A Review on Blockchain and It's Security Issues and Challenges

-Shaili Trivedi
Master's degree in computer science
University of Massachusetts, Lowell

"We have elected to put our money and faith in a mathematical framework that is free of politics and human error"
-Tyler Winkelvoss

Abstract : ***One of the newest developing technologies in the realm of information technology is blockchain. Blockchain is a decentralized, traceable, temperamental, and trusted distributed database system run by multiple nodes. Blockchain is used not only in cryptocurrencies and electronic money, but also in other applications such as financial transactions, healthcare, insurance, IoT, data storage, etc., promising more functionality and greater resilience. However, important aspects and debates about blockchain security issues, challenges and policies are being raised around the world. Focusing on blockchain security issues, this review paper reviewed 3 to 4 research papers. The notable work of this review article concerns the concept of the blockchain the ecosystem, the partitioning of the blockchain, the implementation of the blockchain, and finally the security issues and challenges of the blockchain. This overview paper is useful for new research work on blockchain and security-related questions.***

I. INTRODUCTION

Blockchain refers to the blockchain technology that is used in cryptocurrencies like Bitcoin and Ethereum. It was originated by an Austrian cryptographer, who called it 'blockchain'. The name is derived from an analogy with a physical block, which is a unit of data. When Satoshi Nakamoto published his paper on bitcoin in 2008, it became the first application of blockchain. The same year, he created a new cryptocurrency called Bitcoin and introduced its blockchain technology for the first time. The goal of this technology was to develop a kind of digital money that could be sent instantly and securely without the assistance of a third party. A public record of everything that occurs on the network is what the blockchain was intended to be.

The blockchain was designed to be a public record of everything that happens on the network. Transactions are recorded as blocks, which are linked together with timestamps and bitcoin addresses. Each block contains two types of data: a hash of the previous block's header and a hash value of the current block. Without downloading the complete chain, it is feasible to validate a transaction using this combination of data. Blockchain uses a cryptographic hash function to create a linked list of transactions from the genesis block. The chain is secured by a consensus protocol which ensures that every node on the network has the same copy of all previous blocks, making tampering with data impossible.

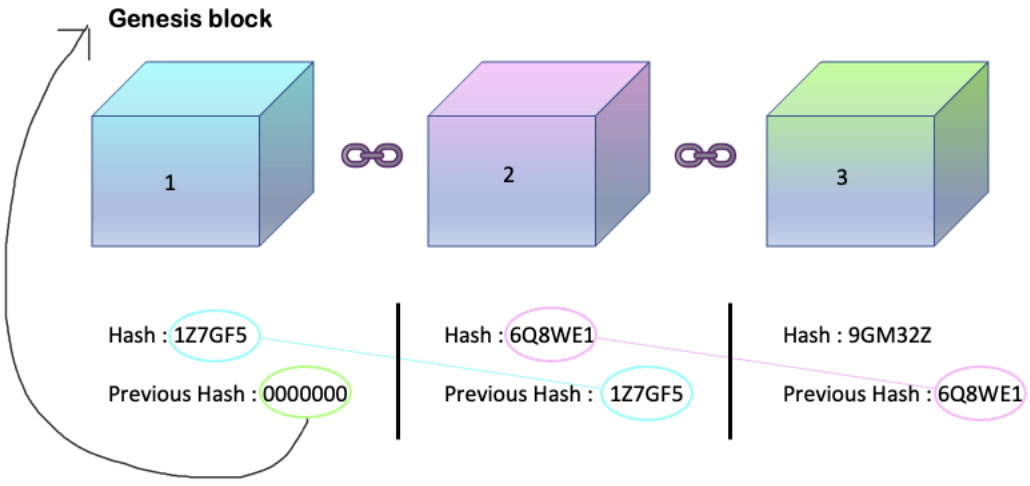

Fig 1 : Genesis and Blockchain

Blockchain works on a distributed ledger system where all the transactions are recorded publicly and permanently. The ledger has three main components: blocks, chains, and miners. Blocks contain transactions and miners validate those transactions by solving complex mathematical problems using resources like CPU or GPU power. Once validated, these blocks are added to the chain so that they can be further verified by other miners or nodes connected to them through the network.

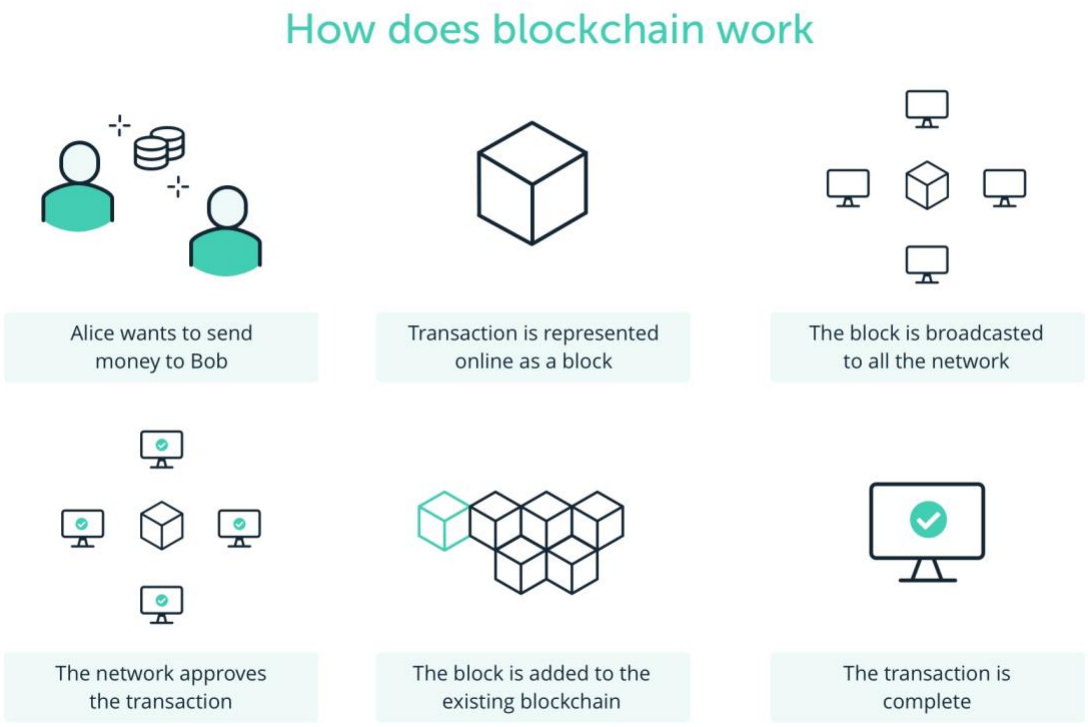

Fig 2 : Working of the Blockchain

II. CATEGORY OF BLOCKCHAIN

According to the nature of user and business needs, blockchain can be divided into public blockchain, private blockchain, Consortium blockchain and Hybrid blockchain. Following is the figure that explains it in short.

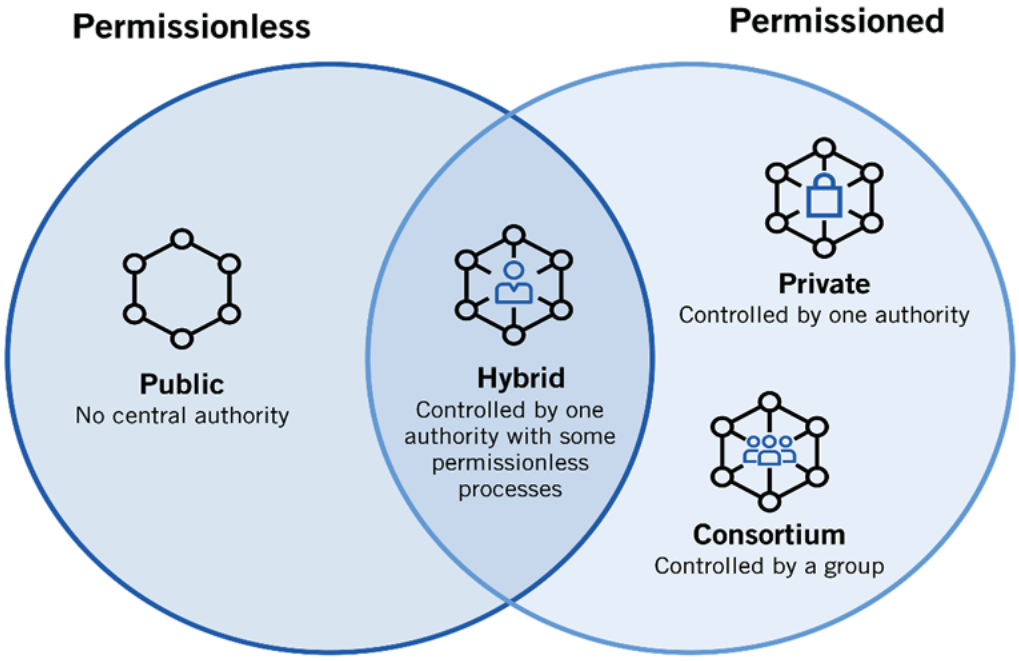

Fig 3 : Types of the Blockchain

A. Public Blockchain

A public blockchain is one that allows anybody to join and take part in the essential operations of the blockchain network. It is possible for anybody to view, publish, and audit the current activity on a public blockchain network, which contributes to the self-governed, decentralized aspect that is frequently highlighted when discussing blockchain technology. For example , Bitcoin, Ethereum, Dogecoin, Dash, Litecoin etc. Figure 3 shows the public blockchain.

B. Private Blockchain

The privacy blockchain can be distributed to an arbitrary extent, but writes are strictly controlled by a single organization. The advantage of a private blockchain is established by teams and participants can verify transactions internally. It carries the risk of security breach as a centralized system while the public blockchain is secured by a game theory incentive mechanism. However, the private blockchain will be more beneficial than other blockchains when it comes to state data privacy laws and other legal issues. For example, Quorum, Hyperledger Fabric, and R3 Corda. Figure 3 shows the private blockchain.

C. Consortium Blockchain

The Private Blockchain Consortium is controlled by an organization or group leader and does not allow all internet users to participate in the transaction verification process. The administrator of the consortium chain determines the user's access rights. A federated blockchain is faster, highly scalable, and provides more privacy for transactions than a public blockchain. For example, Ripple is one of the largest cryptocurrencies that support a rights-based blockchain network. Hyperledger is one of the best examples. Figure 3 shows the Consortium Blockchain.

D. Hybrid Blockchain

A hybrid blockchain is frequently described as a fusion of both public and private blockchain. It combines key elements of both public and private blockchains, and by combining the greatest features of both, it creates transactions and data that are private. Figure 3 shows the Hybrid Blockchain

III. APPLICATION OF BLOCKCHAIN

While the idea works extremely well for Bitcoin and other cryptocurrencies, but there are loads of other useful applications of blockchain technology.

A. ***Money Transfer :*** Compared to utilizing current money transfer services, adopting blockchain for money transactions may be cheaper and quicker. This is especially true for international transactions, which are sometimes costly and delayed.

B. ***Financial exchanges :*** Furthermore, investors enjoy more autonomy and security with a decentralized exchange since they are not required to deposit their money with the centralized authority. Blockchain exchanges provide quicker and more affordable transactions.

C. ***Smart Contracts :*** In a smart contract, the conditions of the agreement between the buyer and seller are directly encoded into lines of code, making it a self-executing contract. The agreements and underlying code are spread throughout a decentralized blockchain network. Transactions are traceable and irreversible, and the code regulates their execution.

D. ***Insurance :*** Customers and insurance companies may benefit from more transparency if smart contracts are used on a blockchain. Smart contracts can also expedite the payment-receipt procedure for claimants.

E. ***Real estate :*** In order, to transfer deeds and titles to new owners after real estate transactions, a ton of documentation is needed huge verify ownership and financial information. Real estate transactions may be documented using blockchain technology, which can offer a more accessible and safe way to verify ownership and transfer it. This can expedite processes, lessen paperwork, and result in cost savings.

F. ***Secure personal Information :*** By using private and public keys, people may control and own their data through blockchain transactions. It is not permitted for third-party intermediaries to collect and abuse data. Owners of personal data can regulate when and how a third party can access it if it is kept on the blockchain.

G. ***Securely share medical Information*** **:** Doctors and other medical professionals may be able to access accurate and current information about their patients by keeping medical data on a blockchain. It can really guarantee that patients who see many doctors receive the best care. Additionally, it helps expedite the process of retrieving medical information, enabling earlier treatment in some circumstances. Additionally, clinicians may quickly determine if a patient is insured, and their medical treatment is reimbursed if insurance information is included in the database.

H. ***Secure Internet of Things networks :*** To build tamper-resistant records of shared transactions, IoT enables devices connected to the Internet to transfer data to private blockchain networks. Without the requirement for centralized control and administration, IBM Blockchain lets your business partners to exchange and access IoT data with you. To avoid disagreements and foster confidence among everyone in the permissioned network, each transaction may be independently validated.

IV. SECURTITY ISSUES AND CHALLENGES

A. ***Forking issue :*** A fork, as used in the context of blockchain, is a technological event that takes place when a blockchain divides into two distinct branches. Up to the break, these two branches had a same transaction history. After that, they all move forward on their own, independently.

   i. ***Hard Fork :*** The term "hard fork" refers to the permanent modification of a blockchain network's protocols that separates a single coin into two and validates blocks and transactions that were previously invalid or the opposite. A transaction into the new chain is invalid into the old chain because network nodes are using an earlier version, which the new version does not accept. For transactions to be made on the fork chain, miners must replace their outdated software with the most recent version. The blockchain network requires the miner nodes to vote for the acceptance and integration of version modifications

   ii. ***Soft Fork*** : The term "soft fork" refers to a change in the software protocol for a blockchain where the older nodes accept the new transaction blocks as legitimate and the previously valid transaction blocks are rendered invalid. In a soft fork, most miners must upgrade their software to take advantage of the new regulations. While the old nodes' mined blocks won't be validated by the new nodes, both the new and old nodes will participate in the same network and demand significantly more computer power than the old nodes.

B. ***51 % Attack :*** A 51% assault (also known as a majority attack) is a possible attack on the integrity of a blockchain system when a single bad actor or group can seize control of more than half of the network's hashing power, potentially resulting in network instability. A single rogue user, or a team of bad users operating together, can override the network's consensus process and engage in fraudulent activity like double spending if they control more than 50% of the total network hashing rate for a blockchain. With adequate computing power, the attacker might deliberately change the sequence of transactions, preventing some or all of them from being verified.

C. ***Eclipse Attack :*** Instead of attacking the entire network, an eclipse attack targets a decentralized network to isolate a particular user or users and obscure its view of the other nodes. It eclipses its view of the other nodes after isolating.

D. ***Timestamp Dependence*** : When a smart contract uses the block, there is a timestamp reliance risk. It can be taken advantage of by malicious miners, who can quickly rearrange the timestamp.

E. ***Application Bugs :*** Every software-based solution is created by a person. The actions of a human are not error-free. Therefore, human code mistakes serve as the entry points for attacks to blockchain applications. The majority of blockchain apps are part of open platforms that anybody

F. ***Integration Issue :*** Another significant obstacle for the firm is replacing the current system with a new blockchain application in terms of cost, infrastructure setup, employee mentality, management expectations, etc.

V. CONCLUSION

Due to its decentralized platform and peer-to-peer network, the blockchain is without a doubt a developing technology in recent years, particularly in the sphere of information technology. There is a significant and exceptional potential for blockchain in many businesses, which will promote the creation of such a dependable, secure, and immutable system in the future. While there are still concerns that need to be resolved, some of them have already been handled as the blockchain application's new technology idea becomes more reliable. Despite having a large number of benefits, it has various security weaknesses that have been emphasized in this article. The regulator must handle the related regulatory concerns for this cutting-edge technology, and companies must be prepared for the implementation of blockchain technology, which might lessen the system's effect.

REFERENCES

[1] https://efaidnbmnnnibpcajpcglclefindmkaj/https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[2]https://efaidnbmnnnibpcajpcglclefindmkaj/https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1482&context=jitim

[3] https://www.sciencedirect.com/science/article/pii/S2096720922000072

[4] https://builtin.com/blockchain/blockchain-applications

[5] https://www.fastcompany.com/90722111/5-blockchain-security-issues-and-how-to-prevent-them#:~:text=ROUTING%20ATTACKS,transmitted%20to%20internet%20service%20providers.

[6] https://www.geeksforgeeks.org/blockchain-forks/#:~:text=Soft%20Fork%3A%20when%20the%20blockchain,block%20at%20the%20same%20time

[7] https://dci.mit.edu/51-attacks

[8] https://cointelegraph.com/explained/what-is-an-eclipse-attack