GROWING SECURITY NEEDS: BLOCKCHAIN A SOLUTION

Hemant Swami[1], Mr. Pankaj Kumar[2]
[1]M.Tech Scholar, [2]Assistant Professor
Department of Computer Science and Engineering
Jaipur Institute of Technology- Group of Institutions, Jaipur (Raj)

Abstract: Transactions are recorded on the Blockchain and can be viewed by a variety of people. Blockchain also securely registers assets, making them permanently important for years to come. Blockchain gets rid of the need for trust in a transaction. The technology eliminates wait times for verification and can help with consistency and security when it comes to regulated negotiations, ensuring fair payments and more.

Keywords: Blockchain, Security, Secure Hash

1. INTRODUCTION

A blockchain is a digital record that contains records, or blocks. The blocks are linked and secured by cryptographic proofs. A computer scientist and physicist began working on the first prototype of blockchain technology in the early 1990s, aiming to secure digital documents. [1]

Satoshi Nakamoto generated the Bitcoin cryptocurrency system in 2008, which was inspired by cryptographers such as Dave Bayer and Hal Finney. It is sometimes referred to as the first cryptocurrency. [1]

Blockchain technology is where cryptocurrencies begin. The blockchain usually has a decentralized, distributed and public digital ledger that is responsible for keeping a permanent record (chain of blocks) of all previously confirmed transactions. Bitcoin is a borderless currency that operates without the need of a third party intermediary. Transactions are verified by decentralized nodes and stored in a public ledger. [1]

The blockchain is resistant to tampering and fraud, making it a great candidate for data storage. Bitcoin is inherently unique because the blockchain cannot be altered and records cannot be tampered with. Bitcoin can solve the problem of falsified data, as all Bitcoin transactions are fixed within its blockchain - once a transaction is made and accepted by the network, it's permanently recorded within. Bitcoin also means less paperwork and automation is needed for business transactions. [2]

Bitcoin's blockchain is a Byzantine fault tolerant system. Essentially, this means that the bitcoin network can operate continuously as a distributed network even if some of the node’s present dishonest behavior or inefficient functionality.

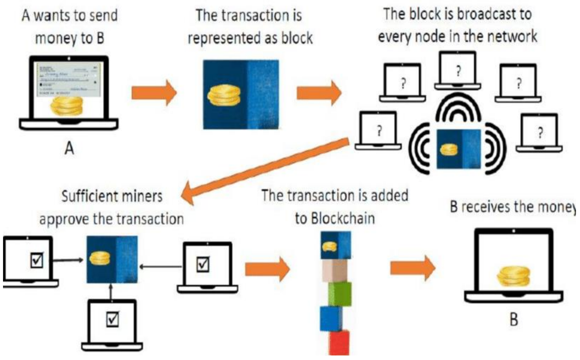
A wants to send money to B
The transaction is represented as block
The block is broadcast to every node in the network
A
Sufficient miners approve the transaction
The transaction is added to Blockchain
B receives the money
B

Fig 1. Blockchain Concept

This was made possible with Bitcoin's Proof of Work consensus algorithm, which is an essential part of the mining process. Blockchain technology can also be implemented in other areas, such as healthcare, insurance, and supply chain. Blockchain technology was designed to operate as a shared registry and is typically used for decentralized systems. However, blockchain may also be deployed for centralized databases to provide integrity and reduce operational costs. [2]

2. WORKING OF BLOCKCHAINS

Blockchain is a technology that is fairly new, and even still in the early stages of development. There are so many applications for this that we're only just beginning to figure out what it can do. The biggest problem is figuring out how to monetize it, but there are all types of Blockchain solutions being made. [3]

Blockchain is a combination of following technologies:

- Cryptographic keys: Blockchain technology is used to secure digital identity, the most important aspect of Blockchain technology. Digital signature authorizes and controls transactions for individuals who hold two keys: a private key and a public key. [3]

- Digital Signature: A digital signature is a unique sequence of numbers, used to prove that you are the owner of an identity. Individuals on the blockchain network act as authorities and use this digital signature to approve transactions. These transactions are verified by mathematic equations, which allow for successful transactions between connected parties. In summary, Blockchain users use cryptography keys to perform different types of digital interactions over the peer-to-peer network. [4]

3. TYPES OF BLOCKCHAIN

There are four different types of blockchains. They are as follows:

- Private Blockchain Networks: This type of blockchain allows companies to customize the accessibility and security parameters, mainly for private networks that are not open to the public. Private Blockchains are better for closed networks, like those for private businesses. These networks allow for customization and security options such as the accessibility of the network and its authorization. [5]
- Public Blockchain Networks: Cryptocurrencies like Bitcoin and other cryptocurrencies started because of public blockchains, which played a role in popularized distributed ledger technology. These blockchain, among other things, help eliminate security issues and making sure that data is dispersed rather than being centralized. With DLT, there is mechanisms for verifying data that comes from the network; two currently popular consensus methods are proof of stake and proof of work [5]
- Permissioned Blockchain Networks : Hybrid blockchains, also known as permissioned blockchains are the best of both worlds. These blocks allow authorized individuals to participate in the network and transactions. Organizations typically set up these types of blocks for better structure when assigning who can participate in the network. [6]
- Consortium Blockchains: Permissioned blockchains have both public and private components. With a consortium blockchain, multiple organizations can manage a single network of this type. This is because it's more difficult to set up. What are the benefits of consortium blockchains? Security is high, and collaboration between organizations is key for these types of blockchains. [6]

4. BLOCKCHAIN SECURITY

Within the blockchain community, it is often said that the technology can't be hacked. But 51% attacks allow threat actors to "gain control over more than half of a blockchain's compute power and corrupt the integrity of the shared ledger". With this method, security professionals must treat blockchain as a useful tool, not always the answer to all problems. In order to commit a 51% attack, a single miner needs 51% of the hash power in order to produce false data for the blockchain. [7]

Private blockchains might be more appropriate for enterprises who are concerned about the confidentiality of the information moving through the network. The two main types of blockchain, public and private, offer different levels of security. Public blockchains "use computers connected to the public internet to validate transactions and bundle them into blocks to add to the ledger. … Private blockchains, on the other hand, typically only permit known organizations to join." [8]

Public blockchains are designed around the principle of anonymity to protect user identity. This function would allow anyone to read transaction records, whereas a private blockchain would keep transactions anonymous and secure. [9]

Blockchain technology is growing fast, and it is changing our world. As developers make new apps, security should be their top priority. They should use a number of methods for testing and making sure that the app doesn't have any weaknesses before releasing it; these include security risk assessments, creating threat models, and performing static code analysis. [10]

5. BENEFITS OF BLOCKCHAIN

- Enhanced security: Blockchain technology can protect the privacy of unique data by like a digital ledger. The blockchain network makes data more secure and tamper-proof because it's spread across multiple computers. Blockchain makes it difficult for hackers to view data and transaction records because the data is stored on a decentralized network of computers and not one single server.[11]
- Greater transparency: Blockchain is a better, more secure solution to storing data because it uses a distributed ledger system. Blockchain's transparent transactions eliminate fraud and multiple databases are not needed because blockchain uses the same data in multiple locations. [11]
- Instant traceability: Blockchain tracks assets as they move from one location to the next, providing detailed information related to sourcing and distribution. For example, customers are able to find information on where something was manufactured and any potential issues that arose during its production. This also provides a more transparent method of determining what to buy. [12]
- Increased efficiency and speed: Blockchain streamlines traditional time-consuming paper-heavy processes by removing the need to use third-party mediation. Blockchain can store transaction documentation, eliminating the need to exchange paper. Blockchain makes clearing and settlement more efficient because there is no need for reconciling ledgers. [12]
- Automation: You can have transactions done automatically with pre-specified conditions like smart contracts. They can increase efficiency and speed up the process. With the use of a smart contract, you can automate your transactions and processes. Pre-specified conditions are triggered when certain events happen and the next part of the process is automatically carried out. This eliminates the need for third parties to confirm that terms were met or for humans to intervene in any way. For example, insurance claims can be processed without the need for human intervention by providing all necessary documentation. [13]

6. CONCLUSION

Blockchain is immutable, which provides many opportunities for companies. It's not possible to change any information that is on the blockchain. Blockchain technology offers transparency, and is useful for a range of purposes in society. Some public blockchains are designed to offer greater transparency, which can be carried forward into any business process.

REFERENCES

[1] W. Meng E. W. Tischhauser Q. Wang Y. Wang and J. Han "When Intrusion Detection Meets Blockchain Technology: A Review" IEEE Access vol. 6 pp. 10179-10188 2018.

[2] T. Golomb Y. Mirsky and Y. Elovici "CIoTA: Collaborative IoT Anomaly Detection via Blockchain" Network and Distributed Systems Security Symposium (NDSS) 2018.

[3] R. Jain Extending Blockchains for Extending Blockchains for Risk Management Risk Management and Decision Making and Decision Making [online] Available: https://www.cse.wustl.edu/~jain/talks/ftp/pbc_ibf.pdf

[4] T. Salman R. Jain and L. Jupta "probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making" The 9th IEEE Annual Ubiquitous Computing Electronics &amp; Mobile Communication Conference November 2018.

[5] K. Yamada and H. Saito "What's So Different about Blockchain? — Blockchain is a Probabilistic State Machine" IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW) pp. 168-175 2016.

[6] F. Gai B. Wang W. Deng and W. Peng "Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network" Database Systems for Advanced Applications 2018.

[7] The official GoChain client gochain [online] Available: https://gochain.io.

[8] D. Qin C. Wang and Y. Jiang "RPchain: A Blockchain-Based Academic Social Networking Service for Credible Reputation Building" International Conference on Blockchain 2018.

[9] J. Yu D. Kozhaya J. Decouchant and P. E. Verissimo "RepuCoin: Your Reputation is Your Power" IACR Cryptology ePrint Archive 2018 2018.

[10] C. Tang L. Wu G. Wen and Z. Zheng "Incentivizing Honest Mining in Blockchain Networks: A Reputation Approach" IEEE Transactions on Circuits and Systems II: Express Briefs 2019.

[11] M. Pilkington "Blockchain technology: principles and applications" Research handbook on digital transformations 2016.

[12] M. Mettler "Blockchain technology in healthcare: The revolution starts here" 2016 IEEE 18th International Conference on e-Health Networking Applications and Services (Healthcom) 2016.

[13] K. Christidis and M. Devetsikiotis "Blockchains and Smart Contracts for the Internet of Things" IEEE Access vol. 4 pp. 2292-2303 2016.