

Comparative Study of Permissioned Blockchain Platform for Interoperability and Access Control of Electronic Health Record

Mrs. Pranalini Joshi¹ and Dr. Pratibha Mahajan²

¹⁻²Department of Computer Engineering Vishwakarma University Pune, India
Email: Pranalini.joshi-317@vupune.ac.in, pratibha.mahajan@vupune.ac.in

Abstract— Healthcare is one of the promising domains, where Blockchain technology can be used. As healthcare data contains personal and sensitive information of individuals, security to healthcare data has prime importance. Healthcare data breaches not only affect financial loss to medical institutions but also disturb the health of patients. The use of Blockchain technology can help to overcome this problem by providing security, efficiency, and authenticity to transactions. One of the major challenges that medical institutions are attempting is to select suitable and standard Blockchain platform to make secure and transparent transactions among various stakeholders. This paper presents comparison of existing permissioned Blockchain platform based on various parameter.

Index Terms— Blockchain, Electronic Health Record, Corda, Quorum, Hyperledger Fabric

I. INTRODUCTION

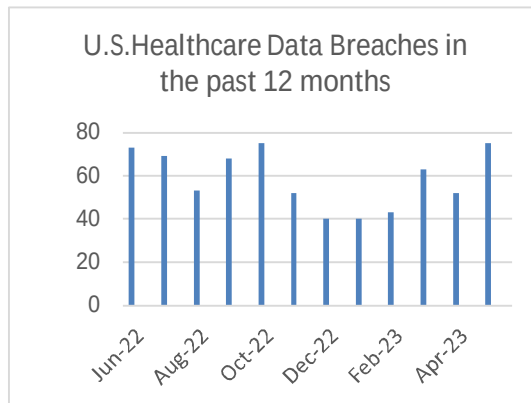
Electronic Health Record (EHR) is storing medical data and records of individual digitally, these records are collected from sensor data and electronic medical records (EMRs). As Healthcare is a data-intensive domain, large amounts of data is produced, stored, distributed, and accessed daily. For example, every time when patient goes to hospital, healthcare data gets created which can be by various stakeholders like doctors, caretakers etc. [1]

According to the survey done by Stanford Medicine [2], 153 Exabyte healthcare data were generated in 2013 and it was expected to reach 2314 Exabyte healthcare data in 2020. A survey reported that the healthcare analytics industries are growing at an exponential rate with a compound annual growth rate (CAGR) of 27.3% and this is anticipated to reach 29.84 billion USD by 2022 from 8.92 billion USD in 2017 [3]. Healthcare data contains personal and sensitive information that attract cyber criminals. Most common attack on Electronic Health Record (EHR) is ransomware attack. According to graph published by HIPPA [4] see Graph 1, average number of records breached every month is 6104761 and for every healthcare record which is breached, it costs around \$380 USD per second. There are various ways to breach healthcare data like hacking, theft, unauthorised access etc. Figure 1 [6] shows the different ways for healthcare data breaches.

In the healthcare industry, various stockholders are Patients, Doctors, Insurance Company and pathology laboratories and Governing bodies etc. EHR contains sensitive and private health information, as it is often used by various stakeholders for following actions confidentiality and integrity of healthcare data needs to be protected from external attackers as well as from illegal access attempts inside the network [1].

For example, Insurance companies require patients' data for analyzing it properly and provide the services, but it

is frequently seen that data gets manipulated by the companies and leaked [5]. Therefore, security of the Electronic Health Record (EHR) is a very important but crucial and challenging task. Hence, to preserve a definite trust between the various stakeholders, to defend the data from the misuse and to make Electronic Health Record (EHR) available for emergency on a common platform, a new system with seamless access, transaction, and storage management is needed. Due to limitations of centralised systems like scalability and reliability, Digital world is moving towards distributed technology and Blockchain is most secured, rapidly growing distributed system which can be used for interoperability and access control of Electronic Health Record. Many People consider Blockchain means public Blockchain or Bitcoin or cryptocurrency and can be used only for development of financial applications, but Blockchain can be private or permissioned and can be used for non-financial applications like healthcare domain.



Graph 1: Healthcare Data Breach in past 12 months [4]

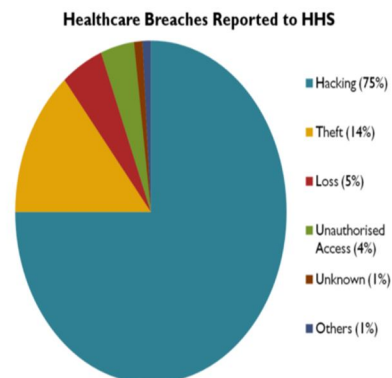


Figure.1: Different ways for Healthcare Breaches

A. *Permissioned Blockchain*

Permissioned Blockchain is closed network Blockchain where only designated parties can be involved and take part in consensus process. It is a fully decentralized network across known parties. It can be private or Consortium Blockchain. Private Blockchain is mainly designed for one organization and has centralized structure where a single entity has the full power to take decisions and validate the process. Whereas in Consortium blockchain, group of organizations can participate and only few nodes can take part in consensus process. Compared to permission-less Blockchain, Permissioned Blockchain consumes less energy, can be implemented easily and faster in nature. Figure 2. shows permissioned and permissionless blockchain details. As aim of this research theme is to handle access control and interoperability of electronic health record among various medical organization using Blockchain Technology, study of consortium Blockchain has been done and suitable platform is selected for implementation. During Survey, it is observed that Corda [8], Quorum [9], Fabric [10], Ripple [11] and Staller [12] are the popular permissioned Blockchain platforms. Out of these five permissioned Blockchain platform, Ripple and Staller deals for financial transaction only and hence not taken into consideration for comparison.

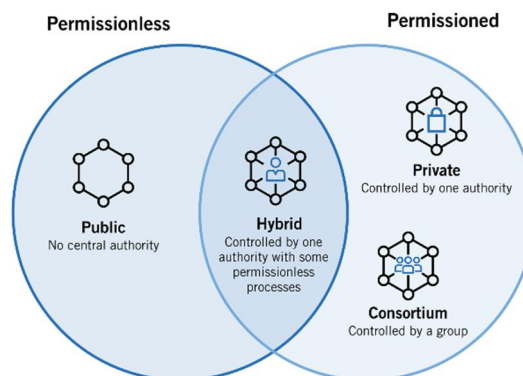


Figure 2: Types of Blockchain [21]

II. PARAMETERS ON BASIS OF WHICH COMPARISON OF BLOCKCHAIN PLATFORM HAVE BEEN DONE

This Section describes the parameters which are considered to compare existing popular Blockchain platforms i.e Quorum, Corda, and Hyperledger Fabric

A. Consensus

Validity of transactions and blocks are checked using a mechanism called consensus mechanism. Only valid transactions are added into block and only valid block is added into Blockchain. Consensus is one of the vital processes in Blockchain. Depending upon Blockchain Framework, consensus mechanism varies, hence it plays pivotal role in selection of Blockchain Network.

RAFT or IBFT are consensus mechanisms used in Quorum. RAFT and RBFT consensus mechanism are used by Corda. Hyperledger Fabric supports PBFT, KAFKA, RBFT, Sumeragi, and PoET consensus algorithms. In addition to this fabric also support plug and play consensus mechanism [23]

B. Modularity

Extent to which a software gets divided into smaller modules is referred as modularity. Modularity can specify the portability and future development of a product. It also supports the advance addition in the system, if required in future. As every business organisation wish to extend their business, it supports modularity. Modularity is considered in comparison as it predicts the extensibility of product.

C. Corda

Corda which is also known as R3 Corda is open source Blockchain platform developed by R3 Lab in 2017. It has two modules, Notary Pool, and Corda Node.

1. *Notary Pool*: It is Corda's consensus service. It ensures that every transaction has unique input state. Notary service is established by a notary cluster, notary cluster is a group of one or more notary workers.
2. *Corda Node*: One party in a business network represents corda node. This party operate node which has CorDapps installed on it which is used to interact with other nodes in a network. CorDapps define operations and interactions of business network [13]. Corda Node also maintains the ledger.

D. Quorum

Quorum is open source Blockchain platform developed by JPMorgan Chase in 2016. It has three Modules. Quorum node, transaction manager and enclave. [14]

1. *Quorum Node*: It maintains the ledger and use as interface to communicate with client and other nodes
2. *Transaction Manager*: Transaction Manager store and verify the transaction. It manages privacy of transaction and provide access to encrypted transaction, but it does not have access to any sensitive private keys.
3. *Enclave*: Enclave are used to perform cryptographic operations. All the private keys of transactions are sealed in Enclave. All encryption/decryption operations are done within the Enclave. Figure 3 shows basic Quorum architecture.

E. Hyperledger Fabric [12]

Hyperledger Fabric is an open source Blockchain framework, initiated by the Linux Foundation in 2015. It has the following five modules.

1. Membership service provider
2. Client
3. Endorsers
4. Ordering service nodes
5. Committers.[9]

1. A membership service provider

It preserves the permissioned nature of Fabric. It is a mechanism that provides cryptographic identities to peers. It allows identity to be trusted and recognized by the rest of the network.

2. Client

A member or member application which initiates the transaction is called client. It sends transactions to the peers specified by the endorsement policy.

3. Ordering Service Nodes (OSN /orderers)

These are the nodes that collectively form the ordering service. Sequences of transactions are maintained by ordering services.

4. Endorsers

Nodes that execute Chaincode and endorse transaction are called Endorsers. It also prevents double spent of transaction.

5. Committers

All the node in hyperledger do not maintain copy of ledger. Nodes which maintain a copy of ledger are called committers. After the consensus process OSNs send block to committer and Committer nodes add block to the Blockchain.



Figure 3: Basic Quorum architecture

C. Language Support

Language support indicates languages used to write smart contracts. Selected permissioned Blockchain framework are designed by three different companies and support different languages to write smart contract. Concept of smart contract was initially introduced in Ethereum Blockchain framework [16] and solidity is language used to write smart contract. However, there are handful of resources available which works on solidity. Proficient developers will be available for popular languages like Java, JavaScript and Python. Smart contracts in quorum are written using solidity. Smart contracts in Corda can be written using Kotlin or Java language and Chain code (means smart contracts) in Hyperledger Fabric can be written using GO, JavaScript, or Java language. As Chaincode in Fabric can be written using three languages maximum skilled developers can be available to work on Fabric platform Hence language support should also be taken into consideration while selecting suitable Blockchain Framework

D. Transaction Rate

Transaction rate means number of transactions executed per second. Transaction rate decides the speed of system. The higher the transaction rate, the faster the system which in turn will attract organizations to adopt the framework. Hence transaction rates are also taken into consideration while comparing Blockchain framework. In Quorum, the Transaction rate varies between dozens to hundreds of transactions per second depending on configuration. Corda measures between 15 and 1678 transactions per second. Hyperledger fabrics do 3500 transactions per second [15] which indicates that Hyperledger fabric is faster than Quorum and Corda.

E. Cryptocurrency [18]

Currency used to validate transaction is one major filter to differentiate the platforms, different platforms support different cryptocurrency, but some platforms do not require any cryptocurrency module. As Quorum is built on Ethereum, it uses Ether as cryptocurrency, Hyperledger Fabric does not use any cryptocurrency and Corda uses traditional Fiat Money.

F. Security and Privacy

Private key is used to sign every transaction and gets verified with its public key. Every Block in Blockchain is encrypted with cryptographic hash function, so no one can read data without knowing hash value [23]. Zero knowledge proof (ZKP) technique is used by Hyperledger Fabric and Quorum to hide data from unauthorized users. Corda uses hardware security model for providing security and privacy to data [18]

G. Test Network [17]

Developers do not deploy code unless testing of code has been done. Test network is a Blockchain where working of applications can be tested. Test network can be public test network or private test network. Corda has a public test network whereas Hyperledger Fabric has a private test network. For using private test network, Developer needs to create their own set up for testing.

Table 1 shows comparison of permissioned Blockchain platforms based on parameter discussed above.

TABLE I: COMPARISON OF PERMISSIONED BLOCKCHAIN PLATFORM

Sr. No	Property	Quorum [9]	Corda [8]	Hyperledger Fabric [10]
1	Governance	JPMorgan	R3 Labs	Linux Foundation
2	Consensus	RAFT or IBFT	RAFT and RBFT	PBFT, KAFKA, RBFT, Sumeragi, and PoET
3	Modularity	3 Modules 1.Quorum Node 2.Transaction Manager 3.Enclave	2 Modules 1.Notary Pool 2.Corda Node	5 Modules 1.MSP 2.OSN 3. Client 4. Endorsers 5. Committers
4	Language Support	Solidity	Kotlin, Java	JavaScript, GO, JAVA
5	Transaction Rate	dozens to hundreds of transactions per second depending on configuration. (Had slow transactions [15])	Corda measures between 15 and 1678 TPS (Much faster transactions than quorum [15])	3500 TPS (Fastest Transaction [15])
6	Currency	Ether	Fiat money	None
7	Test Network	No	Public	Private

III. CONCLUSION

This Paper has discussed why Blockchain technology is necessary to execute healthcare applications and then presented a comparison of three Permissioned Blockchain platforms. This comparison is done based on various parameter valuable for a platform selection to build healthcare applications. We observed that Hyperledger Fabric is the most suitable platform to handle access control and interoperability of electronic health records due to following reasons.

- It has a higher transaction rate.
- It supports popular general-purpose languages for Chaincode implementation.
- It has large list of consensus algorithms, and it also supports plug and play consensus mechanism.
- It does not require currency to process transaction.

REFERENCES

- [1] Christian Esposito, Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, Kim-Kwang Raymond Choo "Blockchain: A Panacea for Healthcare Cloud- Based, Data Security and Privacy?", IEEE Cloud Computing Co published by the IEEE CS and IEEE Com Soc January/February 2018
- [2] "Harnessing the Power of Data in Health, Stanford Medicine 2017 Health Trends Report", available: <https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf> 2017.
- [3] Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim, "Blockchain in Healthcare: Challenges and Solutions" Big Data Analytics for Intelligent Healthcare Management, Chapter 8, (Elsevier Inc.)
- [4] <https://www.hipaajournal.com/may-2023-healthcare-data-breach-report/>
- [5] Sabyasachi Chakraborty, Satyabrata Aich, Hee-Cheol Kim, "A Secure Healthcare System Design Framework Using Blockchain Technology ", International Conference On Advanced Communications Technology(Icact), February 2019
- [6] Elizabeth Snell "41% of Health Data Breaches Stem from Unintended Disclosure ", Available:<https://healthitsecurity.com/news/41-of-health-data-breaches-stem-from-unintended-disclosure>, 2017.

- [7] Satoshi Nakamoto "Bitcoin: A peer-to-peer electronic cash system", Bitcoin white paper, October 31, 2008
- [8] R. G. Brown, "The Corda Framework: An Introduction," Retrieved, vol. 27, p. 2018, 2018.
- [9] Morgan, J. P. "Quorum whitepaper." New York: JP Morgan Chase (2016).
- [10] Androulaki, Elli, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." In Proceedings of the thirteenth EuroSys conference, pp. 1-15. 2018
- [11] Benji, Mariya, and M. Sindhu. "A study on the Corda and Ripple blockchain frameworks." In Advances in big data and cloud computing, pp. 179-187. Springer, Singapore, 2019.
- [12] <https://www.stellar.org/?locale=en>
- [13] <https://docs.r3.com/en/platform/corda/4.8/enterprise/node/component-topology.html>
- [14] Baliga, Arati, I. Subhod, Pandurang Kamat, and Siddhartha Chatterjee. "Performance evaluation of the quorum blockchain platform." arXiv preprint arXiv:1809.03421 (2018).
- [15] <https://www.corda.net/blog/transactions-per-second-tps/#:~:text=But%20currently%20Corda%20measures%20between,out%20at%20around%207%20TPS>
- [16] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper 3, no. 37 (2014): 2-1.
- [17] Connors, Collin, and Dilip Sarkar. "Comparative Study of Blockchain Development Platforms: Features and Applications." arXiv preprint arXiv:2210.01913 (2022).
- [18] Nadir, Rana M. "Comparative study of permissioned blockchain solutions for enterprises." In 2019 International Conference on Innovative Computing (ICIC), pp. 1-6. IEEE, 2019.
- [19] A. A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094
- [20] Clincy Victor, and Hossain Shahriar. "Blockchain development framework comparison." In 2019 IEEE 43rd annual computer software and applications conference (COMPSAC), vol. 1, pp. 922-923. IEEE, 2019.
- [21] <https://www.simplilearn.com/tutorials/blockchain-tutorial/types-of-blockchain>
- [22] RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai, "Blockchain: Opportunities for Health Care" White paper, Deolite, August 2016
- [23] Joshi, P. and Gokhale, P., 2021. Electronic health record using blockchain and off chain storage: A systematic review. Information Technology in Industry, 9(1), pp.247-253.
- [24] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), 2017
- [25] Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil and Georgia Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives" Article