2019 5th International Conference for Convergence in Technology (I2CT)
Pune, India. Mar 29-31, 2019

A study on Blockchain enabled Applications and its Security Issues

Nilima D. Pai
B.Tech. Computer
Mukesh Patel School of Technology Management and Engineering, NMIMS, India
pai.nilima1998@gmail.com

Shaheen Mondal
B.Tech. Computer
Mukesh Patel School of Technology Management and Engineering, NMIMS, India
shaheen30mondal@gmail.com

Abstract- **Blockchain technology was first established because of its use in cryptocurrencies, but its applications are not limited just to this field. We have explored other fields like Finance, Auditing, Digital identity, Digital Voting and Healthcare where blockchain can be used to increase efficiency, and how it fares compared to the traditional systems. The paper compares the traditional and blockchain enabled systems based on parameters like privacy, data and application security, consensus algorithms and mining computations. However, like any other technology, this one too might have flaws which can be exploited. This paper also lists the security challenges that need to be kept in mind while implementing these systems.**

Keywords- security; blockchain; shared ledger; key management; consensus; cryptocurrency; bitcoin; healthcare; finance; auditing; identity; digital voting; comparison

I. INTRODUCTION

Blockchain is one of the latest buzzwords in a lot of industries. It is a technology which is set to change the nature of the internet as we know it today, from an information based internet to a value based one [1]. The average investment in blockchain projects in 2017 has been $1 million [2] and is expected to have a yearly growth rate of 75% till 2021. One of the most famous applications of this technology is Bitcoin, but apart from this, there are multiple other fields where blockchain can be used to increase accuracy, credibility and efficiency.

The questions we address in this review paper are what blockchain is, why it is supposed to be secure, which are the applications where blockchain can be used to improve efficiency. This paper also compares the new blockchain system with the traditional systems, and highlights any security issues that might arise.

Blockchain can be defined as "secured, shared and distributed ledger that facilitates the process of recording and tracking resources without the need of a centralized, trusted authority" [3]. It records data and events in an immutable and decentralized fashion, and relies on public entities to verify and finalize these transactions. The verification process consists of private servers which act as individual nodes. These nodes mine transactions using security algorithms like Proof of Work (PoW) or Proof of Stake (PoS) and when a sufficient number of transactions are mined, they are grouped into a block. This block is then broadcasted to all other nodes for verification, and if a majority of nodes accept the new block, it is added to the 'chain of blocks' with a link/ hash to the previous block for maintaining a linearity. Information is encrypted and digitally signed. Each member in the network stores an identical copy of the blockchain and contributes to the process of adding blocks to the network. The longest chain at any point of time is considered to be the correct one and the other blocks are pruned, and the transactions in those blocks are considered to have never happened [11]. The blockchain architecture consists of 4 layers as shown in the figure 1.

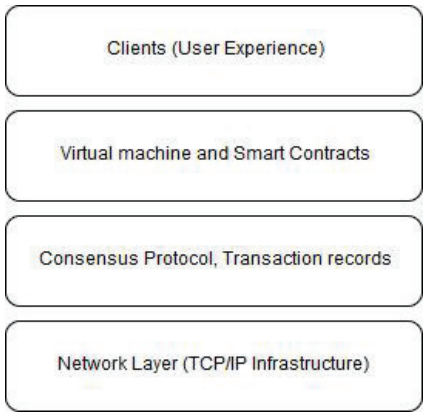

Fig. 1. Blockchain Architecture

However, there are still some drawbacks of some of the protocols used in the blockchain system. One of these is the energy efficiency of the PoW algorithm which utilizes energy and hardware for no real useful work.

The objective of this paper is to provide a review on how blockchain replaces the traditional systems in some of the applications, and the security issues that it's developers will have to keep in mind. Also, if you are looking to replace the data storing and recording system in your company with one of these solutions, this paper will help you decide the pros and cons of actually going for it. The possible blockchain applications we describe are shown in figure 2.

II. RELATED WORKS

There are some other papers which have covered security issues like privacy, provenance and integrity services like [3], comparison of various blockchain platforms as well as DLT security challenges [8]. Blockchain security challenges have also been discussed in [9]. The paper [3] also describes similar issues along with countermeasures for possible attacks. Paper [10] provides solutions for recording data in a decentralized manner which can be used in financial services or cryptocurrencies.

978-1-5386-8075-9/19/$31.00 ©2019 IEEE

III. APPLICATIONS OF BLOCKCHAIN

Cryptocurrencies are digital or virtual currencies that use cryptography for security. Cryptocurrencies are used online and are not centralized [4]. The decentralized control of each cryptocurrency works through distributed ledger technology, or a blockchain [5]. The first decentralized cryptocurrency, Bitcoin, which is a worldwide digital payment system that transfers value as fast and as efficiently as data, was created in 2009 by pseudonymous developer Satoshi Nakamoto [5]. It has reached a capitalization of 180 billion dollars as of January 2018 [3]. Due to this growing fame of Bitcoin cryptocurrency, several other applications (like finance, auditing, e-voting etc.) have discarded the traditional systems and adopted blockchain architecture for their working. Cryptocurrency, contrary to fiat currency, is not backed by a central government or bank [6]. Even though cryptocurrency has drawbacks like difficulty in understanding, volatility and uncertainty, the many advantages that cryptocurrency offers over fiat currency makes it more beneficial to the consumers. The several advantages include no inflation, international mobility, ease of use, privacy, no third party, high security and protection against identity theft [7].

Further, we discuss some other applications of blockchain, mainly focused on how they replace the traditional systems, and their security issues.

A. FINANCE

The main reason for adopting blockchain in financial technology (commonly known as FinTech) is utilizing the security and reliability of the underlying infrastructure and implementing smart contract functionalities [11].

In traditional financial systems, transactions take a day or several days. Also, transactions have to be carried out in country specific fiat money. Distributed Ledger Technology can be used for any transaction including currency, gold, arbitrary securities, etc. Bitcoin arose to eliminate central authority. It was found that blockchain allows parties to do financial transactions without any centralized authority and with low transactional cost [12].

Financial services can be implemented using permissioned blockchains which use permissioned consensus protocols. It means that the nodes or miners mining the blocks are verified and selected private ones. Thus, there is reduced transaction latency, operational risk, process friction, liquidity requirements as found out in [11]. Financial institutions like the New York Stock Exchange, Bank of America, JPMorgan, Fidelity Investments, Standard Chartered and Bank of Canada are testing the blockchain technology and digital currency alternatives. The critical difference between this and other technology solutions is that cryptocurrencies require every party involved to adopt it [13].

However, existing cryptocurrencies have a rate of a handful transactions per second. To achieve optimum efficiency when used in financial institutions, it must increase to dozens. To make this happen, the structure of the current blockchain architecture must change, say by using solutions like Bitcoin NG (Next Generation), Hybrid Protocols, Solidus, or Spectre protocols [11].

B. AUDITING

Traditional security auditing systems are usually privately developed and employed for specific business purposes [17]. Blockchain can be used to create a public auditing system which also has the ability to keep its records classified. The very nature of the blockchain technology makes it suitable for recording data about events in a verified and immutable fashion. Data may be timestamped for additional security. A private or permissioned blockchain can be used to ensure that the records are kept safe [18].

The system described in [17] is ISO/IEC 15408-2 compliant and has functions for automatic response, data generation, audit analysis, audit review, event selection (for querying), and storage. The blocks consist of each security event (or incident) and are retained in the inherent blockchain network.

The implementation consists of 3 stages:

1. Proof of concept- a private blockchain network based Ethereum, and simulation of smart contracts for a single node
2. Security enforcement- even if a hacker is able to recover a block, the data is coded and protected by a unique key
3. Analysis enhancement- data analysis, security event forecasting and smart alerting mechanisms

However, some of the issues that the system will have to deal with are data confidentiality at IOT node level, and trying to maintain the balance between performance efficiency and ensuring credibility of access during data holding and recovery operations.

C. DIGITAL IDENTITY

A digital identity is the body of information about an individual, organization or electronic device that exists online [21]. The digital identity of a person must contain the fundamental information of a person along with the biometrics. Estonia was the 1st country to use blockchain at a national level with their E-Citizenship program. Estonia utilized the distributed ledgers technology to create their own identity system called ID-kaarts or ID-cards [19].

Currently, in India, Aadhaar is being used a form of national digital identity. Aadhaar is a 12 digit unique-identity number allotted to all Indian citizens based on their biometric and sociological data [20]. It used by many institutons in India. With Aadhaar, all the information of the 135 crore Indian citizens is available at central storage and can be used effectively for applications like banking, pensions, income tax etc. [20].

Along with the numerous advantages Aadhaar and other national identity systems have, they also many pitfalls which cannot be ignored. Aadhaar project, like many other projects, is being handled by foreign private companies. It is also sent to Foreign Companies for research and development. This leads to data erosion and may also compromise the privacy of every individual. This identification can even be used to forge transactions in banking and cause heavy loss to numerous people. Blockchain gives a solution to all these problems. Also, the centralization of authority in Aadhaar will create several other issues which can be prevented by implementing decentralized blockchain technology.

Merits of implementing blockchain in digital identity include easy tracking and management of digital identities, elimination of digital clones and improving data sharing and integration by cutting down the cost incurred by the traditional data system. Customers can also experience faster transaction and quicker data verification [21]. Utilization of Aadhaar along with Blockchain opens the possibilities to endless secure and efficient applications in the fields of finance, healthcare, national security, citizenship documentation or internet marketing [20]. The implementation using Blockchain technology works as follows

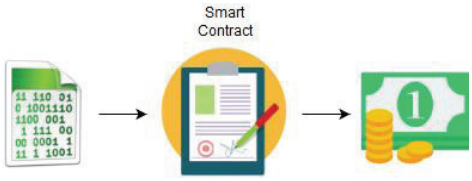

Fig. 2. Information flows through smart contract

1. Initially, an Ethereum block chain network will have to be created [20].
2. Next, smart contracts will be generated. The chaincode or smart contract will be executed after a suitable event by all the entities involved, it acts as the trigger to the blockchain network, as shown in figure 3. Whatever updates that take place in the data will be added to the public ledger, to ensure clarity in the records. Each transaction would have to go through the smart contract [20].
3. Then, we will have to create a distributed application which can be easily and effectively used. Every transaction should be signed by the correct private key. It will uniquely authenticate every identity. [20]

D. DIGITAL VOTING

E-Voting is an application of blockchain which is very closely related and even based on our previous application of digital identity.

The current electoral systems use conventional paper ballot system. The aspect of security and clarity is still threatened in large elections which use the traditional offline system [14]. A single organization has complete command over the database and system and it becomes considerably easier to manipulate the results and data store [14].

Blockchain technology is a very good answer which can be used to address all the issues in the traditional systems [14]. Blockchain makes the voting decentralized and makes the database public which is useful to find any discrepancies [14]. Also, it makes voting much easier and user-friendly. It can be programmed according to the needs of each election and has high verifiability and integrity [14]. In the blockchain implementation, each voter's vote acts as a transaction that can be recorded into a blockchain and track voice counting. Everyone can sanction the concluding voting computation because of the public blockchain analysis track. It maintains data integrity and protects the results from manipulation [14]. An efficient and simple way of implementing blockchain in our voting process is shown below in figure 4.

Fig. 3. Flow Design [14]

In the beginning, each participating server renders a public and a private key. Each of these has a public key list of all nodes. During election, each node gathers results from each voter. After this is accomplished, the nodes wait for their chance in the block. When the block arrives on each node, verification is done to ascertain if the block is legitimate or not. If yes, then the data in the block is added in the data store.

After the updating process, the server checks whether the node identification that was brought belonged to him or not. If the node gets a chance, it will generate and present a block that has been filled in digital signature to transmit to all nodes with the help of turn laws. This presented block contains the identification node, the next identification node(token), timestamp, hash of previous node, voting result and digital signature of the code [14].

E. HEALTHCARE

Electronic Health Record systems today which are maintained by healthcare institutions are often accessible to only that institution, and not even available to the patients to keep track of their own health records. These records are not convenient for the patient to carry forward should the patient have/ choose to change his healthcare provider, nor are they shareable to researchers and scientists who need the data to carry out a comprehensive study. Blockchain has the power to address the interoperability challenge and to be a technical standard to share data. It can promote advanced medical research based on large pools of data, as well as the development of precision medicine.

The health blockchain described in [15] has to have three important components: scalability, access protection and information privacy. The paper proposes a blockchain which contains only an index and metadata of all the health records, which in turn would be stored in a data lake. The user can exercise complete control over his data and assign permissions and denominate who can query and write data to his blockchain through a mobile application, as shown in figure 5. At the same time, researchers will be able to mine data from a large database of anonymized but detailed records.

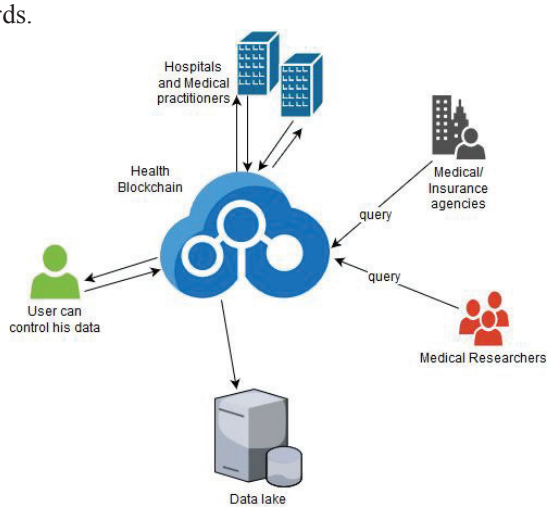

Fig. 4. Healthcare Blockchain and its entities

Paper [1] has described a key management system for Body Sensor Networks used in recording health data, and also a lightweight backup and recovery scheme for the public and private keys of the blockchain. The advantages of this system are

1. Storage of keys: no need to change keys, hence there is no need to store historical data about keys. This reduces storage cost, as well as access time
2. The blockchain does not store the key, only a clue to the key
3. Blockchain does not store private data, only ciphered text

IV. SECURITY CHALLENGES

We now know that, blockchain is more efficient compared to most traditional systems but to fully utilize the potential of block chain we need to ensure that there are no security concerns in our implementation. Security measures in any blockchain include entity authentication, confidentiality, privacy services, provenance services and integrity services [3].

A node is considered to be active if it has and maintains a certain number of connections A node that does not allow the transmission of data, or broadcasts wrong data, must be identified to maintain the state of the system. A private blockchain may allot the more central positions in the blockchain network to conventional trading partners, and may need new nodes to keep a relation to one of these specified nodes as a security tactic to ensure it works as it is expected [13]. If we have uncommunicative nodes, it might be cause for a security concern as the network must be able to function with or without those nodes. It causes a significant obstacle for fast paced transactions, which is one of the key requirements for financial services [13].

The processes used for consensus when the network decides to accept or reject a block have a certain delay associated with them because of which the system remains vulnerable for that time. This is not much of an issue in private blockchains, as operators can select and permit only those nodes to act in the consensus process [16]. Though the data stored in the blockchain (or servers) is secure, as it is encrypted, a major vulnerability lies in the security of the private keys allotted to the users. This is a matter of personal security, and not actually a failure of the blockchain system itself [16].

Apart from this, security of the blockchain also depends on various parameters like data security, storage security, physical security, privacy and application security. Especially, for privacy, an important consideration is of the Right to be Forgotten which due to the immutability characteristic of blockchain, might not be upheld, however, there have been some solutions.

As shown in figure 5, the privacy system consists of access control policies through smart contracts or through specific transactions defined in the system. Also, the owner may or may not interact with the service (blockchain) through a service provider.

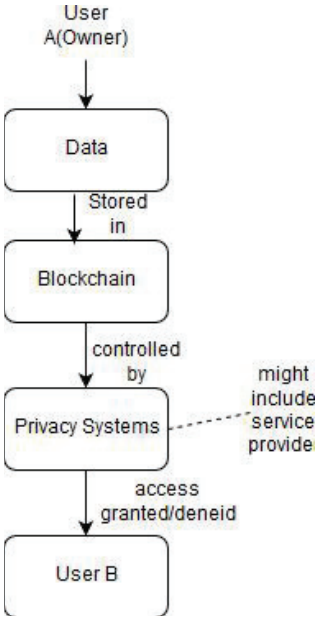

Fig. 5. Privacy systems

Metadata is used to track data and/ or a physical supply chain. The changes in metadata of the information are requested and recorded through smart contracts or special transactions specified in the system.

The acceptance or rejection by the controller consists of either voters or miners voting on the proposed changes. This may also be done by a centralized Provenance auditor, but this way does not utilize the consensus mechanism of blockchain. This is shown in figure 6.

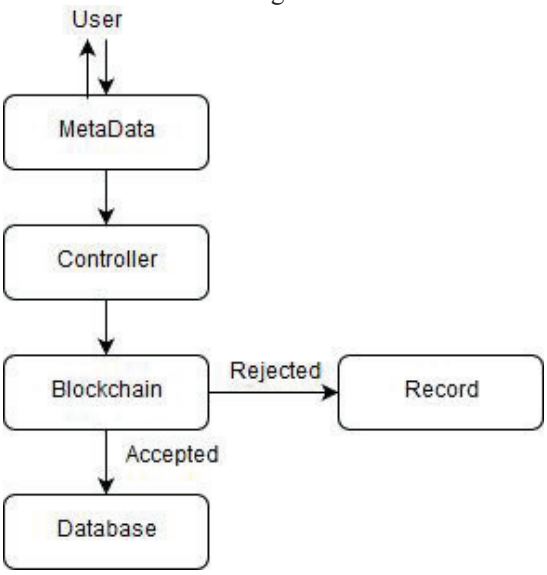

Fig. 6. Provenance services

V. INFERENCE

The table below compares the traditional systems and blockchain based systems with respect to various parameters. Depending upon these, it can be decided whether switching to blockchain is beneficial.

TABLE 1. COMPARISON OF TRADITIONAL AND BLOCKCHAIN SYSTEMS

Parameters	Traditional systems	Blockchain systems
1. Privacy	Encryption depends upon implementation. Users usually are not anonymous.	Data stored once can't be removed, might interfere with Right to be Forgotten. Data is encrypted by default. Users remain anonymous
2. Data security	Data can be changed by authorities	Data stored in immutable fashion, so can't be changed
3. Storage and Physical security	Depends upon physical safety of database	Depends upon physical safety of database
4. Application security	Depends on design	Depends on design
5. Scalability	Depends on how system is designed	Increasing number of nodes might require change in the structure of blockchain implementation
6. Consensus algorithm	n/a	Security is compromised if majority in the network is attained by a single miner
7. Mining computations	n/a	Different algorithms can be used: PoW, PoS, PoET, etc. [3]. These differ in complexity, time required and energy efficiency.

VI. CONCLUSION

In this review paper, we presented a brief study about what exactly blockchain is and what are its different merits. We also gave a short summary on cryptocurrency and how it utilizes blockchain. We discussed various applications of blockchain like finance, auditing, digital identity, voting and healthcare and we compared the traditional systems of these applications with the blockchain based systems. We mentioned the diverse security issues that one might face while using blockchain and also addressed the security services provided by it. Finally, we stated the differences between traditional systems and blockchain architecture based systems with respect to multiple parameters which are important to know while studying this topic. Future research directions include overcoming all the security issues stated in this paper and advancing blockchain further to new kinds of applications.

ACKNOWLEDGEMENT

We wish to thank our parents for their inputs and support, Prof. Krishna Samdani for his guidance and our college for the opportunity to pursue this subject.

REFERENCES

[1] Huawei Zao, Peidong Bai, Yun Peng, Ruzhi Xu, "Efficient key management scheme for health blockchain", CAAI Transactions on Intelligence Technology, 2018, Vol. 3, Iss. 2, pp. 114- 118.

[2] Expanded Ramblings, https://expandedramblings.com /index.php/blockchain-statistics/, 10/10/18

[3] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, Mohammed Samaka, "Security Services Using Blockchains: A State of the Art Survey", CAAI Transactions on Intelligence Technology, 2018, Vol. 3, Iss. 2, pp. 114- 118.

[4] Forbes, https://www.forbes.com/sites/forbescommunicationscouncil/ 2017/11/15/the-financial-revolution-and-the-many-benefits-it-brings-crypto currency-blockchain-technology/#f4de4833cc0a, 10/10/18, 2:07 pm

[5] Wikipedia, https://en.wikipedia.org/wiki/Cryptocurrency, 10/10/18, 1:51 pm

[6] Daily Forex Report, https://www.dailyforexreport.com /benefits-cryptocurrency-jordan-lindsey/ , 10/10/18, 2:26pm

[7] Coinpupil, https://coinpupil.com/altcoins/advantages-isadvantages-of-cryptocurrency/, 10/10/18, 2:40 pm

[8] Joanna Moubarak, Eric Filiol, Maroun Chamoun, "On Blockchain Security and Relevant Attacks", IEEE Middle East and North Africa Communications Conference, 2018

[9] I.C. Lin, T.C. Liao, "A survey of Blockchain Security Issues and challenges", International Journal of Network Security, Vol. 195, 2017, pp. 653-659

[10] P.L. Seijas, S. Thompson, D. McAdams, "Scripting Smart Contracts for Distributed Ledger Technology", Cryptology e-Print archive, Report 2016/ 1156, 2016.

[11] Ittay Eyal, "Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finanace and Banking Realities", IEEE Computer Society, 2017, pp. 38- 49

[12] Pasu Poonpakdee, Jarotwan Koiwanit, Chumpol Yuangyai, Watchara Chatwiriya, "Applying Epidemic Algorithm for Financial Service based on Blockchain Technology", IEEE, 2018

[13] Harvard Business Review, https://hbr.org/2017/01/the-truth-about-blockchain, 10/10/2018

[14] Rifa Hanifatunnisa, Budi Rahardjo, "Blockchain based E-Voting Recording System Design", IEEE, 2018

[15] Laure A. Linn, Martha B. Koo, Healthit.gov, https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare .pdf, 26/07/2018

[16] Harvard Business Review, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends, 10/10/2018

[17] Shi-Cho Cha, Kuo-Hui Yeh, "An ISO/IEC 15408-2 Compliant Security Auditing System with Blockchain Technology", IEEE Conference on Communications and Network Security, 2018

[18] Pedro W. Abreu, Manuela Aparicio, Carlos J. Costa, "Blockchain technology in the Auditing environment", IEEE

[19] Medium, https://medium.com/@bryzek/how-blockchain-is-used-by-governments-as-a-form-of-national-identity-e24a4eefb7d8, 12/10/18

[20] Kumaresan Mudliar, Harshal Parekh, Dr. Prasenjit Bhavathankar, "A Comprehensive Integration of National Identity", International Conference on Communication, Information & Computing Technology (ICCICT), 2018

[21] WhatisTectarget, https://whatis.techtarget.com/definition/digital-identity, 12/10/18