Research Inventy: International Journal of Engineering And Science
Issn (e): 2278-4721, Issn (p):2319-6483, PP: 06-11
www.researchinventy.com

A Review Study on Blockchain Security

Souvik Halder[1] , Shuvo Bangal[2], Sangita Majumder[3], Avijit Mondal[4]
Department of Computer Science and EngineeringTechno International Batanagar avijitmondal88@yahoo.com

Abstract
In modern times, blockchain technology is seen as an innovative technology paradigm. Blockchain-based networks, distributed apps, and distributed ledgers are becoming the foundation of our digital life. Blockchain is a circulated database that maintains a collective set of data, those are called blocks, and each encoded block of code contains a past record of all the blocks that precede it. The connection of these blocks is called a blockchain.

There are many aspects to reviewing blockchain technology, but blockchain security is always a user concern. Security is typically assessed in terms of integrity, confidentiality, and availability. This review attempts to provide a broader perspective on the security issues associated with blockchain technology and also discusses the various security risks associated with common blockchain set-up. This white paper also describes the various cryptographic techniques used in blockchain systems to secure data and protect it from vulnerabilities.

Keywords
Decentralization, Distributed System, Security, Vulnerability, Encryption, Chaining,Transaction.

I. Introduction

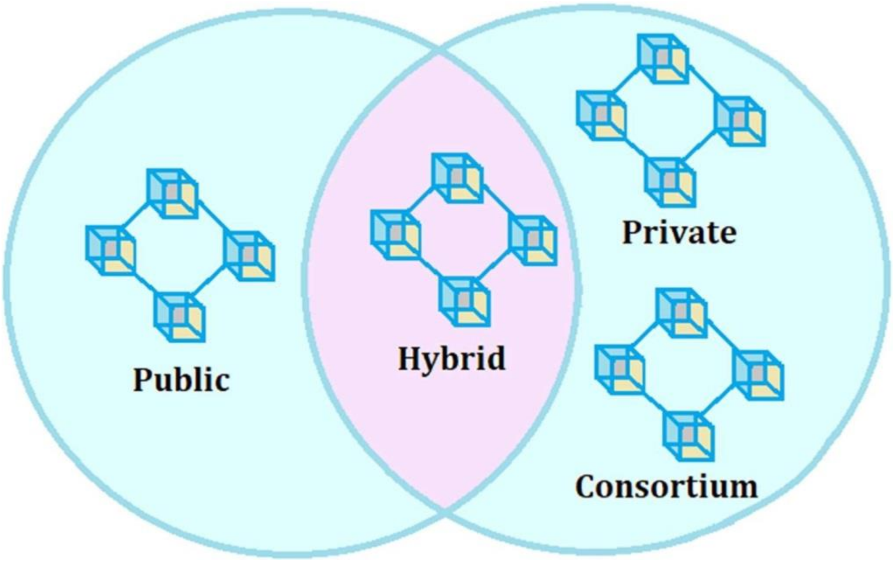
Blockchain is one of the most developing technologies in the current world which will create a strong impact on many current businesses. Every day it becomes more popular among the researchers, developers and industry experts[3] [4]. Blockchain is a block of distributed blocks which are connected based on cryptography. Each block contains transactions with timestamp and hash value of the previous block. The main underlying intentions behind blockchain is to easily establish trust between two unknown parties. Blockchain, replace the third party of the transaction with some code.

Blockchain started gaining popularity after the release of Bitcoin whitepaper in 2008 by Satoshi Nakamoto. It has a wide range of applications which are increasing every day.
The major uses are cryptocurrency, healthcare, NFTs etc. Actually, blockchain acts as a distributed, decentralized database[4].

The blockchain secures itself with an immutable distributed ledger that cannot be edited or deleted once it is written. Each block has a hash value, and the next block contains the chain stored on every node connected to the network, so it's almost impossible to change. As a developing technology it has some challenges like scalability,privacy leakage, DDoS attack, MITM attack[6].

Types of Blockchain
The blockchain is divided into four major forms based on the nature of the business and individual requirements:

1. **Public Blockchain**
2. **Private Blockchain**
3. **Consortium Blockchain**
4. **Hybrid Blockchain**



1. **Public Blockchain** : Public blockchains are permissionless by nature, allowing everyone to participate, and are totally decentralized. The public blockchain allows all blockchain nodes with equal permissions to access the blockchain, create new data blocks, and validate data blocks. Anybody with a proper internet connection can able to join a blockchain platform and become an approved node, making the public blockchain untethered and unauthorised.

2. **Private Blockchain** : Private blockchain, known as managed blockchain, is an authorized blockchain managed by one entity. The central authority of the private blockchain determines who can be a node. Central authorities do not always give each node the same authority to perform a function. Public access to the private blockchain is limited and therefore partially decentralized. Ripple, an inter-company cryptocurrency exchange network, and Hyperledger, a comprehensive project of open source blockchain applications, are two instancesof private blockchain.

3. **Consortium Blockchain**: A consortium blockchain, unlike a private blockchain, is a licensed blockchain managed by a community of organizations rather than a single organization. As a result, consortium blockchains have greater decentralisation than private blockchains, resulting in increased security. However, forming a consortium can be a difficult process as it requires the collaboration of multiple companies. This poses both a logistics obstacle and a risk of antitrust violations.. In addition, some supply chain participants may lack the necessary technology or infrastructure to adopt blockchain technologies, and those who can may decide that the initial expenditures of digitising their data and connecting to other supply chain members are too high a price to pay.

4. **Hybrid Blockchain**: - A hybrid blockchain is a combination of private and public blockchains. It combines the best aspects of both private and public blockchains, permitting for both permission-based and permissionless systems. With such a hybrid network, users can control who has access to what data stored in the blockchain. Only a selected portion of blockchain data or records can be made public, keeping the rest in the private network secret. The hybrid blockchain system is extremely flexible and allows users to easily join private blockchain using multiple public blockchains.. This improves the security and transparency of the blockchain network[4].

Applications of Blockchain

Blockchain technology's core characteristics include decentralization, transparency, immutability, and automation. These elements can be applied not only to cryptocurrency but also to many other various industries like financial services, industrial products, manufacturing, healthcare, etc.

I. Commercial Application of Blockchain

A. Cryptocurrencies : Cryptocurrency is a digital currency that uses blockchain technology to record and protect all transactions. Cryptocurrencies (such as Bitcoin) can be used as digital cash to pay for everything from everyday items to large purchases such as cars and homes. You can purchase via any of several digital wallets or trading platforms and digitally transfer them when you purchase the item. The blockchain records transactions and new owners. The appeal of cryptocurrencies is that everything is recorded in a public ledger and protected by cryptocurrencies. This ensures that all payments are irrefutable, time-stamped, and securely recorded[2].

Examples*:* Bitcoin, Ethereum, Litecoin, Ripple, etc.

B. Smart Contracts : A smart contract is a self-executing contract in which the content of a buyer and seller agreement is written directly into lines of code[7]. Smart contracts are computerized transaction protocols that implement contract terms. By using smart contracts, we can make transactions traceable, transparent and immutable. Ethereum-based smart contracts can be used to generate digital tokens to perform transactions. Using smart contracts, we can create a voting system where you can add and remove members, change voting rules, change the time of debate or change the majority rule[8].

C. NFTs : A non-fungible token is a unit of data that has been identified as unique and non-exchangeable. In short, they are digital assets. According to Rafferty, NFTs are revolutionizing the world of digital art and collectibles. "We use decentralization and the Ethereum blockchain to connect artists and streamers directly with fans, sell NFTs, receive donations from fans, and exchange rewards and donations for crypto token exchanges. "Creates", says Chantal Anderson. Founder and CEO of Reel Mood, a music and pop culture streaming network[6] [9].

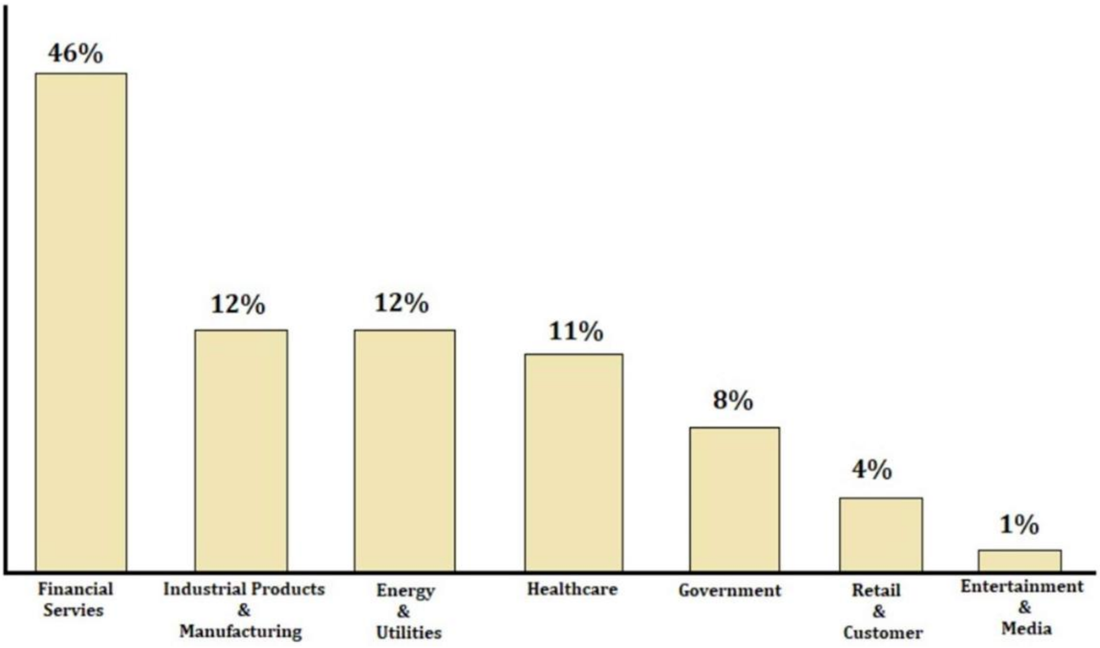
II. Blockchain Applications in Real World Industry

A. Healthcare : Blockchain has a wide range of applications in health care. It helps medical researchers reveal the genetic code by facilitating the secure transfer of patient medical records, managing the drug supply chain, and enabling the secure transfer of patient medical records. The blockchain for healthcare has many features, including- Protecting health data, managing EMR data, tracking illnesses and outbreaks, etc[7].

B. Banking : Blockchain allows untrusted syndicates to agree on subscription terms and eliminates the need for individuals to have to rely on agents for exchange. Blockchain can offer faster instalments and lower costs than banks by recording instalment decentralization[6]. Protection of stocks, bonds, voting resources, etc. is set in the open blockchain. This will increase the productivity of the capital sector. The features of blockchain in banking are: Cost savings, fastesttransactions, improved security[7].

C. Government : Blockchain-based digital governments can protect data, and reduce fraud, waste, and misuse while increasing trust and accountability. In the government's blockchain-based model, individuals, businesses, and governments share resources through a cryptographically protected distributed ledger. This structure eliminates single points of failure and essentially protects sensitive civil and government data[7].

D. Other Applications : Blockchain can be applied not only to cryptocurrency mining and smart contracts, then also to other areas such as energy and utilities, entertainment and media, education, elections, supply chainmanagement, IoT and insurance[7] [9].



Security Issues and Different Challenges

A. Majority Attacks or 51% Attacks : 51% of attacks on blockchain networks are aimed at forking double-payment blockchains[10]. The biggest security challenge for blockchain is 51% attacks. This is relatively fictitious, allowing an attacker to roll back a transaction in a sidechain or branch alternate block to hide information that occurs in the blockchain's mainchain. The possibility of mining a mining area by a miner depends on proof of work. To mine further blocks, miners cooperate and use more computing power to keep control of the network. If a person or group has more than 51% computing energy, that person or group of person can figure out the nonce. This helps miners determine which blocks are legal and which are not[10]. This helps attackers modify transactions that can trigger double-payment attacks, and also helps blockers prevent blockers from validating transactions. However, you don't necessarily have to get 51% hash power to put your blockchain network at risk. Double-payment attacks are possible with less than half the hash power, but this is very unlikely to succeed[10].

B. Eclipse Attack : In an Eclipse Attack, an invader attacks a distributed system to quarantine a explicit user, relatively than attacking the entire system. This kind of assault can happen in a distributed blockchain network because not every device can connect with all other computers in the network at the same time. Bitcoin nodes can only grip 8 departing connections and 117 arriving connections. The restricted outbound connection allows an attacker to insert malicious code to establish the connection. There are two sorts of Eclipse attacks that may happen on Ethereum. The first one an attacker can create an inbound PCP connection from Maxpeers to a malevolent node before the client establishes an outbound TCP connection. The second one is said to be due to the table. On reboot, the victim is more likely to take all outgoing nodes from the opponent's nodes[10].

C. **Forking Issue** : Another blockchain issue is forking. Branching an indirect branch within a *blockchain* is a provisional or enduring and can occur once the blockchain is split in dual. Forks differ depending on the blockchain type, architecture, and use case. Forks are divided into two categories:

a. **Hard Fork**: A hard fork is a *permanent* change in the protocol on blockchain system that device a single cryptocurrency into dual and authorizes previously invalid blocks and transactions. The reverse is also true. The network node uses the old version, which is no longer valid in the revised version. In the old chain, transactions to the new chain are invalid. Drillers have to update their previous version to the new version in order to trade on fork chains. Minor nodes must vote on the blockchain network to accept and incorporate version changes. Bitcoin, an instance of a hard fork in August, 2017 and the Bitcoin Cash wallet banned Bitcoin and Block transactions[10][11].

b. **Soft Fork**: A soft fork in the blockchain means a modification in the software procedure where previously acceptable blocks of transactions are unacceptable and out-dated nodes identify the innovative blocks of transactions as accepted. The fork is backwards well-matched. During a soft fork, most developer's requirement is to update their software version to apply the innovative rules. The computation power mandatory for innovative nodes is much advanced than for out-dated nodes. Blocks mined by out-dated nodes can't confirmed by innovative nodes, but innovative and out-dated nodes will work in the similar system[10] [11].

D. Application Bugs : All software-based solutions are developed by humans.
Human behaviour is not without mistakes. Therefore, human coding errors create a channel for threats in blockchain applications. Many blockchain appliances belong to open platforms and anybody can join these networks[11]. For example, one of the major MtGox attacks happened in 2014, with a reported loss of $ 600 million, and another Bitfinex attacks occured in 2016 at a cost of $ 65 million. In 2016, hackers utilized a coding flaw in a virtual business program called Decentralized Autonomous Organization (DAO) to steal a $ 55million Ether digital currency fund.

E. Regulatory Issue : To address this issue, "Cryptocurrency Regulations around the World" was published in 2018. Operation of blockchain applications around the world must be accompanied by many complex economic and political regulations, and there is no central bank policy for that. Like few countries ban Bitcoin and do not accept payments. Bitcoin is decentralised blockchain controlled by a particular individual and the central bank cannot control it. Digital currencies cannot also be used for payments via banking channels until the appropriate regulatory framework is in place. More research is needed before cryptocurrencies are adopted worldwide.

A total of 82 nations around the world have announced that cryptocurrencies are legal, but this legalization will support cryptocurrencies in a way that governments in these countries raise the issue of ease of use for blockchain applications. It does not mean that. More research is needed before cryptocurrencies are adopted worldwide.

F. Scalability Issue : The popularity of this new technology has grown significantly along with other IT − enabled services in various areas such as IoT, education, farming, health care, insurance, banking, etc. The processing power or speed of the blockchain depends entirely on its computation power. For comparison, Bitcoin processes 4.6 transactions per second, while VISA processes an average of 1,700 transactions per second. Blockchain-based transactions are very slow, which is a big problem for businesses and rely on a high-performance legacy transaction processing system. Lack of standards and interoperability in another blockchain platform is another challenge of adaptability. According to Deloitte, there are five things for widespread adoption of blockchain systems, which are ((i) Transaction speed, (ii) Standards and Interoperability, (iii) Improved technical feasibility, (iv) Support regulation, and (v) Expansion of the consortium[11].

a. Several significant scaling methods have been proposed to adopt blockchain technology, but each of them has limitations. One of the main problems is the sharing of databases. For blockchain development, database shares are processed, storage system computation and storage workloads are improved over peer-to-peer (P2P) networks, and each node can only process transactions through the corresponding shared database. increase. The main challenges in sharing databases on the blockchain are related to security and communication between the nodes of the network. This includes increasing the complexity of blockchain developers who require additional communication protocols[10].

b. However, various solutions have been proposed to solve these problems. Proof of Stake (PoS) is more efficient than Proof of Work (PoW). Two practical Byzantine Fault Tolerance (PBFT) nodes look for consensus in the presence of malicious nodes. Consensus Democratic Consensus; Tendermint is another consensus algorithm based on the Byzantine algorithm, which is very well scaled to handle about 10,000 transactions lips seconds.

G. Integration Issue : Modifying existing systems with new blockchain applications is another major challenge for the company in terms of cost, infrastructure setup, human thinking, and administrative expectations. Integrating new applications into existing legacy integrated systems is a major business challenge. When an organization needs to completely rebuild its legacy system in order for the two technologies to successfully integrate. Due to the lack of skilled blockchain developers, it is very difficult to recruit technical experts. Data loss and security breaches, on the other hand, can discourage companies from switching to blockchain-based applications. Data loss breaches can promote fraud, cause blockchain security problems, and become an obstacle to new application integration problems.

II. Conclusion

With its distributed platform and peer-to-peer network, blockchain, a undoubtedly new technology in the recent years, specifically in the area of information technology. For the various organizations that drive the progress of such dependable, secure, and unchangeable systems, blockchain has an important scope to note. There are problems that need to be solved, but as the new technical concepts of blockchain applications become more stable, some problems have improved. While there are quite a few benefits, there are some security concerns emphasized in this paper. Regulators need to report regulatory problems associated with this innovative technology. At the similar time, organizations need to be prepared to adopt blockchain technology that can decrease its effect on present systems.

References

[1]. Pierro, M. D. (2017). What is the blockchain? Computing in Science & Engineering.

[2]. Ashish Sharma & Dinesh Bhuriya (2019, January). Blockchain,Digital Currency.

[3]. Ishmaev, G. (2017). The blockchain era as a property organization. Metaphilosophy,(27February2018]).

[4]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K.(2016). What is the status of blockchain technology research? a thorough examination PLOS ONE, vol. 11, no. 10, e0163477.

[5]. Marco Iansiti, Karim R.Lakhani (2020). Technology and Operations Management Unit and theDigital Initiative.

[6]. Ali, M., Nelson, J., Blankstein, A., Shea, R., and Freedman, M. J. (2019). The BlockstackDecentralized Computing Network.

[7]. J. Zhang, S. Zhong, T. Wang, H.-C. Chao, J. Wang (2020, January), Blockchain-based Systems and Applications: A Survey, Journal of Internet Technology.

[8]. Z. Zheng, S. Xie, H. N. Dai, X. Chen, H. Wang (2018, January), Blockchain challenges and opportunities: A survey, International Journal of Web and Grid Services, Vol. 14, No. 4, pp. 352-375.

[9]. G. Peters, E. Panayi (2018), Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money,in Technology.

[10]. H. Wu, C. Tsai (2019, October). An intelligent agriculture network security system based on private blockchains, Journal of Communications and Networks, Vol. 21, No. 5, pp. 503-508.

[11]. M. Khan, K. Salah (2018, May).IoT Security: Reviews, Open Challenges and Blockchain Solutions, Next Generation Computing Systems, Vol. 82, pp. 395-411.