A Comparative Analysis of Blockchain Platform: Issues and Recommendations-Certificate Verification System

K. Kumutha, S. Jayalakshmi

A Comparative Analysis of Blockchain Platform: Issues and Recommendations-Certificate Verification System

Kumutha.K[1*] and Dr.S.Jayalakshmi[2]

[1]Tagore College of Arts and Science, Chennai. India
kumutha.k@hotmail.com

[2]Department of Computer Applications, VISTAS,
Chennai. India
jai.scs@velsuniv.ac.in

Abstract. The requirement for the blockchain era maintains growing, and many of the improvement platforms are going vital flow. Amongst those, businesses are further than ever keen to go for blockchain solutions, and they are inclined to the role of a large number of assets for that. There are many more blockchain development platforms are available. Ethereum and Hyperledger platform are greater famous today. The purpose of this research is to examine Ethereum and Hyperledger fabric theoretically and then to observe the problems and recommendations. This research suggests Hyperledger fabric Framework proposes a certificate verification system to avoid the fake and provide high level of security.

Keywords: Blockchain, Ethereum, Hyperledger Fabric, Comparative Analysis and Certificate Verification.

1 Introduction

The future internet is blockchain technology. The first blockchain is Bitcoin which is introduced by Satoshi Nakamoto; it is Bitcoin that came into existence in 2009[1]. Now the Bitcoin became more popular. Bitcoin is the most popular digital money used on peer to peer network in the case of the blockchain. Blockchain technology has the abilities that are Decentralized, Distributed, Secure and Faster, Transparent, and non-modifiable. These are more beneficial than the existing technologies. It is a linked list like data structure that maintains details of data and its transactions via a peer to peer network publically. The great advantage of blockchain enables most of the authors made to implement the educations system. It can store student details such as degree certificates and history of the provider and the address of the student's data in the network. The blockchain technology uses several consensus algorithms and common procedure execution through the distributed public ledger, business logic (smart contract), and cross- chain concepts. There are several blockchain development platforms are available. Each one has its own feature. This research paper analysis overall feature of Ethereum and Hyperledger fabric platform and based on this suggest suited platform implement the use case. These techniques maintain a change of the data integrity by keeping the attributes of transactions such as time, space, and instantaneous multifunctional overlays with constraints such as recordable, traceable and determinable, cost and tradable procedure, etc.,

This article has discussed the concepts of blockchain structure and its function and comparative analysis of blockchain platforms Ethereum and Hyperledger fabric. And also this paper presents the proposed certificate verification system design and its

process.

2 Blockchain

A blockchain is a type of linked list data structure that is used in many distributed ledger technologies. It bundles all the changes made to the ledger (transactions) into packages called blocks and chains them together, using cryptographic hashing, providing an immutable record of all transactions from the genesis (first) block. The structure is presented in Fig 1.

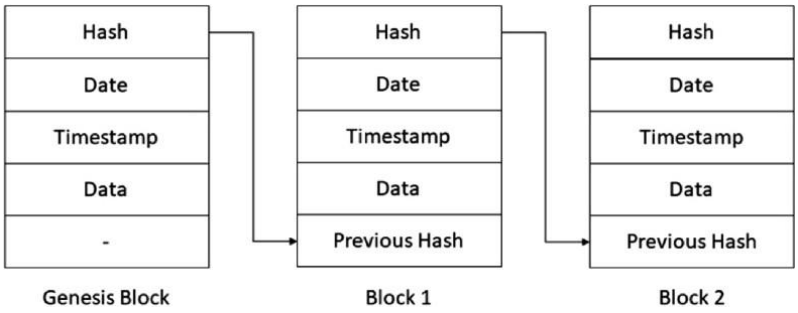

Fig. 1. Structure of a block

Each movement of records is secured with hashing SHA-256 algorithm and then all the transaction summary will be grouped and saved as blocks of data. Then the blocks are joined with the hash price of the previous block and so on and secured from tamper-proof. However, the hash of the block has calculated the use of all the transactions and the hash of a previous block. So, the hash of the ultimate block represents the total blockchain as one value, which makes comparing two chains really easy. As described, blockchain is an immutable report of all transactions. Consensus algorithm: The algorithm used for all the events to agree on a single world state is referred to as a consensus algorithm. Ethereum use the Proof of Work algorithm to reach consensus. All transactions in the previous blocks are validated and then, a new block is added to the blockchain. A consensus protocol consists of agreement, weak validity, robust validity and termination.

3 Blockchain platform

The demand for the platform for blockchain creation is growing day by day in support of business have started to explore the Blockchain based use cases. Another explanation why the number of blockchain platforms is growing is also the growth of dApp production. This article will assist in choosing the best blockchain application for project if who are new to this technology.

5.1 Ethereum

Ethereum is a global and open-source distributed and decentralized platform for all the decentralized applications. Ethereum is energetic since 2015, Vitali k Buterin is the co-founder. It is a permissionless blockchain platform. It has an inner cryptocurrency which is regarded as Ether. It additionally supports smart contracts. A smart contract is a programming code that is completed when an event is triggered. Ethereum operates these steps Block Validation, Node Discovery, Transaction Creation, and Mining in case of the transaction flow.

5.2 Hyperledger Fabric

The Linux Foundation, which established the ecosystem in December 2015, manages Hyperledger. The framework is open source and a modular architecture is supported. Two types of modes are available on Hyperledger: the validating nodes and the non-validating nodes. The validation nodes verify transactions, manage the ledger and

perform the BFT consensus protocol. It follows the execute- order-validate paradigm. IBM and Digital Asset had been the two agencies that constructed the preliminary model of Fabric. It alternatively suffers from two drawbacks. First, it has lacks validated applications and secondly, lacks of skilled programmers able to use this technology.

4 Comparative Analysis of Blockchain platform

This section compares Ethereum and Hyperledger Fabric platforms and table- 1 shows the overall features to gather and highlight the differences between them. And also find out the problems and recommendations of the blockchain development platform to implement the use case.

4.1 Architecture

Ethereum is the permissionless Blockchain for any kind of application. The transactions; are executed by using digital wallet "Gas" by the nodes and fully transparent. In contrast, Fabric affords bendy solutions for personal permissioned blockchain that permit safety and confidentiality. The latter is brought to the Fabric the use of channels that furnish unbiased ledgers on hand only to its users. So, it is viable to create multiple channels and join only some of the users to them. In this case, the ledger is private (cannot be accessed with the aid of non-registered users) and it is viable to share confidential records barring all the network noticing it.

4.2 Consensus Algorithm

Currently, Ethereum is designed to validate the transactions by using proof-of-work consensus algorithm, the place all the nodes agree upon a frequent reality and thereby the ledger. In contrast, Fabric lets in nodes to pick out between no-op (no consensus needed) and an agreement protocol (PBFT) whereby two or greater parties can agree on a key in such a way that both have an impact on the outcome. Thus, Fabric has fine- grained management over consensus and restrained get right of entry to transactions which consequence in extended overall performance scalability and privacy [2].

4.3 Applications

As Ethereum is public and totally obvious it ought to be efficaciously used for most of the ownership storages such as real estate and crypto-currency. Currently, it is feasible to use Ethereum as a fee technique in many methods such as grocery stores, ice-cream shops, online stores, etc. Fabric, on the different hand, gives a way to keep exclusive information that is required for any furnish chain. It permits many applications to be built on the pinnacle of a non-public blockchain, for example, educational certificate, electronic health records, or insurance, where information cannot be shared across the community however it needs to be accessible for precise contributors considering that it is totally private.

4.4 Smart contract Language

One of the largest differences in blockchain platform is programming language. Ethereum uses Solidity language for writing smart contracts for applications and in contrast, Hyperledger uses more languages such as Go, JavaScript, Python and node.js etc. This ensures many programmers to write chaincode in Hyperledger instead of gaining knowledge of a new language [3]. Language help is certainly one of the biggest discrepancies. On the other hand, Ethereum supports languages that are explicitly designed to be used for writing Ethereum smart contracts, such as Solidity and Hyperledger Fabric, supporting more than one common programming language

such as Go, JavaScript, and node.js. This takes us to a scenario where writing chain code is feasible.

4.5 Scalability

In Hyperledger fabric the transaction goes with the flow is divided into orderers, endorsers, and peers. Peers are the recipients of ordered sets of transactions, which they then commit to the network. Endorsers test the cryptographic signatures of a transaction to confirm that is steady with the state of the ledger [4]. Such a permission and modular method advantage the typical scalability of the network, which is the upper bound of transactions that can be processed in a given time- frame. This is special from Ethereum, where the roles played with the aid of the nodes that partake in the consensus protocol are identical, at the cost of its transaction throughput.

4.6 Smart contracts and Chaincode

A "smart contract" is actually a program that runs on the Ethereum blockchain. In Ethereum, the User money owed can engage with a smart contract through submitting transactions that execute a feature described on the clever contract. Smart contracts can define rules, as a normal contract, and robotically enforce them by way of the code [4]. In Hyperledger, clever contracts are referred to as chaincode and, not like Ethereum smart contracts, don’t require costs to be executed. Chaincode is developed with present programming languages, whereas in Ethereum clever contracts are developed with newly designed domain-specific languages such as solidity and accomplished with the aid of EVM. In the case of Hyperledger fabric, the well-supported language for the development of chaincode is Golang. In Fabric interoperability with Ethereum smart contracts is made possible.

5 Problem and Recommendations

The comparative analysis of blockchain structures indicates most of the applications are developed in Ethereum based; only a few papers spoke about the Hyperledger cloth due to lake of experts. And additionally there is a scalability issue in Ethereum compare to Hyperledger [table-I]. Legacy solutions Institutions have invested huge amounts of money into developing the infrastructure and placing up this software, integrating it into their processes. The team of workers has been skilled to operate these structures and it ought to be tough for them to transition to decentralized solutions.

5.1 Problems

Block chain’s scalability: The greater information blocks are added to the blockchain, the slower it works, as it begins taking extra time to analyze all the facts history. Of course, distributed ledger applied sciences are becoming greater scalable nowadays, inventing new approaches of growing the speed of transaction processing [5,10]. High preliminary costs: The fee of altering the environment, putting up the infrastructure, the value of blockchain development itself, as well as blockchain training for the staff. It could be pretty hard to foresee the true economic advantages of blockchain integration in the long run, which encompass reduced costs in management, record-keeping, and extra gains from introducing crypto repayments and rewards.

5.2 Recommendations

The order-execute architecture of the Ethereum blockchain framework slowdowns the transaction processing time. Smart contracts are packages going for walks on an Ethereum blockchain. They are immutable to change, and hence cannot be patched for bugs once deployed as public. Thus it is essential to ensure that the designed smart contracts are bug-free and well-developed before deployment. Change in smart

contracts shows security, architecture, and/or usability problems. On the different hand, In Hyperledger Fabric supports non-public blockchain to use off-line CouchDB and on-line ledger. Changeable statistics are maintained in CouchDB and immutable facts like certificates on line ledger according to that maintain chaincode. Since its permission, architecture, scalability function insists to pick this platform to use the industrial applications [6]. Hyperledger Fabric is quickly gaining recognition and popularity. Most builders prefer it as it approves software enhancement and encourages writing, but it offers centralization and contains a membership carrier node that needs the member's identity, which is largely based on Proof of Work (PoW) and Proof of Stake (PoS) and is just a public blockchain.

Table 1. Comparative Analysis of Ethereum vs. Hyperledger

Characteristics	**Ethereum**	**Hyperledger**
Type of Blockchain	Public/Private	Private
Governance	Ethereum developers	Linux Foundation
Application type	It is general purpose so suited for B2C transactions	It is permissioned type hence suited for B2B transactions
Coin/Token	Ether-ETH as a coin	No such a token/coin
Consensus protocol	PoW/PoS	No predefined consensus protocol ,pluggable
Smart contract	Smart contract	Chaincode
Language	Solidity	Go, Java and Node.js
Nature of Transactions	Publically distributed anyone can access the ledger of transactions	Not public hence the authorized node can access the ledger
Partners	IC3,Microsoft,Accenture,Consens ys,Intel,Santader,CME Group,J.P. Morgan etc.	Air bus ,Accenture, American Express, Cisco, Daimier, J.P. Morgan, Intel ,IBM, SAP etc
Throughput	Up to 20 Transactions per second(tps)	>2000 Transactions per second(tps)
Block-release Timing	12 seconds	Configurable
Transaction Size	Actual max size: 89KB configurable	Maximum size configurable
Transaction Rate	10 transactions/second	1000 transactions/second
Mining	PoW/PoS	N/A

Hyperledger comes with different structures such as Fabric, Iroha, Indy, Sawtooth and Burrow [12]. Though, Hyperledger Fabric (HLF) has been preferred to be utilized in this work due to its inherent privateness and role-based get right of entry to mechanism for getting access to the files that would be suiting to endorse the certificate verification system to prevent fake.

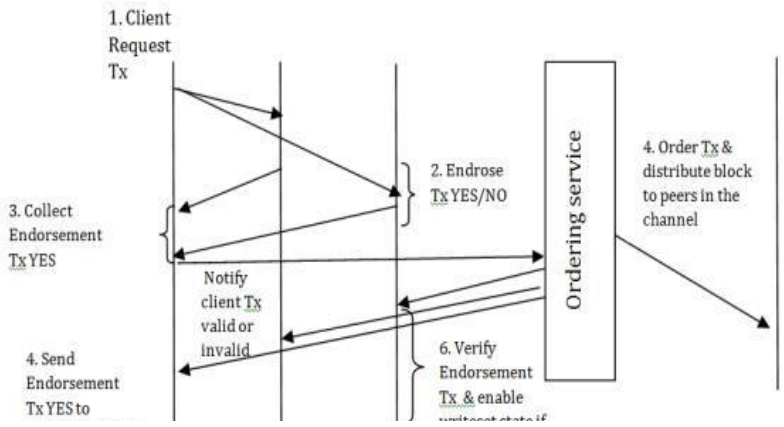

Fig. 2. Transaction flow in Hyperledger Fabric

The architecture of the Hyperledger Fabric consists of peer nodes, nodes for ordering, and client applications. Two functions can be supported by a peer node: a

committer when it holds the ledger by committing transactions and an endorser when it endorses the result after using the chaincode to simulate the transactions completed. In addition, a peer can be an undertaker for particular types of transactions when serving as an endorser for others. Prior to committing it to the ledger, the ordering nodes take care of the order of the transactions in a block. This role can be centralized as effectively as it is decentralized. The function of peer and ordering nodes is comparable to the work performed in Ethereum by miners.

The feature of the transaction flows [fig.2] offers aspects of centralized as well as decentralized in Hyperledger Fabric blockchain science that continues facts with tamper-proof which will keep away from the intruder to get right of entry to and fakes the certificates from the blockchain. No one can access and adjust the certificates different than one who has got right of entry. So this effective function of the Hyperledger Fabric platform suggests that to put in force this blockchain technology to verify the diploma certificates and student's details insecure. The blockchain establishes a set of consensus and frequent operation mechanisms via the general ledger, smart contract, and cross-chain technology. The mechanism solidifies the data movement shaped by using time, space, and instant multidimensional overlays by way of programming to form recordable, traceable, determinable, priced, and tradable technological know-how constraints [2].

6 Proposed Work

The awards and degree certificates of the education institutes can include only the name of the group and the data of the recipient. There is a shortage of excellent anti-forgery mechanisms in this case, and as a result, several times the graduation certificates to be cast are often found. The architecture that would be suggested uses the permit to address the issue of false certificates is the Hyperledger Distributed Ledger Technology (DLT) to grant the following advantages [7],[8]. The blockchain network will issue the certificate in digital form through a distributed ledger, approved access, uniquely identifiable digital certificate and prevents forgery. In addition, it is very difficult to tamper with or manipulate the immutability nature of blockchain allows digital certificate in the distributed ledger and it is very straightforward to check the originality of digital certificate. This system utilizes quite a number of features of blockchain science is a machine for industry-institute interaction the use of Hyperledger.

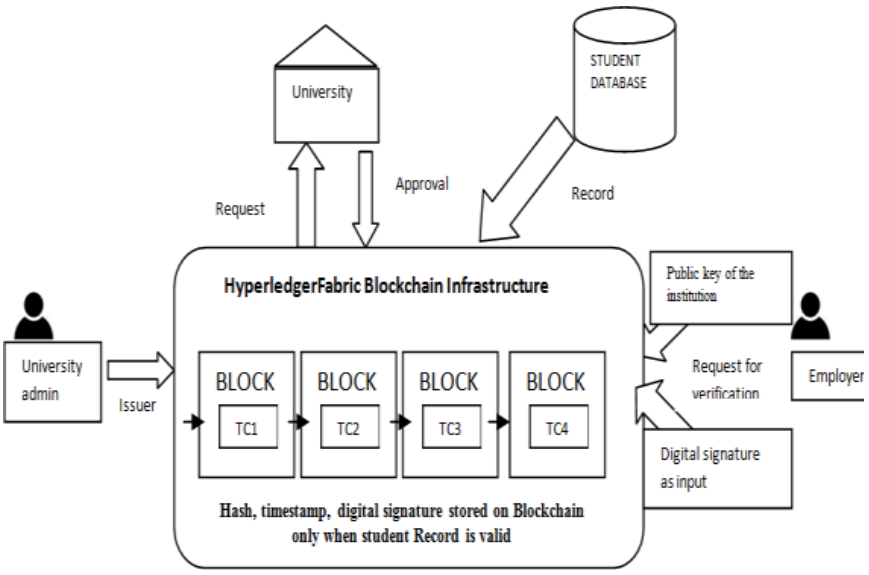

Fig.3. Proposed model of certificate verification system

Certificates furnished by education institutes, or certification units, universities, will have to be admitted to the scheme, and will be able to search through the system

database. The authorities can provide a certificate through the system if students meet certain criteria. After the students have earned their certificates, they will be able to enquire about any certificates they have gained. The service provider is in charge of system renovation [13].

5.1 Process

To process the digital certificate verification system follows the following steps. The first step the blockchain must endorse the users. In this use case universities, institutes, students, and employers are users who verified by using multiple authentication systems through user id, password, biometric (face scanning, retina, fingerprint), and OTP generation. In step two, the valid user can upload the certificate details into the blockchain network with required certificate details and each created certificate will be stored in CouchDB which in turn will return the unique hash generated using the SHA-2S6 algorithm [14]. CouchDB used to store scanned certificate since only the essential details student id, serial no, date and time of issuing the certificate, issuing authority id, qualification along with the hash value. Once the block is created and then verified by a suitable consensus algorithm and the valid block is added to the blockchain network. Then a QR code, OTP, and query string will be created by the device to be affixed to a hard copy certificate to authenticate a hard copy of the certificate via the phone and website. The framework not only provides verification of the certificate, but also stores the certificate in digital form forever, provided the immutability of the distributed ledger [8]. And changing this certificate or producing a fake certificate with the same data is almost impossible. Thus, this proposed system can solve the issue of counterfeit certificates. The process flow is illustrated in Fig.4.

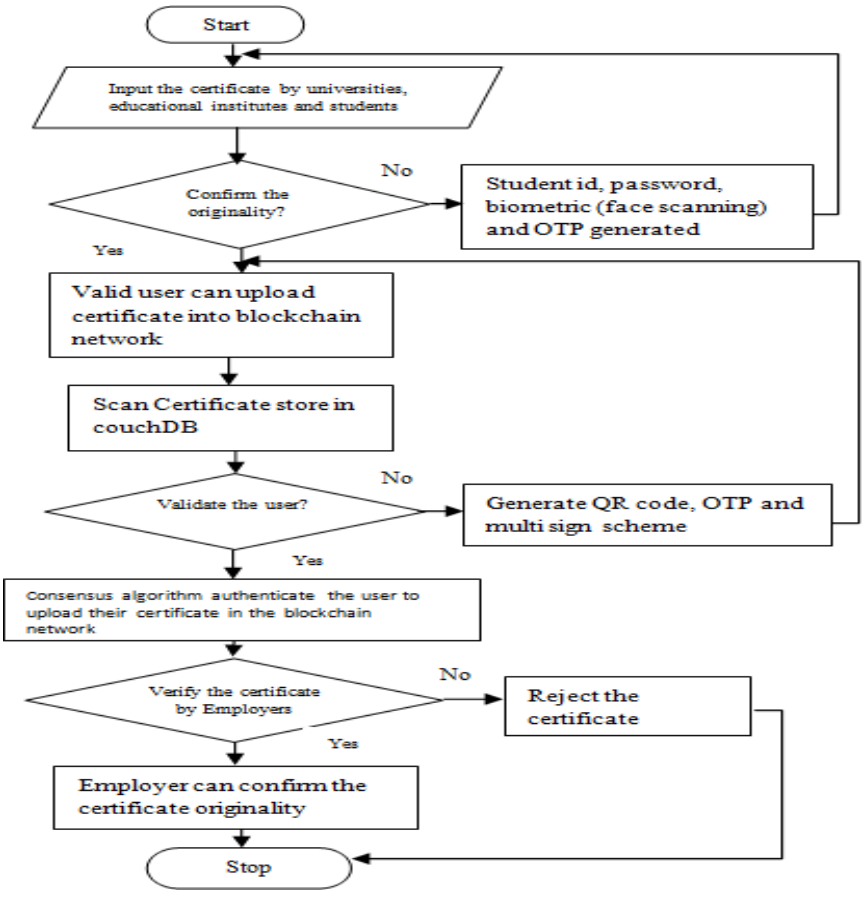

Fig.4. Process flow of certificate verification system

7 Conclusion

The intention of this research is to take a look at Ethereum and Hyperledger blockchain platform features theoretically and then identified that the Hyperledger Fabric Platform is a perfect blockchain-based framework for verifying educational certificates. that specializes in specific issues is proposed [15]. Hyperledger Fabric, however, is designed for private use situations consisting of educational certificates verification inside the blockchain where every node participant have records handiest relevant for them. The risk of certificate forgery is minimized by using the proposed blockchain-based application. In this proposed system, the certificate application process and the automated certificate awarding process are open and transparent. Thus, businesses or organizations may ask for information from the blockchain network on any certificate. Thus, this proposed system guarantees the consistency and security of data. For future work, put in force the present day variations of these platforms and experimentally compare them the usage of distinct overall performance metric such as latency, throughput and transaction rate.

References

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” http://Www.Bitcoin.Org, p. 9, 2008.
2. M. Valenta and P. Sandner, “Comparison of Ethereum, Hyperledger Fabric and Corda,” 2017.
3. Macrinici, D., Cartofeanu, C., Gao, S., Smart Contract Applications within Blockchain, Telematics and Informatics, journalhttps://doi.org/10.1016/j.tele.2018.10.004.
4. Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, “Blockchain and Smart Contract for Digital Certificate,” Proceedings of IEEE International Conference on Applied System Innovation 2017.
5. [online]Available: https://www.blockcerts.org.
6. Dinesh Kumar K, Komathy K, Manoj Kumar D.S , “Blockchain Technologies in financial sectors and industries”, International Journal of Scientific and Technology Research Volume 8, Issue 11, pp. 942 -946, 2019.
7. Benyuan He, “An Empirical Study of Online Shopping Using Blockchain Technology”, Department of Distribution Management, Takming University
8. Zhenzhi Qiu, “Digital certificate for a painting based on blockchain technology,” Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.
9. W. Diffie, P. C. Van Oorschot, M. J. Wiener, “Authentication and authenticated key exchanges,” Designs, Codes and cryptography 2(2), 107-125 (1992).
10. “Ethereum project,” https://github.com/ethereum/wiki/wiki/ White-Paper [Accessed: 13-Jan-2018].
11. MIT Media Lab, “What we learned from designing an academic certificates system on the blockchain,” Medium, no. December, p. 2016.
12. E. Androulaki et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchain,” no. 1, 2018.
13. https://www.indiatoday.in/education-today/featurephilia/story/how-students-and-employers-can-spot-and-eliminate-fake-degrees-1725931-2020-09-27
14. Dinesh Kumar K, Senthil P, Manoj Kumar D.S “Educational Certificate Verification System Using Blockchain “,international journal of scientific & technology research volume 9, issue 03, march 2020 ISSN 2277-8616 82 ijstr©2020
15. S. Jerril Gilda, Maanav Mehrotra -Blockchain for Student Data Privacy and Consent International Conference ,2018 - ieeexplore.ieee.org