Promoting Trustless Computation Through Blockchain Technology

Prateek Pandey¹ · Ratnesh Litoriya¹

Received: 13 February 2019 / Revised: 21 March 2020 / Accepted: 15 April 2020 / Published online: 20 May 2020
© The National Academy of Sciences, India 2020

Abstract Records, irrespective of their nature (whether electronic or paper-based), are vulnerable to fraud. People's hard-earned money, their personal information, identity, and health are at a higher risk than ever due to the misuse of technology in doing forgery. However, the technology can also be used as an answer to counteracting against fraudulence prevalent in affairs from every walk of life. This short paper attempts to present the blockchain technology as a solution to overcome the menace of forgery by promoting trustless computing in business transactions. The paper explains the blockchain technology and a variety of its implementation through five different use cases in the field of drug supply chain, health insurance, land record management, courier services, and immigration records. The immigration blockchain is also proposed as a solution to check pandemic like the coronavirus (COVID-19) effectively. The implementation of the Blockchain is performed using a locally built IBM's hyper-ledger fabric-based platform, and Ethereum public platform. The results are encouraging enough to substitute existing business operations using Blockchain-based solutions.

Keywords Blockchain · COVID-19 · Proof of work · Trustless computing

Introduction

Blockchain, in a straightforward way, can be described as a linked-list data structure where each node (or a computer) is addressed using a hash function of the current and all the historical nodes arranged chronologically [1]. As a consequence of this arrangement, if any node, intermediate or terminal, is tampered with, the decentralized network thus formed by making replicas of the Blockchain shall not accept it by a democratic mechanism called consensus. Therefore, the data rest inside the Blockchain is tamper-proof. Although the cost of maintaining the blockchain network is too high, yet it turns out to be a promising area in which organizations and nations are investing heavily [2].

The most significant selling point of the blockchain technology is that it does not require the participants of the network to trust each other; thus, the necessity of a transaction arbitrator becomes unwarranted. Therefore, virtually all the use cases, from money transaction to mushroom supply chain, and from agricultural commodity market place to electronic health records (EHR) are a potential client for blockchain technology.

Blockchain is broadly categorized in two ways: public Blockchain and private Blockchain. Public Blockchain is characterized by the fact that anybody can actively participate in the network. Private Blockchain, on the other hand, is a restricted network where all the active participants are authorized by some governing authority to make transactions.

Apart from permission, the consensus is another vital parameter on which Blockchains can be differentiated. In the case of public blockchains, the consensus is achieved using time-taking and computationally intensive algorithms like proof-of-work (PoW). PoW is used as a

✉ Ratnesh Litoriya
litoriya.ratnesh@gmail.com

Prateek Pandey
pandeyprat@yahoo.com

¹ JAYPEE University of Engineering and Technology,
Raghuvarh, Guna, India

disincentive for the attackers, and thus provide security to the network [3]. Due to the high cost of computing power involved in PoW, the industry is looking towards other consensus approaches like proof-of-stake (PoS). Private Blockchain, on the other hand, becomes selective in giving permissions to participate, and resort to a mechanism called a selective endorsement, in which some predetermined endorsers are made responsible for validating or invalidating a transaction. Performance-wise, private blockchains have higher transaction throughput than public blockchains, which need more time and computation power to approve a transaction owing to PoW.

In this article, the authors propose the use of Blockchain in five different use cases, namely drug supply chain, health insurance, land record management, courier services, and immigration records. Before setting up a blockchain network, it is essential to ascertain the type of Blockchain which varies from use cases to use cases; therefore, a discussion on the problems and solution objectives for the use cases is warranted to determine the blockchain type and is presented in the subsequent paragraphs.

Use Case 1: Drug Supply Chain

The drug supply chain is vulnerable to encroachment by fraudsters who introduce counterfeit medicines through various access points. Medical store owners can purchase fake drugs from unauthorized dealers and can make a bounty. Another related problem is the reselling of the already sold medicine. This happens when a patient is admitted to the hospital, and the caretakers are told to purchase unnecessary medication [4]. Later those medicines are smuggled back to the drug store, by the staff, in the hospital premises. Consider a Blockchain-based solution, where each drug sachet bears a QR Code that can be scanned through an authorized mobile app. Any customer may check the authenticity of the drug he or she purchases, as the provenance of the drug is traceable. Also, once a drug is sold against a prescription, the same is recorded on a public ledger, making it impossible to resell with a bill.

Use Case 2: Health Insurance Schemes

Around 100 billion INR annual losses are suffered by the insurance industry in India, owing to fake claims [5]. Generally, insurance frauds are done in two ways: (1) People get admitted to the hospitals for at least 24 h to claim insurance; however, actually, they are not seriously ill. (2) People hide their old diseases and treatments undergone at the time of buying new health policies, in order to avoid the increased premium cost. If a nation-wide blockchain is prepared that will register the birth,

vaccination, medical treatments, and even death registration, the chances to hide pre-existing diseases and treatment would become difficult. Also, the quality of treatment would be improved, as a treating physician would know the historical health-related details of the patient on a mouse click.

Use Case 3: Land Record Management

Unlike developed countries, India put forth a strong case for blockchaining land record keeping. Civil courts and newspapers are filled up with a number of cases where perpetrators have forged the records and rob the owners of their rightful properties [6]. Keeping land records on Blockchain not only secure the data from tampering but can also be helpful in land provenance at the time of selling or purchasing an immovable asset.

Use Case 4: Courier Services

With the growing availability and popularity of the Internet, B2C online market is also on the rise. This rise in online business also provides a boost to the supporting services like a courier. Though delivering a consignment late is a cause of bad user experience, but getting a rock in the box while you are expecting a mobile phone is a shock [7]. India has been witnessing such incidents of fraud delivery since the inception of the E-commerce market. On complaining, both the courier partner and the seller deny any involvement in the forgery, and often the customer or the online business facilitator has to pay for it. By keeping the consignment handovers over a blockchain and using X-Ray imagery smartly can deter the forgery to a great extent and thus help to restore the customers' trust in E-Commerce activities.

Use Case 5: Immigration Records

Nowadays, exponentially spreading pandemic COVID-19 (or coronavirus) presents a potential use case for recording a trail of individual's immigration data [8]. Various South Asian countries allowed immigrants to enter without screening that had a recent travel history to China, South Korea, and badly hit European countries. Had any reliable and handy way to verify visitors' travel trail were present, it would have been an effective measure to check the diffusion of the virus.

The above-discussed problems can also be solved using a centralized system approach, but centralized systems possess vulnerability to attack; therefore, a decentralized approach is suitable. Also, the issue of trust among stakeholders advocates the use of Blockchain in a decentralized system.

Whether a particular use case should be implemented as a public or a private blockchain is a crucial decision to make. Immigration information is a kind of personal record, which is vulnerable to breach of privacy if caught in the wrong hands; thus, immigration blockchain should be made privately available to only a few identified government authorities, of course, apart from the immigrant. Courier tracking is mostly an internal affair of the logistics company involved and does not have to include other parties invalidating the consignment at every handover stage. Thus, keeping the courier management use case on a private blockchain ought to serve the purpose. Land records application, on the other hand, is made for the public in general, and therefore, using a public blockchain platform. Drug supply and health insurance use cases ought to be built around a private blockchain owing to the selective participation of the stakeholders.

Implementation and Validation

The Blockchain-based pilot solutions for each use case are implemented on the Ethereum platform and a locally built architecture based on IBM's Hyperledger Fabric [9]. Ethereum is an excellent platform for public blockchains, and hyper ledger fabric is generally used for private blockchains. Therefore, Drug supply, health insurance, and land records blockchains are implemented over the Ethereum network, whereas immigration and courier blockchains are implemented on hyper ledger fabric.

For the Ethereum setup, the Rinkeby public network is used for deploying the smart contracts using Infura API. For locally testing the contracts, the Ganache server is used for testing. All the contracts are written in Node.js, and the communication to the Ethereum world is made using the Web3 module.

The locally built Hyperledger Fabric-based blockchain architecture use four types of nodes called clients, endorsers, organizer, and the committers (Fig. 1). The architecture is decentralized because the same Blockchain is replicated over multiple nodes, which participate in

Fig. 1 Hyperledger fabric-based blockchain architecture

computing. The replica of the Blockchain is available at endorser nodes, and committing nodes; however, no blockchain is maintained on client nodes whose sole purpose is to request transactions. Endorsers receive transaction requests from clients and either endorse or reject those requests. Ordering service collects these transactions to assign their respective blocks and sending them to the committers and endorsers. Three endorsers (E_0 , E_1 , and E_2), two committer nodes, and five ordering nodes are used in this experiment. While Rinkeby public network uses PoW as consensus, the locally built architecture uses PBFT [10], and No-op (no consensus needed) approaches.

Ethereum works on the concept of smart contracts, which are nothing but computer codes that execute on the network when some criteria are met. A typical use case that takes place in land asset transfer is the transfer of entitlement from the landowner to the buyer. Code snippet 1 shows this sample contract written in Solidity programming language for Ethereum.

Code Sinippet 1:

```

13. pragma solidity ^0.4.17;

14. contract LandTransfer{
15.     address public registrar;
16.     address public seller;
17.     address public buyer;

18.     function LandTransfer( ) public{
19.         registrar=msg.sender;
20.     }
21.     function enterSeller( ) public payable{
22.         require(msg.value>100 ether);
23.         seller=msg.sender;
24.     }

1.     function enterBuyer( ) public payable{
2.         require(msg.value==10000 ether);
3.         buyer=msg.sender;
4.     }
5.     function performTransaction()    public
        restricted(){
6.         registrar.transfer(100 + this.balance*0.05);
7.         seller.transfer(this.balance);
8.     }
9.     modifier restricted( ){
10.        require(msg.sender==registrar);
11.        _;
12.    }

```

Table 1 Transaction throughput in different configurations of the participating nodes

Config #	Endorsing nodes	Ordering nodes	Committing nodes	Throughput (transactions/s) Immigration Records	Throughput (transactions/s) Courier Tracking	Config #	Endorsing nodes	Ordering nodes	Committing nodes	Throughput (transactions/s) Immigration Records	Throughput (transactions/s) Courier Tracking
1	1	1	1	10	9	9	3	1	1	9	9
2	2	2	1	8	7	10	3	2	2	7	8
3	2	3	1	9	7	11	3	2	1	6	7
4	2	4	2	5	6	12	3	3	2	6	6
5	2	4	1	5	5	13	3	3	1	6	6
6	2	5	2	4	5	14	3	4	2	5	6
7	2	5	1	4	5	15	3	4	1	5	5
8	3	1	2	8	7						

The above LandTransfer contract can be stated as follows:

1. A seller has to pay 100 ether for entering into contact, whereas buyer just pay the buying price
2. Registry charges include 100 ether plus 5% of the total selling price as commission
3. The only registrar can perform the transaction

For implementing private Blockchain on the locally build system, we take the example of an immigration application. Since this is a private network, therefore, only those who are permitted can participate or view the network information.

Authentication and Authority Agency (AAA) performs this operation of giving authority. We assume that

immigration checkpoints are located at all international airports, seaports, and roadway borders. Whenever an immigrant enters, their entry is recorded on a public ledger used by all the participating countries. Every such entry is a new transaction requested by the client node. This request goes to the endorsing nodes (see Fig. 1) where smart contracts get executed, and the request is then sent back to the client nodes with an endorsement. By this time, no ledger update takes place. The client then sends the endorsed request to the ordering nodes, where PBFT or No-op algorithm works to assign an existing block or a new block to a transaction. Afterward, the news about the newly created block is broken out to the adjoining peers (committing nodes and endorsers), and all the nodes update their Blockchain accordingly; thus, a consistent ledger is

Fig. 2 System configuration versus throughput **Fig. 3** Endorsing nodes versus throughput

maintained at every participating node. The test network was laid using five computer systems (nodes) reserved for ordering service. Three nodes were designated as endorsing nodes, and two nodes were given the task of committing the transactions on the ledger. Endorsing nodes and committing nodes to maintain their copies of blockchains, which, of course, have to be kept consistent by the consensus algorithms running on the network. Each block was fixed at 20 KB size and can contain ten transactions, roughly. A time limit of 5 min was also assigned to each shaping block; otherwise, a block might have to wait for too long to commit itself in the Blockchain if no new transactions are coming up. The outcome of the discussed exercise is that whenever a foreign visitor or a resident citizen enters into the national territory, the immigration

trail of the said person can be verified, and if required, the same person can be quarantined then and there without giving a chance to contract the disease to others.

While implementing the private Blockchain for immigration records and courier tracking, we observe the performance of the built network in terms of throughput, which is the number of transactions written in the ledger per second. Throughput is a concern because consensus algorithms like PoW or PBFT take time to verify a transaction. We created 15 different configurations of nodes and test the throughput of immigration records and courier tracking implementations on each configuration. The results are tabulated in Table 1 and plotted in Figs. 2, 3, 4 and 5.

Fig. 4 Ordering nodes versus throughput **Fig. 5** Committing nodes versus throughput

By looking at Table 1 and the performance graphs, it can be concluded that the network throughput is mainly influenced by the ordering nodes and by choice of consensus algorithm involved. The performance of public blockchains we created is not observed because the pilot applications were deployed on Rinkeby public blockchain network, and the typical network latency for Rinkeby is 15–30 s.

Conclusion

In a nutshell, this article presented a holistic approach to answering the fraudulence prevalent in a number of businesses—public or privately owned. The solutions that are

proposed are all based on using Blockchain as an underlying platform to perform transactions, thus providing security and transparency to counteract against encroachments of all forms, be in lands, drugs, insurance claims, courier delivery, or the most deadly of all COVID-19. The authors presented the performance observed after the implementation of the said applications and noticed that the throughput is a significant concern in blockchain implementations. In the case of private blockchains, the number of validating nodes (ordering nodes) plays an important part in deciding the performance of the network. In this testing period, when the entire world is severely affected by the coronavirus, the suggested use case of the

blockchain technology for immigration data recording can act as a major force in repelling future viral attacks.

References

1. Jaeger LG (2018) Public versus private: What to know before getting started with blockchain. IBM. <https://www.ibm.com/blogs/blockchain/2018/10/public-versus-private-what-to-know-before-getting-started-with-blockchain/>. Accessed 15 Feb 2020
2. Matisek JW (2018) The blockchain arms race: America vs. China. *The National Interest*
3. Hooda P (2018) Proof of work (PoW) consensus. <https://www.geeksforgeeks.org/proof-of-work-pow-consensus/>. Accessed 15 Feb 2020
4. Mahajan V (2010) White coated corruption. *Indian J Med Ethics* 7:18–20
5. Pandey P, Litoriya R (2020) Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. *Health Policy Technol* 9:69–78
6. Naveen P (2017) Bigger than Vyapam, Madhya Pradesh Land record ‘scam’ cry in digital drive. *The Times of India*
7. Ghunawat V (2017) Online shopping goes bizarre: customer buys smartphone on Amazon, gets a stone delivered instead. *India Today*.
8. The Ministry of Home Affairs (2020) Advisory: travel and visa restrictions related to COVID-19. Bureau of Immigration. <https://boi.gov.in/content/advisory-travel-and-visa-restrictions-related-covid-19-0>. Accessed 15 Mar 2020
9. Hyperledger fabric: the flexible blockchain framework that’s changing the business world. IBM. <https://www.ibm.com/blockchain/hyperledger>. Accessed 30 June 2019
10. Hao X, Yu L, Zhiqiang L, Zhen L, Dawu G (2018) Dynamic practical byzantine fault tolerance. In: *IEEE conference on communications and network security, CNS 2018*, pp 1–14

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.