Review Article

A review on healthcare information systems and consensus protocols in blockchain technology

Cleverence Kombe[1*], Mussa Ally[2] and Anael Sam[3]

PhD Scholar, School of Computational and Communication Science and Engineering, Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania[1]
Lecturer, School of Computational and Communication Science and Engineering, Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania[2]
Senior Lecturer, School of Computational and Communication Science and Engineering, Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania[3]

Abstract
Blockchain is a distributed ledger technology whereby transactions are bundled into blocks that are chained together cryptographically by hash pointers. Blockchain solutions add trust and privacy to the existing internet due to its tampering resistance and advanced cryptography characteristics. In healthcare systems, the technology has been implemented to ensure transparency, auditability, interoperability, and proper governance and management of patient information. This study evaluates blockchain based healthcare systems. Three most common systems were chosen from public, private/consortium blockchains. The evaluation was done using framework for performance monitoring for blockchain systems. To describe resource usage, we used five performance evaluation metrics i.e. memory consumption, disk write and read performance, network data utilization, transaction execution per unit time, and central processing unit (CPU) usage. The study revealed that the system developed using consortium-based platform outperformed private and public blockchain for more transactions per unit time, and proper utilization of resources of connected nodes such as CPU, Memory, and Disk storage.

Keywords
Blockchain healthcare systems, Consensus protocols, Performance evaluation, Framework, Interoperability, Public blockchain, Private blockchain, Consortium blockchain.

1.Introduction
Blockchain technology is a distributed electronic ledger of digital records, events or transactions that are cryptographically secure, extremely hard to forge, and updateable through a consensus protocol agreeable to all connected nodes. [1] The technology uses decentralized consensus algorithms to control database consistency. The database is purely distributed in nature and is shared to all nodes connected to the network. Transactions in the databases are bundled together for specified period of time to form a block of certain number of transactions. These blocks are linked cryptographically through hash pointers to form a chain of blocks with transactions (*Figure 1*) [1–3].

The technology has a multitude of applications in various sectors including but not restricted to financial services, retail and consumer goods, energy, higher education, transportation, manufacturing, and telecommunication technologies. It can be applied in financial services and contracts including various financial assets, for example derivatives, options, swaps, and bonds. The blockchains are also used to implement applications beyond the financial services industry and in more general-purpose industries such as government, health, media, the arts, and justice [3–7].

Blockchains are either permissionless or permissioned. Permis sionless are open-ended systems whereby any node can conduct transactions as well as take part in the consensus process to advance the network. They are publicly available therefore number of nodes are expected to be large, and these nodes are anonymous and untrusted since any node can join the network. Examples of

---
*Author for correspondence

permissionless blockchains are bitcoin and ethereum blockchains. Permissioned blockchains on the other hand are close-ended whereby transactions are can be done by any node but the process of advancing the network is restricted to a fixed set of peering nodes that are run by consortium members. Platforms like hyperledger fabric and multichain are aimed at consortiums where participation is close-ended [2], [8–10].

The performance of blockchain systems is defined by consensus algorithm being used. The consensus algorithm plays a very crucial role in maintaining the safety and efficiency of blockchain. Achieving consensus in a distributed system is challenging, consensus algorithms must be resilient to failures of nodes, partitioning of the network, message delays, messages reaching out-of-order and corrupted messages. They also must deal with selfish and deliberately malicious nodes. For a blockchain network, achieving consensus ensures that all nodes in the network agree upon a consistent global state of the blockchain [1, 11–13].
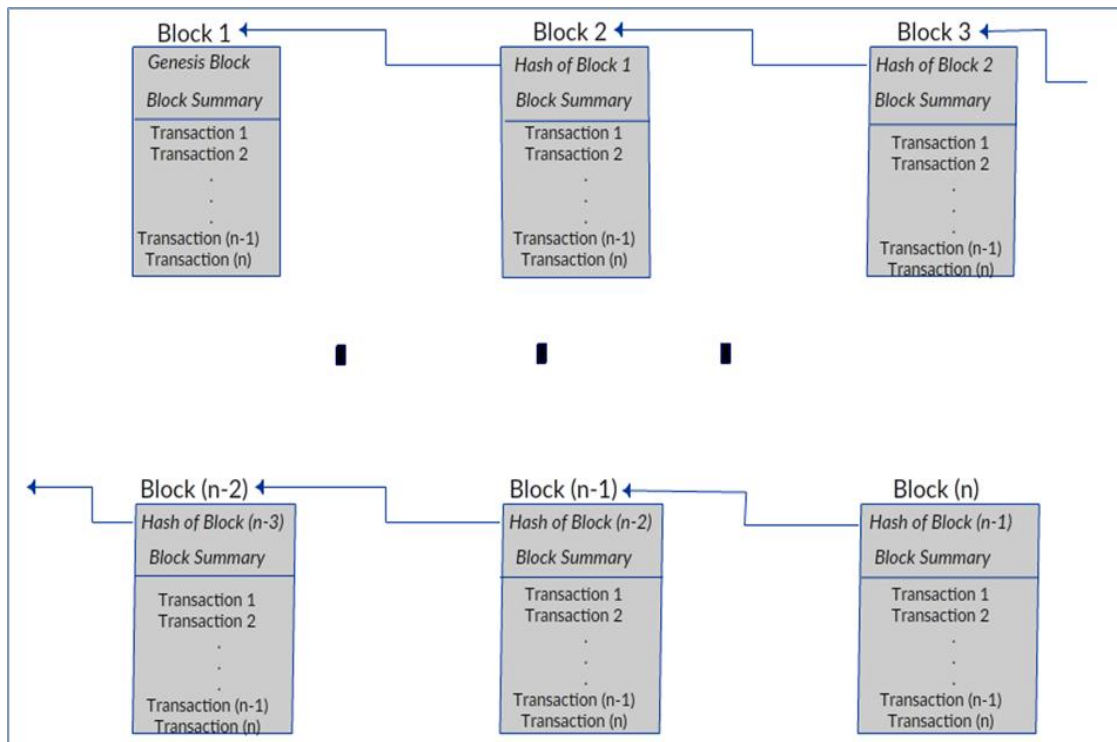
Figure 1 Blockchain concept

Permissionless blockchain consensus algorithms such as proof-of-work, proof of stake and delegated proof of stake support open-ended participation but have issues in reaching low latencies, immediate transaction finality, high performance and good scalability. Permissioned platforms on other side have semi-trusted members where only known participating nodes that are part of a consortium, are verified and registered. Number of these members is small therefore, it is easy to employ alternative consensus algorithms than in permissionless blockchain[13–15].

Consensus algorithms such as byzantine fault tolerance, SIEVE and cross-fault tolerance are fast, use low computation power but cannot have any open-ended participation. To address these limitations, several algorithms have been proposed in the literature and others are in test networks i.e. lightning network and sharding protocols, with each algorithm making the required set of assumptions in terms of synchrony, message broadcasts, failures, malicious nodes, performance and security of the messages exchanged. *Table 1* shows the summary of blockchain consensus algorithms with their individual characteristics [16–19].

Most of the blockchain systems run Turing complete programs known as smart contracts that encapsulate business logic to be executed when certain conditions

are satisfied. Once a smart contract program is deployed, it cannot be changed. So, unlike other software programs, the only way a smart contract can be modified is by deploying a new instance [2, 20–24].

Nevertheless, in the blockchain systems, valuable assets known as tokens or digital coins can also be implemented. Blockchain application's token is a smart contract that contains software code defining the token's functionality and a list of addresses (users) assigning ownership. So, a token is an artificial construct designed to give representation of ownership. The token can represent any fungible good or service on a blockchain. In addition, a token can be used as a reward or incentive, financial instrument, or a voting mechanism [25–27].

This paper focuses on evaluating the performance of different implementations of blockchain applications on healthcare sector. The rest of the paper is structured as follow: Section 2 introduces an overview of blockchain based technologies and system for healthcare. In section 3 this research presents performance evaluation along with metrics selected for evaluation. Section 4 presents the findings of the study, and section 5 discusses and analyses the findings. And lastly, section 6 concludes the paper and recommends the future work.

Table 1 Blockchain consensus algorithms and their characteristics

Algorithm	Hash Power	Number of nodes	Identification of new nodes	Transaction verification speed
Proof of work	Yes	Large	Public	Slow
Proof of stake	Yes	Large	Public	Slow
Delegated proof of stake	Yes	Low	Private	Fast
Proof of elapsed time	Yes	Low	Private	Fast
Deposit-based consensus	Yes	Large	Public	Fast
Proof of importance	Yes	Low	Private	Fast
Byzantine fault tolerance	No	Low	Private	Fast
Federated Byzantine agreement	No	Low	Private	Fast
Hybrid proof of work and proof of stake	Yes	Large	Public	Slow
Proof of DDoS	Yes	Large	Public	Slow

2.Blockchain technologies for healthcare information systems

The healthcare is a field that requires more efficient and secure system for managing medical records, pre-authorizing payments, settling insurance claims, and performing and recording more complex transactions. The blockchain technology provides solutions to those problems. The electronic medical records are currently kept in data centers and access is limited to hospital and care provider networks. Centralization of such information makes it vulnerable to security breach and can be expensive to maintain [28]. To eliminate that, blockchain stores the complete medical history for each patient, with multiple granularities of control by the patient, doctors, regulators, hospitals, insurers, and among others, providing a secure mechanism to record and maintain a comprehensive medical history for each patient. These ensures tamper-resistant means of storing medical history; reduced time in resolution of insurance claims and increased efficiency in providing insurance quotes; and complete medical history of the patient for use by physicians for precise drug recommendations[28–30].

2.1Blockchain healthcare information systems
Blockchain technology has already been applied to many different aspects in the healthcare domain for validating patient data, managing electronic health records (EHRs), tracking research methods to manufacture safer drugs, among others. For example, in ensuring proper interoperability, integrity, and privacy of patients' information, Guardtime and Estonian e-Health authority are working together in implementing blockchain technology nationwide. Additionally, the aim of implementing the technology is to ensure transparency, auditability and most importantly proper governance and management of patient information [5, 31, 32]. However, prescrypt under SNS bank N.V and Deloitte is making a system that makes it easier for patients to get prescriptions that are securely stored in blockchain. The system provides patients with full ownership of their medical records, allowing them to revoke and grant provider access to their personal data. *Table 2* shows summary of some of the currently available healthcare systems in blockchain ecosystem [32, 33, 34–41, 42–50].

Table 2 Healthcare information systems in blockchain technology

Blockchain System	Type of blockchain	Blockchain platform	Smart contract execution	Token usage	Application
MedRec	Public	Ethereum	Yes	No	Medical data management
MediLedger	Consortium/ Private	Ethereum Parity	Yes	No	Pharmaceutical supply chain
SimplyVital Health	Consortium	Health Nexus	Yes	Yes	Electronic healthcare records
Robomed Network	Public	Ethereum	Yes	Yes	Electronic healthcare records
Healthureum	Public	Ethereum	Yes	Yes	Healthcare management
Gem	All	All	No	No	Patient data
DokChain	Consortium	Hyperledger Sawtooth	Yes	Yes	Financial and clinical data
MediBloc	Public	QTum	Yes	Yes	Healthcare data platform
BlockMedx	Public	Ethereum	Yes	Yes	Doctor prescription
Patientory	Public	Ethereum	Yes	Yes	Electronic healthcare records
MedicalChain	Consortium	Hyperledger Fabric, Ethereum (for token)	Yes	Yes	Electronic healthcare records

3. Performance evaluation for blockchain based healthcare systems

3.1 Metrics for performance evaluation

The evaluation process was performed based on experiment done using performance monitoring framework for blockchain systems [51]. Metrics considered are transactions per second (TPS), transactions per network data (TPND), transactions per memory second (TPMS), transactions per CPU (TPC), and transactions per disk I/O (TPDIO) as shown in *Figure 2*. These metrics were chosen because measurements of data usage and resources consumption can be determined and compared for different systems.

3.1.1 Transactions per second (TPS)

TPS is a measurement of throughput in a period of time which represents the number of transactions completed in a second by a blockchain system. We take period of time from t_a to t_b as time spent by blockchain system to perform certain number of transactions (Txs). So, TPS of node (n) in a system determined by the following formula:

$$TPS_n = \frac{Count(Txs\ from(t_a, t_b))}{t_b - t_a} (Txs/s) \qquad (1)$$

Therefore, the average *TPS* for number (N) of nodes is:

$$\overline{TPS} = \frac{\sum_n TPS_n}{N} (Txs/s) \qquad (2)$$

3.1.2 Transactions per network data (TPND)

TPND is a measurement of network flow consumption in a period of time when blockchain systems share the state of blocks through transfer of data between the nodes by using consensus protocol. This process ensures each node in the system is in the same state.

To calculate *TPND* in the network, we take a session from time t_a to time t_b as time taken in a blockchain network to consume certain amount of network flow for certain number of transactions (Txs) in kilobytes (kb). *TPND* of a node (n) in a network can be determined by the following formula:

$$TPND_n = \frac{Count(Txs\ from(t_a, t_b))}{\int_{t_a}^{t_b} UPLOAD(t) + DOWNLOAD(t)} (Txs/kb) \qquad (3)$$

Where UPLOAD(t) is the size of upstream to the network at time t and DOWLOAD(t) is the size of downstream at time (t). The averages of TPND for all the nodes connected to the network were determined by the following formula:

$$\overline{TPND} = \frac{\sum_n TPND_n}{N} (Txs/kb) \qquad (4)$$

3.1.3 Transactions per memory second (TPMS)

TPMS is a measurement to represent the utilization of physical and its corresponding virtual memory for transactions of a blockchain based programs for a certain period of time. To calculate *TPMS* of a node (n) connected to a blockchain network from time t_a to

time t_b with execution of certain number of transactions (Txs), the following formula were used:

$$TPMS_n = \frac{Count(Txs\ from(t_a,t_b))}{\int_{t_a}^{t_b} PMEM(t)+VMEM(t)} (Txs/(MB.s)) \quad (5)$$

Where $PMEM(t)$ is a physical memory occupied by a blockchain program from time t_a to time t_b and $VMEM(t)$ is its corresponding virtual memory in the same time. The average $TPMS$ for entire network is calculate by the following equation:

$$\overline{TPMS} = \frac{\sum_n TPMS_n}{N} (Txs/(MB.s)) \quad (6)$$

3.1.4 Transactions per CPU (TPC)

TPC is a measurement which represent metric to monitor CPU usage during executions of smart contracts in blockchain network. TPC differ from one application to another depending on encryption algorithms, hash computations and consensus protocols utilized. Equation (7) shows formula to calculate TPC of node n from time t_a to t_b:

$$TPC_n = \frac{Count(Txs\ from(t_a,t_b))}{\int_{t_a}^{t_b} F*CPU(t)} (Txs/(GHz.s)) \quad (7)$$

Where F is frequency of single CPU core and CPU(t) is a CPU usage of a blockchain application from t_a to

t_b. The average TPC for entire blockchain network with nodes N is:

$$\overline{TPC} = \frac{\sum_n TPC_n}{N} (Txs/(GHz.s)) \quad (8)$$

3.1.5 Transactions per disk I/O (TPDIO)

TPDIO is a metric to measure the utilization of read and write to the secondary storage during execution of blockchain applications such as contracts executions and block commits in a specific period of time. The formula for calculating TPDIO for a node n connected to the blockchain network is as follow:

$$TPDIO_n = \frac{Count(Txs\ from\ (t_a,t_b))}{\int_{t_a}^{t_b} DISKR(t)+DISKW(t)} (Txs/kb) \quad (9)$$

Where t_a and t_b are the time to start and finish program execution respectively, $DISKR(t)$ and $DISKW(t)$ are the amount of data read from storage and data written to the same storage respectively from time (t_a) to time (t_b). The average of TPDIO for whole network with number of nodes (N) is:

$$\overline{TPDIO} = \frac{\sum_n TPDIO_n}{N} (Txs/kb) \quad (10)$$
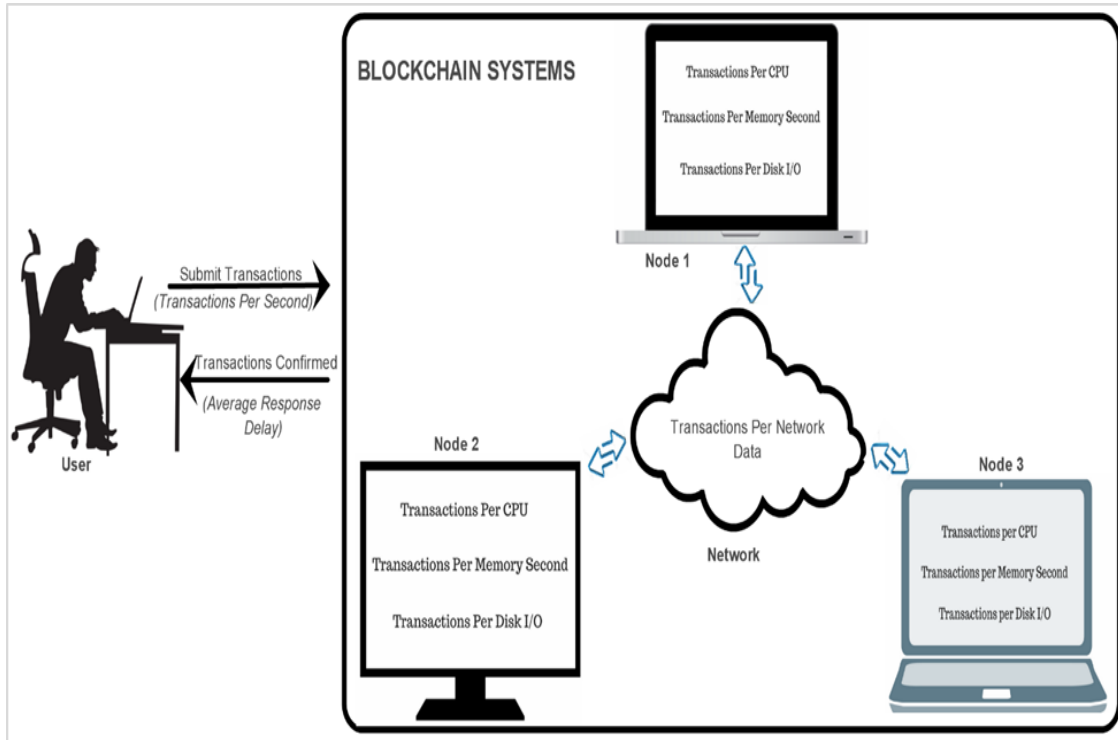
Figure 2 Metrics for evaluating blockchain systems

4.Evaluation results

The evaluation was done based on performance experiment conducted on Ethereum[52], Parity[53], and Hyperledger Fabric[54] blockchain platforms. The experiment was based on 1000 smart contracts using nodes with Intel Core i7-4790 3.60GHz CPU and 8GB of RAM [51]. The blockchain based healthcare systems evaluated were selected based on their popularity, type of blockchain they belong, and their overall functions. These systems are patientory [37] which runs on public ethereum platform [42], MediLedger [36] running on private parity platform [35], and MedicalChain[34] running on consortium hyperledger fabric platform[48].

Data in smart contracts stored in ledgers consist of world state (information stored in key-value databases) and blockchain state (the history of all transaction in root form i.e. markle patricia tree for ethereum and parity platforms and bucket tree for hyperledger fabric platform). The transactions assessed in the following processes; 1) user submitting data/input to the system from his/her node, 2) the process of checking the validity of entered data from other nodes in the network, 3) the execution process done with smart contract code, 4) the process of propagating and comparing results, and 5) updating the world state and the state of the blockchain.

From the analysis of evaluation, *Figure 3* shows the comparison of transactions executed by three systems (patientory, MediLedger, and MedicalChain) per unit second. The results indicated that MedicalChain system developed in consortium-based platform (hyperledger fabric) perform more transactions per second compared with other two systems (patientory and MediLedger).

Furthermore, *Figure 4* shows the transactions executed to utilize 1 kilobyte of network flow of data in one second. These results indicated that Ethereum based system patientory consumes half a bandwidth spent by a hyperledger based system MedicalChain. On other hand, parity based system MediLedger use twice as much as bandwidth of MedicalChain and four times bandwidth of patientory.
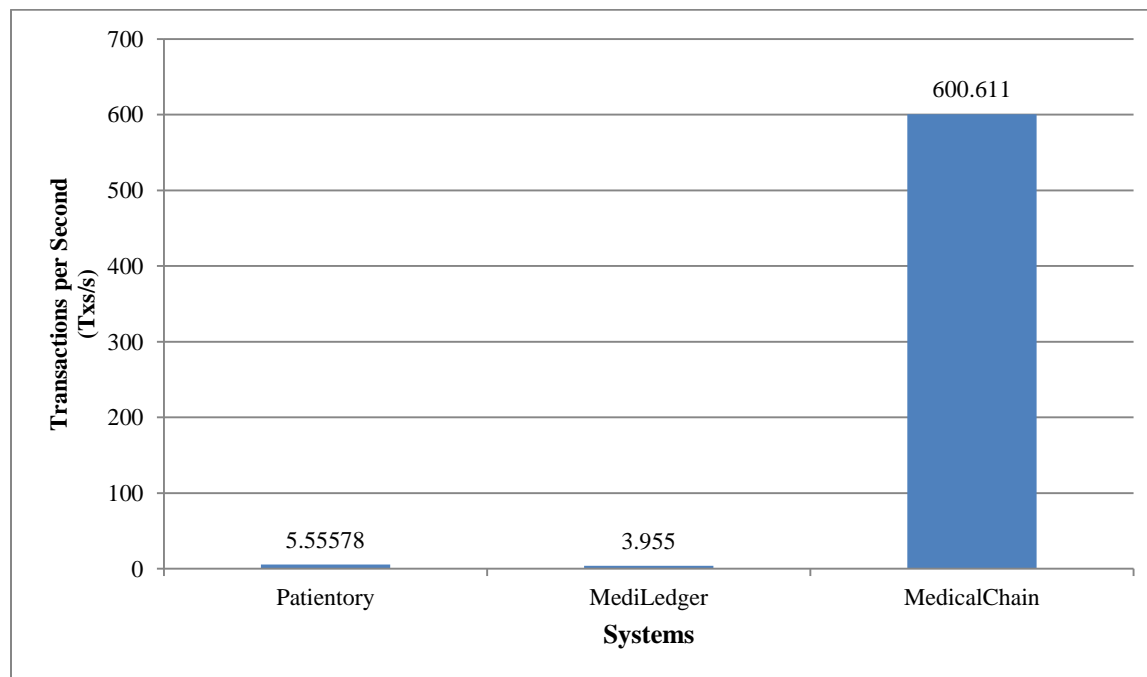

Figure 3 Average transactions executed on each second
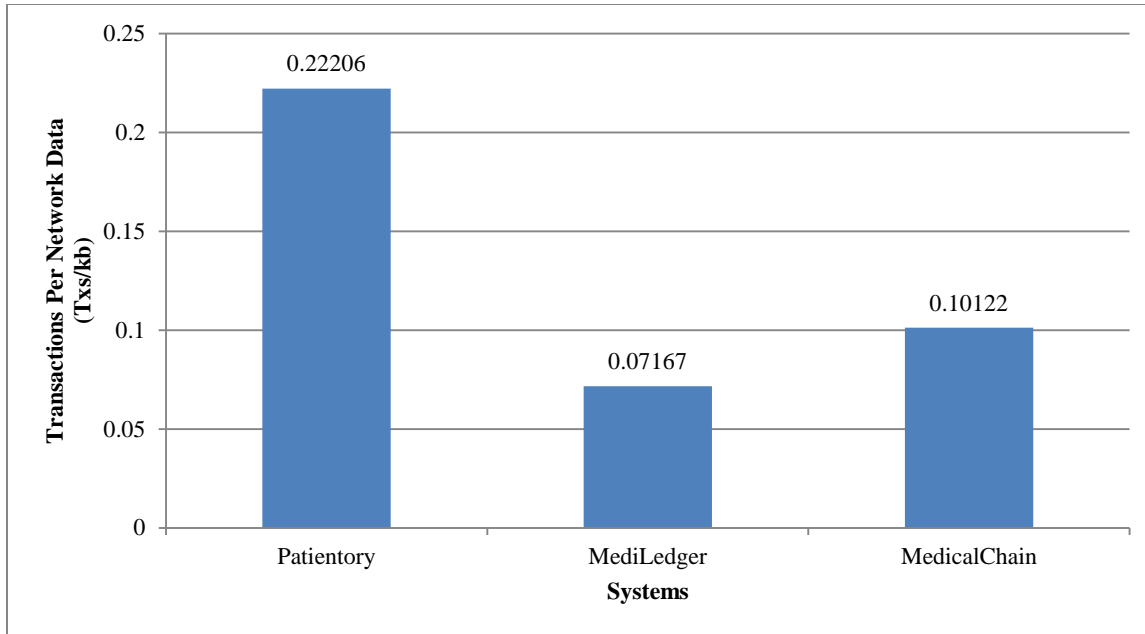
Figure 4 Number of transactions which consume one kilobyte of blockchain network data

However, *Figure 5* shows the number of transactions healthcare systems usage to utilize 1 megabytes of node's memory per unit time. The results indicated that hyperledger based system MedicalChain use over 4 transactions per 1 megabyte second of node's memory. In addition, other systems i.e. Patientory and MediLedger used 6.8% and 1.06% of a single transaction respectively to consume 1 Megabytes Second of node's memory.

Additionally, *Figure 6* shows number of transactions healthcare systems used to consume 1 gigahertz of a node's single CPU core per unit time. The results indicate that hyperledger based system MedicalChain perform better than other two systems with 2.6 transactions per 1 gigahertz second of node's CPU. Other two systems i.e. patientory and MediLedger used 1.9% and 1.4% of 1 transaction to consume 1 gigahertz second of a node's CPU.
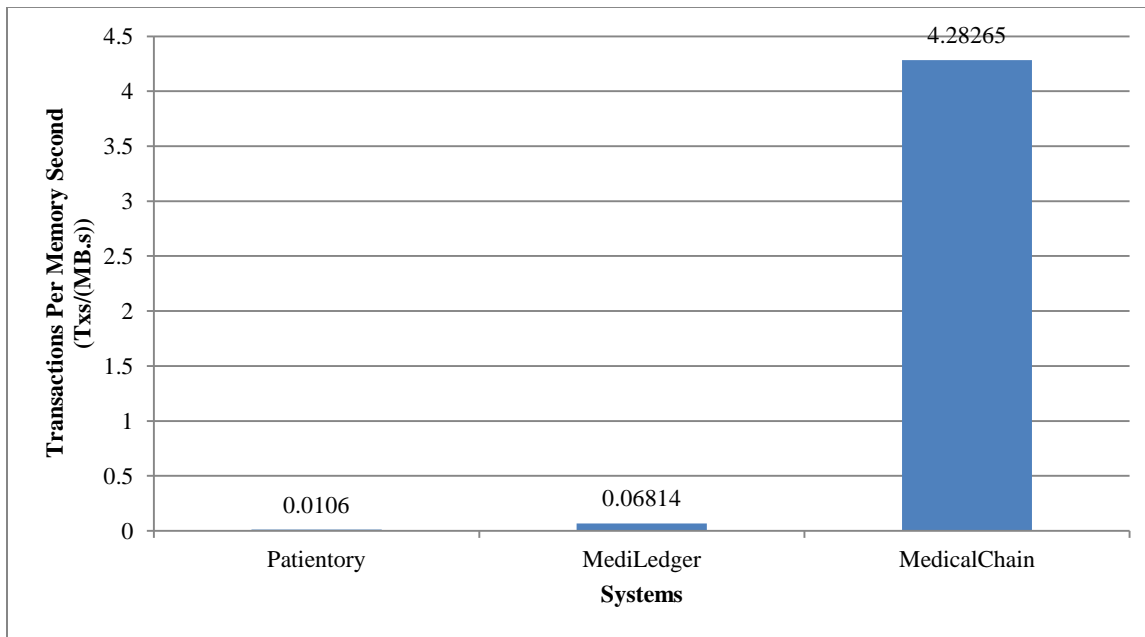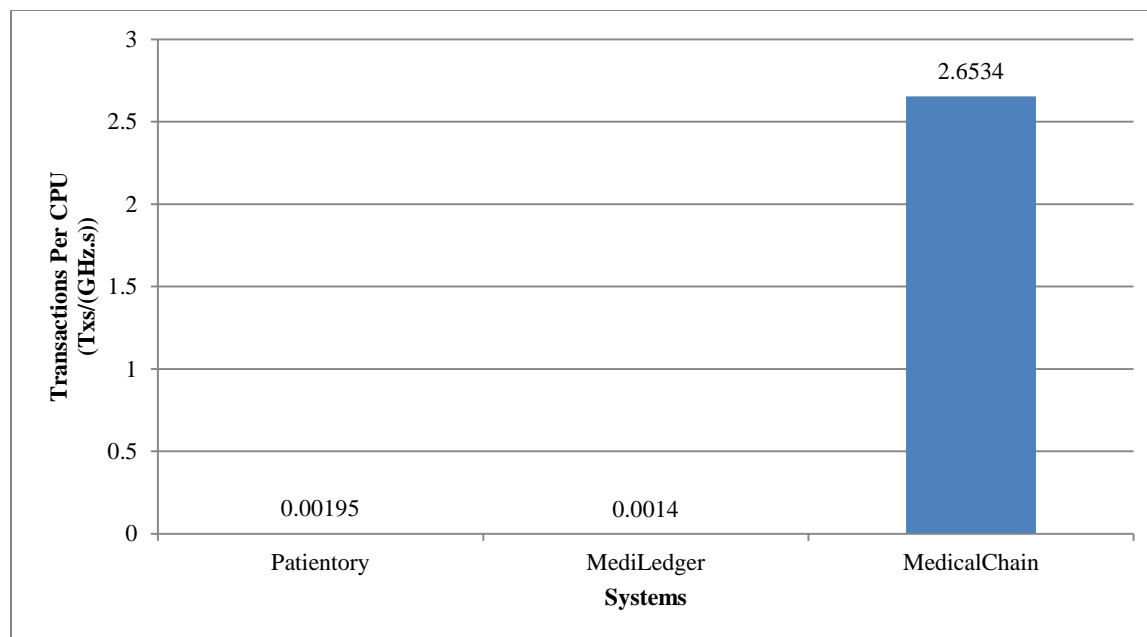

Figure 5 Transactions of blockchain system which utilize one megabytes of node's memory per second

Finally, *Figure 7* shows number of transactions used by healthcare system to read and write 1 megabytes of data per unit time from/to a node's disk storage. Results indicated that ethereum based system patientory read and write more transactions per 1 megabyte second than other two systems. It read and write 26.57% of 1 transaction per 1 megabyte second.

Hyperledger based system MedicalChain have read and write 13.81% of 1 transaction per 1 megabyte second. The parity-based system MediLedger have the lowest metrics of read and write of 0.26% of 1 transaction per 1 megabyte second.

Figure 6 Transactions performed by the blockchain system in a CPU cycles per second
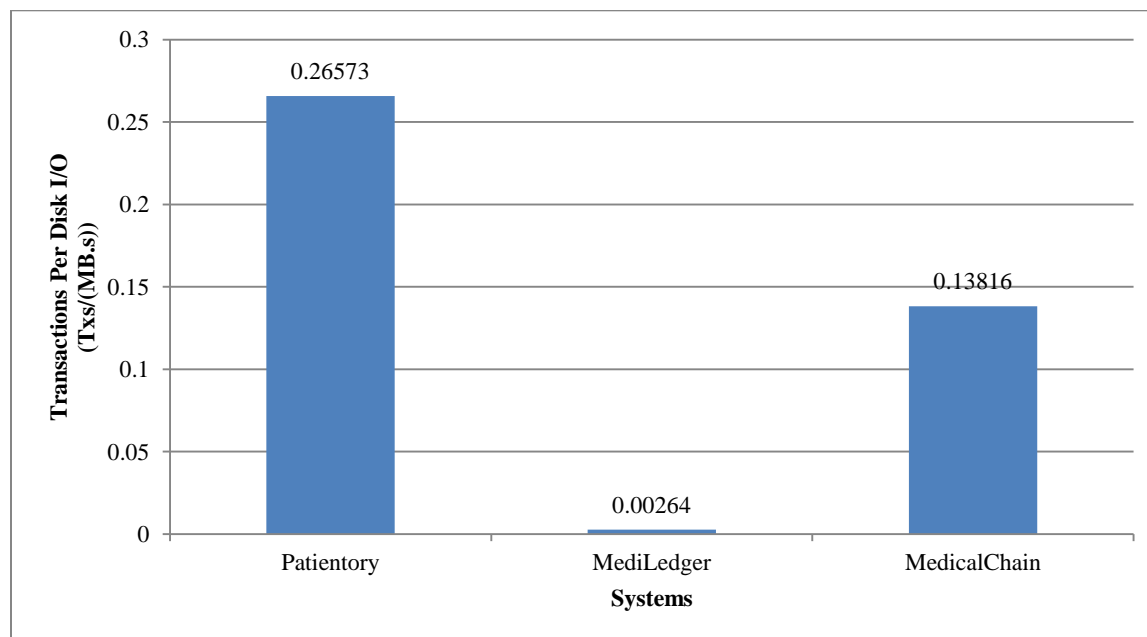
Figure 7 Transactions executed to consume one megabyte of storage reads and writes per second

5.Discussion and analysis

Results in this study indicated that hyperledger based system MedicalChain exceeds systems from parity and ethereum platforms (patientory and MediLedger) in executing more transactions per unit time, utilizing RAM by performing more transactions per 1 megabyte of memory, and executing more transactions per one cycle of CPU. Similarly, Dinh et al. [55] study reveals that hyperledger fabric applications outperforms ethereum and parity despite of using different evaluation metrics like fault tolerance. Nevertheless, other study [56] shows that hyperledger fabric achieves higher throughput and lower latency compared to ethereum platform. Consistently, these studies [57–59] indicate overall performance of hyperledger fabric smart contracts outshines other platforms smart contracts (parity and ethereum). Additionally, some studies [10, 50−60] suggest that for security purposes, confidentiality and privacy, permissioned blockchains (hyperledger) are more secure than permissionless blockchain (ethereum).

However, despite of overall good performance of hyperledger based application, this study revealed that ethereum based application has quicker read and write to and from hard disk, and it consumes little network data than hyperledger fabric and parity-based application. This imply that hyperledger-based applications fit better in the environment which require high security measures, connected with average computational devices due its ability of consuming low memory and low computational power. But in environment where writing and reading to/from a storage devices or overall usage of network bandwidth is priority then ethereum-based application performs better.

6.Conclusion and future work

Blockchain based systems still lag behind the centralized storage systems like relational databases by performing fewer transactions per unit time. But on other hand, these systems have advantage of providing more robust and fault tolerance way of storing critical information. To reap the benefits of this technology it is very important for healthcare organizations to perform a research of different platforms, frameworks and implementation approaches of this technology. This study evaluates the performance on blockchain based healthcare systems from public, private/consortium architectures; both from permissioned and permissionless platforms. The findings of the study indicated that the consortium-based platform have

overall better performance than private and public blockchains. Unlike other studies on evaluating performance of blockchain platforms, this study focused on healthcare-based applications. It is envisaged that decision makers, healthcare organizations, and other researchers will make use of the findings in this work in selection of proper platform for healthcare systems implementation based on features they lack. In future, different requirements of blockchain implementation will be assessed for healthcare systems in the developing countries.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Laurence T. Blockchain for dummies. John Wiley & Sons; 2017.
[2] Bambara JJ, Allen PR, Iyer K, Lederer S, Madsen R, Wuehler M. Blockchain: a practical guide to developing business, law, and technology solutions. McGraw Hill Professional; 2018.
[3] Bashir I. Mastering Blockchain. Packt Publishing Ltd; 2017.
[4] Hofmann E, Strewe UM, Bosia N. Supply chain finance and blockchain technology: the case of reverse securitisation. Springer; 2017.
[5] Randall D, Goel P, Abujamra R. Blockchain applications and use cases in health information technology. Journal of Health & Medical Informatics. 2017; 8(3):1-4.
[6] Alketbi A, Nasir Q, Talib MA. Blockchain for government services-use cases, security benefits and challenges. In learning and technology conference 2018 (pp. 112-9). IEEE.
[7] Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. Advances in Computers. 2018; 111:1-41.
[8] Peters GW, Panayi E. Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. In banking beyond banks and money 2016 (pp. 239-78). Springer, Cham.
[9] Sousa J, Bessani A, Vukolic M. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In annual IEEE/IFIP international conference on dependable systems and networks 2018 (pp. 51-8). IEEE.
[10] English E, Kim AD, Nonaka M. Advancing blockchain cybersecurity: technical and policy considerations for the financial services industry. Cybersecurity Policy and Resilience. 2018.
[11] Milutinovic M, He W, Wu H, Kanwal M. Proof of luck: an efficient blockchain consensus protocol. In

481

proceedings of the workshop on system software for trusted execution 2016 (p. 2). ACM.

[12] Zheng Z, Xie S, Dai HN, Wang H. Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services. 2016; 14(4):352-75.

[13] Baliga A. Understanding blockchain consensus models. Persistent. 2017.

[14] Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, et al. On scaling decentralized blockchains. In international conference on financial cryptography and data security 2016 (pp. 106-25). Springer, Berlin, Heidelberg.

[15] Mingxiao D, Xiaofeng M, Zhe Z, Xiangwei W, Qijun C. A review on consensus algorithm of blockchain. In international conference on systems, man, and cybernetics 2017 (pp. 2567-72). IEEE.

[16] Poon J, Dryja T. The bitcoin lightning network: scalable off-chain instant payments. 2016.

[17] Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In proceedings of the ACM SIGSAC conference on computer and communications security 2016 (pp. 17-30). ACM.

[18] Wang S, Vergne JP, Hsieh YY. The internal and external governance of blockchain-based organizations: evidence from cryptocurrencies. In bitcoin and beyond 2017.

[19] Sikorski JJ, Haughton J, Kraft M. Blockchain technology in the chemical industry: machine-to-machine electricity market. Applied Energy. 2017; 195:234-46.

[20] Cong LW, He Z. Blockchain disruption and smart contracts. National Bureau of Economic Research; 2018.

[21] Luu L, Chu DH, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. In proceedings of the ACM SIGSAC conference on computer and communications security 2016 (pp. 254-69). ACM.

[22] Idelberger F, Governatori G, Riveret R, Sartor G. Evaluation of logic-based smart contracts for blockchain systems. In international symposium on rules and rule markup languages for the semantic web 2016 (pp. 167-83). Springer, Cham.

[23] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In symposium on security and privacy 2016 (pp. 839-58). IEEE.

[24] Antonopoulos AM, Wood G. Mastering ethereum: building smart contracts and dapps. O'reilly Media; 2018.

[25] Conley JP. Blockchain and the economics of crypto-tokens and initial coin offerings. Vanderbilt University, Department of Economics; 2017.

[26] Rohr J, Wright A. Blockchain-based token sales, initial coin offerings, and the democratization of public capital markets. University of Tennessee Legal Studies Research. 2017.

[27] Cong LW, Li Y, Wang N. Tokenomics: dynamic adoption and valuation. Second emerging trends in entrepreneurial finance conference 2018. SSRN

[28] Gropper A. Powering the physician-patient relationship with HIE of one blockchain health IT. In ONC/NIST use of blockchain for healthcare and research workshop. Gaithersburg, Maryland, United States: ONC/NIST 2016.

[29] Gupta M. Blockchain for dummies. IBM Limited Edition, US. 2017.

[30] Samuel RE. A layered architectural approach to understanding distributed cryptographic ledgers. Issues in Information Systems. 2016; 17(4):222-6.

[31] Kho W. Blockchain revolution in healthcare: the era of patient-centered dental information system. International Journal of Oral Biology. 2018; 43(1):1-3.

[32] Engelhardt MA. Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review. 2017; 7(10):22-34.

[33] Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. Trials. 2017; 18(335):1-5.

[34] SA Medicalchain. https://medicalchain.com/en/. Accessed 18 September 2018.

[35] https://uploads-ssl.webflow.com/59f37d05831e8500 0160b9b4/5aaadbf85eb6cd21e9f0a73b_MediLedger% 202017%20Progress%20Report.pdf. Accessed 18 September 2018.

[36] https://www.mediledger.com/network. Accessed 18 September 2018.

[37] https://patientory.com/. Accessed 18 September 2018.

[38] Dias JP, Reis L, Ferreira HS, Martins Â. Blockchain for access control in e-health scenarios. arXiv preprint arXiv:1805.12267. 2018.

[39] Hobbs BP, Carlin BP, Sargent DJ. Adaptive adjustment of the randomization ratio using historical control data. Clinical Trials. 2013; 10(3):430-40.

[40] https://robomed.io/. Accessed 18 September 2018.

[41] https://en.healthnexus.ca/. Accessed 18 September 2018.

[42] McFarlane C, Beer M, Brown J, Prendergast N. Patientory: a healthcare peer-to-peer EMR storage network v1.1. 2017:1-19.

[43] Wang S, Wang J, Wang X, Qiu T, Yuan Y, Ouyang L, et al. Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Transactions on Computational Social Systems. 2018; 5(4):942-50.

[44] https://enterprise.gem.co/wp-content/uploads/2016/10/GemOSPlatformWhitepaper. pdf. Accessed 18 September 2018.

[45] Prisco G. The blockchain for healthcare: gem launches gem health network with Philips blockchain lab. Bitcoin Magazine. 2016.

[46] Shieber J. Gem looks to CDC and European giant tieto to take blockchain into healthcare. TechCrunch.2017.

[47] Dhillon V, Metcalf D, Hooper M. Behold the Dreamers. In blockchain enabled applications 2017 (pp. 1-5). Apress, Berkeley, CA.

[48] https://medicalchain.com/en/whitepaper/. Accessed 18 September 2018.

[49] Da Conceição AF, Da Silva FS, Rocha V, Locoro A, Barguil JM. Eletronic health records using blockchain technology. arXiv preprint arXiv:1804.10078. 2018.

[50] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In proceedings of the eurosys conference 2018. ACM.

[51] Zheng P, Zheng Z, Luo X, Chen X, Liu X. A detailed and real-time performance monitoring framework for blockchain systems. In proceedings of the international conference on software engineering: software engineering in practice 2018 (pp. 134-43). ACM.

[52] https://www.ethereum.org/. Accessed 18 September 2018.

[53] https://www.parity.io/. Accessed 18 September 2018.

[54] https://www.hyperledger.org/projects/fabric. Accessed 18 September 2018.

[55] Dinh TT, Wang J, Chen G, Liu R, Ooi BC, Tan KL. Blockbench: a framework for analyzing private blockchains. In proceedings of the international conference on management of data 2017 (pp. 1085-100). ACM.

[56] Pongnumkul S, Siripanpornchana C, Thajchayapong S. Performance analysis of private blockchain platforms in varying workloads. In international conference on computer communication and networks 2017 (pp. 1-6). IEEE.

[57] Baliga A, Subhod I, Kamat P, Chatterjee S. Performance evaluation of the quorum blockchain platform. arXiv preprint arXiv:1809.03421. 2018.

[58] Nasir Q, Qasse IA, Abu Talib M, Nassif AB. Performance analysis of hyperledger fabric platforms. Security and Communication Networks. 2018.

[59] Thakkar P, Nathan S, Vishwanathan B. Performance benchmarking and optimizing hyperledger fabric blockchain platform. arXiv preprint arXiv:1805.11390. 2018.

[60] Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT challenges and opportunities. Future Generation Computer Systems. 2018; 88:173-90.

Cleverence Kombe is currently a PhD scholar in Information and Communication Science and Engineering (ICSE) at School of Computational and Communication Sciences and Engineering (CoCSE) from Nelson Mandela African Institute of Science and Technology (NM-AIST). He received his B.Sc. in Computer and Information Security and M.Sc. in Computer Science from College of Informatics and Virtual Education (CIVE) at University of Dodoma (UDOM) in Tanzania in 2013 and 2016 respectively. His research interest includes Blockchain Technology, Cyber Security, and Artificial Inteligence.
Email: clevernce@gmail.com

Mussa Ally Dida is a lecturer at Nelson Mandela African Institute of Science and Technology (NM-AIST) and an academic manager of Centre of Excellence for ICT in East Africa (CENIT@EA). He has previously been an Assistant Lecturer at NM-AIST from April 2012 to June 2017. He received his PhD in Communication Engineering at Beijing Institute of Technology in June 2017, Masters of Science in Telecommunication Engineering at University of Dodoma in 2011 and Bachelor of Science in Computer engineering and Information Technology from the University of Dar es Salaam in 2008. His research interests include Tanzania Digital Signal Processing, Physical Layer Security, ICT4D and Embedded System for Agriculture.

Anael E. Sam is a senior lecturer at the School of Computation Communication Science and Engineering (CoCSE) at NM-AIST. He earned his PhD in Electronics Engineering from the Faculty of Electrical Engineering and Information Technology at Slovak University of Technology, Slovak Republic. Previously, he held the position of Senior System Test Engineer for Nokia Siemens Networks R&D department (2010- 2012). He also worked as System Test Engineer in R&D of Logica Slovakia s.r.o. a subsidiary of Logica Plc. (2007-2010). He worked for Siemens Program and System Engineering (PSE) s.r.o. Slovakia (2004 – 2007). Also he worked as Software Expert for Alcatel Lucent, Slovakia (2000-2003). His research interests are: Radio, Multimedia, Mobile and Wireless Communication Systems; Electronics and Telecommunication Engineering, Software Quality Assurance Engineering; Mobile Networks Planning and Optimization. He is author and co-author of more than 35 scientific publications