibilities inherent in blockchain codification with respect to patients participation in the management of his own health and is due to the fact that in most advanced health care systems, patients only give information or submit to various diagnostic tests to ascertain their health conditions; but after that, the data generated by the patients are no longer within the control of the patients, this makes the patients vulnerable to various attacks in terms of drug marketing, directed medical surveys and many other exploitative measures.

Unfortunately, the patients are not usually aware that they were specifically targeted by such pharmaceutical companies and concerns. Accordingly, the proposed tri-nodal blockchain model can solve this problem by making the patient a necessary party and operator of a node, where he is prompted for consent before his information can be released to any third party or organization.

III. OPERATIONALIZATION OF A TRI-NODAL DISTRIBUTIVE MEDICAL BLOCKCHAIN NETWORK

As observed above, a medical blockchain network can be executed under a tri-nodal structure with fully responsive internal substructures or information flow under the following subsections:

A. Proof of Work Method

In this design, the flow of information requires two layers of request and access authorization as indicated below:

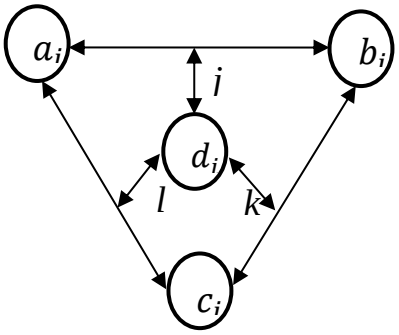

Fig 2: structural nodes and links

Where:

a_i node -represent the medical facility or the doctor

b_i node -represents the pharmacist or drug dispenser

c_i node -represents the outpatient in a remote location

$i(abc)$ -represents the first layer of request and authorization

$d_i(jkl)$ -represents the second layer of request and authorization

Thus, information flow on the blockchain with respect to patient's diagnostic requirement on a first layer request could be structured under a two-step reversible-direction computational analysis, decentralized under the following relativity:

$$a_i \leftrightarrow b_i = \sum a_i b_i + a_i b_i [j_1 j_2 j_3 \dots\dots\dots\dots j^{th}]$$
$$= \sum i(ab) + i(ab) [j_1 j_2 j_3 \dots\dots\dots\dots j^{th}]$$
$$= j \in d_i (ab)i \dots\dots\dots\dots\dots\dots \quad (1)$$

$$b_i \leftrightarrow c_i = \sum b_i . c_i + b_i . c_i [k_1, k_2, k_3 \dots\dots\dots\dots k^{th}]$$
$$= \sum i(bc) + [i(bc)(k_1, k_2, k_3 \dots\dots\dots\dots k^{th}] \text{ and}$$
$$= k \in d_i (ab)i \dots\dots\dots\dots\dots\dots \quad (2)$$

$$c_i \leftrightarrow a_i = \sum c_i . a_i + c_i a_i [l_1 l_2 l_3 \dots\dots\dots\dots l^{th}]$$
$$= \sum i(ca) + [i(ca) [l_1 l_2 l_3 \dots\dots\dots\dots l^{th}] \text{ and}$$
$$= l \in d_i (ca)i \dots\dots\dots\dots\dots\dots \quad (3)$$

The foregoing analysis is representative of first layer information or data request, validation and nodal authorization paths where the players in the network can create data visible to all, by the necessary consensus activities. For instance $a_i \leftrightarrow c_i$ reflects patient and doctor interaction which is also visible to the pharmacist or dispenser.

This information produces different forms of data which can be entered by the parties at their various terminals and made accessible by #key code specific to the individual's terminal. Under this condition the #key codes are the first layer of protection such as; $\#a_i$, $\#b_i$, $\#c_i$, where a_i, b_i and c_i are independent parameters or particulars incidental to the individual's position in the network.

B. Primary Layer of Data Encryption, #identity

It should be noted that individual member has qualifying activity shared and known to all at the inception of the network. The information such as the doctor's or pharmacist's academic and professional qualifications, experiences and work history and those of the patient's medical history and other related personal information such as blood group, genotype, work hazard exposures, etc., form the primary data that are relatedly stored under $\#a_i$, $\#b_i$, $\#c_i$, protocols. These information forms the initial data that is supplied into the network and shared by all with no possibility of change once nodal verification has been done by all the nodes. Such primary data are the basic building blocks.

C. Secondary Layer of Data Protection, #process integrity

Under this layer, the network is believed to be trustless and as such must be protected from *Byzantine effects* by requiring that access, validation and authorization would be needed from the particular member of the network who must issue a digital certificate on a *no trust basis*, thus requiring the consistency of trust on the other member to validate the information. For instance, if c_i interacts with b_i on the basis of a_i directives, then c_i will grant access to its data transmissions with a_i to b_i on the validating condition that the information is safe with b_i, leakage of which should be counted on b_i. This is the secondary layer of data protection represented in Fig 2 as d_i.

On the other hand, if b_i is a *Byzantine node* on account of the public nature of the node, then the proprietary of b_i integrity must require special purpose secondary protection specific for the node.

IV. SYSTEMATIC NATURE OF SEGREGATED BLOCKCHAIN NETWORKS

In view of the requirement for sustainable CAP or Brewer's theorem; as could be seen in equation (1) and (3); note that operators *j,k,l* are tri-nodal consequences of the segregated network, *∑(abc)i,* where their interlacing factor *(ᵢ-factor)* must be the effect of their sum on the segregated network. Thus;

$$_i\text{-factor} = \sum j \in d_i(ab)i + l \in d_i \ (ca) \quad (4)$$

It should be noted that equation (4) implies that if *i*-factor is possible, then consistency, availability and partition tolerance (CAP) can be achieved simultaneously at any point of nodal or cumulative network entry, exit or systematic analysis. Further, equation (4) is indicative that if CAP are properties inherent in a node, then they can be extracted individually or collectively from other nodes on consensus or permissioned basis.

V. APPLICATION OF PROPOSED MODEL AS PROOF OF CONCEPT

The tri-nodal distributed ledger as proposed in this paper can be applied under a remote diagnostic and out-patient treatment and management. Under this platform, network link a_i and b_i is established as a permissioned ledger and as such do not deploy any distributed consensus mechanism. This imply that the relationship of a_i and b_i is an agreement protocol validated by their shared version of truth about their individual entries in the records on the blockchain. Consequently, a patient in a remote location without direct access to a medical facility can access this network through his mobile phone using a created app or USSD codes generated for the network.

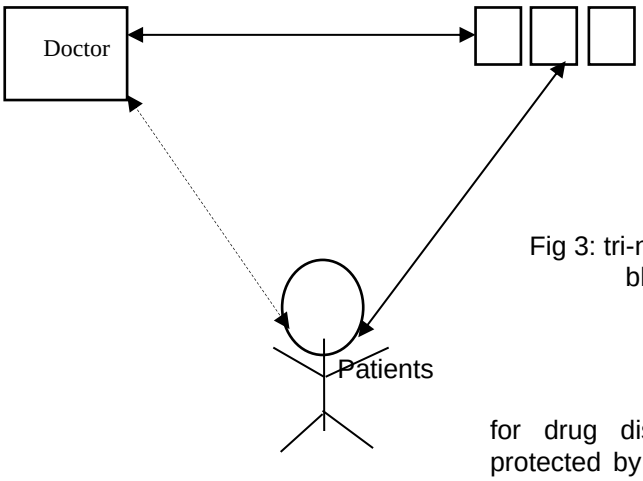

Fig 3: tri-nodal outpatient diagnostics blockchain triangulation

On the basis of Fig 3, the patient becomes a member of the network by establishing a contact with the doctor or medical facility within the parameters of equation (5) expressed as:

$$c_i \leftrightarrow a_i = \sum c_i.\ a_i + c_i a_i\ (l_1 l_2 l_3 \ldots l^{th}) \qquad (5)$$

The patient's network entry effort in equation (5) establishes $\#c_i \leftrightarrow \#a_i$ which is a node and a network link with the already created blockchain $\#a_i \leftrightarrow \#b_i$, which upon completion of diagnosis, the second arm of the chain is established by a link to the pharmacist or drug dispenser and executed as: $\#c_i \leftrightarrow \#b_i$.

The foregoing implies that $\#c_i \leftrightarrow \#a_i$ requires the medical data or information of the patient which can be executed through information entry into the ledger $\#c_i$ where bio-data such as temperature, blood pressure, weight, eye colour and other vital body signs can be captured under a time and data stamp. Since patient's data under $\#c_i$ could be received through patient's responses to a set of well-structured questions supplied through a mobile device. Additionally, for patients in remote locations, each of the question is a vector in the $l_1, l_2, l_3 \ldots l^{th}$ parameter framework and forms the basis for the second layer of proprietary data that must be protected by the network.

Thus, well written computer codes using a digital app platform or USSD codes for responses to questions can be the means of data entry into the blockchain network. This means the chain must be adequately supported by a data service network operator, so that patients in remote locations can be diagnosed of ailments by highly trained medical personnel, using their phones and other mobile devices, and all information are entered into the blockchain and made visible to all members of the network, as depicted in Fig 3.

A. The Network Link, $\#c_i \leftrightarrow \#b_i$

This link under nodes c_i and b_i established data sharing relationship between the patient and the pharmacist and all communications are visible to the doctor or the health facility. This means that the digital certificate of data entry from patient c_i as validated by doctor a_i is transmitted to pharmacist b_i for drug dispensing, and all data entered are protected by $\#b_i$ node and the other nodes. Hence, the consistency of this node determines the integrity of the system and guarantees its availability.

B. Dispensing of Prescription, $\#c_i \leftrightarrow \#b_i$

It is important to note that under this scheme the blockchain network envisage a one direction drug administration from pharmacist $\#b_i$ to patient $\#c_i$. However, the blockchain is also designed for $\#d_i$, which is an internal central information storage and sharing to be visible to all members in the network. This central node is not controlled by any authority but automatically updates itself upon the consensus validation of all the nodes with respect to final entries from any of the nodes.

It is a full proof invulnerable data backup center, sub-linked by *j, k, l* to individual nodes in the blockchain*;* this means doctor $\#a_i$ also has access to the drugs dispensed by $\#b_i$ through a permissionless access to $\#d_i$ and can validate it alongside patient $\#c_i$ who is to receive the drugs and also login the information of his progress with the treatment procedure for doctor $\#a_i$ to evaluate for further necessary action. Under this scheme each node can operate from different locations around the world. In practical terms, the pharmacist or drug dispenser has the obligation to arrange for the mobility or logistics of the drugs and upon dispatch is required to log in the information on the blockchain for tracking and tracing by the other members of the tri-nodal network.

C. Service Payment and Prescription Logistics Under the Network

The blockchain commences with all parameters defined for nodal activities. The proposed platform create opportunity for payment from out-patient $\#c_i$ to doctor $\#a_i$ or pharmacist $\#b_i$ when certain defined consensus obligations have been performed. This imply that out-patient $\#c_i$ may be located in another country different from that of other members of the blockchain and should not have any difficulty in sending payment to either of them. For this purpose, international online payment platform can be integrated into the protocol but not as a node, although payment details are logged into the ledger with transaction details. Thus, the integrated payment services provider must necessarily send report of receiving and transferring the payment to out-patient

$\#c_i$ who in turn enters such proof of payment on the ledger for the validation of the other nodes. This principle also applies with the logistics for drug dispensing from the pharmacist $\#b_i$ to the out-patient $\#c_i$.

D. Single Entry and Simultaneous Storage Data Management

It should be observed that from Fig 2 template, data response in $\#a_i, \leftrightarrow \# b_i$ are simultaneously entered into the central server node $\#d_i$ using link $\overset{\leftrightarrow}{}_j$, same applies to other nodes linked by $\overset{\leftrightarrow}{}_k, \overset{\leftrightarrow}{}_l$. The importance of this double entry is to ensure that all information in all nodes is available on all other nodes and also available at $\#d_i$ data backup. The implication is that, the system is immutable to the extent of its consistency and in the sense that all nodes has access to the information generated by all other nodes. Such access are permissive by reason of digital certificates issued by the individual node operator; consequently, access to $\# d_i$ is shared between the members and any addition of data or information from any of the nodes is simultaneously added to the central $\#d_i$ platform.

Secondly, the single entry double storage ensures a completely distributed data interface making Byzantine conditions almost inexistent and fault tracing easy and efficient.

Conclusion

The paper has significantly considered the application of blockchain technology in medical diagnosis in situations where the out-patient is unable to access the medical facility. In order to achieve this the patient in this study has been viewed as a necessary node in a blockchain network and is capable of sending and receiving messages that are significantly protected, transparent and immutable in the tri-nodal blockchain syntax.

The success of the blockchain lies in the integrity of the nodes as exemplified in the mathematical derivations designed to support the tri-nodal dimensions of the proposed model.
In support of the foregoing, it has been shown that Electronic Medical Records (EMRs) can be collected from patients in remote locations through their responses to questions sent via mobile phones and by responding to those questions on platforms presented by standard medical diagnostic apps or USSD codes operated on the blockchain.

In order to operationalize the tri-nodal distributive ledger under this model, a proof of work scheme was executed to show that nodal consistency, availability and provenance are crucial to the sustainability of an executable blockchain when applied to medical and related fields. Further, the single entry simultaneous storage data management implies the simultaneous storage of data at a central consensus validating server only accessible for information retrieval without any possibility for adjustment should any node develop a Byzantine fault.

The conclusion of this paper is that this model is capable of delivering medical solutions to patients in very remote locations by reason of blockchain intervention in all areas incidental to health care delivery since, on the same platform the doctor and the pharmacist can interact with the patient for the purposes of his diagnosis and treatment at a cost effective manner.

References

[1] I. Bashir, Mastering Blockchain, distributed ledgers, decentralization and smart contracts explained, Packt Pub. Birmingham, UK, 2017, p.1

[2] S. Fang, Z. Cai, and W. Sun, Feature selection method based on class discriminative degree for intelligent medical diagnosis. Comput Mater Continua 2018; 55(3): 419–433.

[3] Y. Zhang, M. Cui, L. Zheng, R. Zhang, L. Meng, D. Gao and Y. Zhang, Research on electronic medical record access control based on blockchain, International Journal of Distributed Sensor Networks, (IJDSN) 2019, Vol. 15(11)

[4] D. Bi, K. Dong, X. Luning, Analysis and prospects of health care big data industry. Big Data Era 2017; 4:6–20.

[5] J. Zhang, H. Li, X. Liu, On efficient and robust anonymization for privacy protection on massive streaming categorical information. IEEE T Depend Secure Comput 2017; 14(5): 507–520.