# DIGITISED AND DECENTRALIZED BLOCKCHAIN TECHNOLOGY

**[1] D.J. Santosh Kumar, [2] P. Sri Guru Charan, [3] U. Manisha, [4] S. Gayatri, [5] P. Sujith Varma**

[1]Assistance Professor, [2]Student, [3]Student, [4]Stuent, [5]Student[1]Computer Science and Engineering
[1]Lendi Institute of Engineering and Technology, Vizianagaram, India

**Abstract** - Current online payment systems rely heavily on financial institutions as trusted intermediaries, which introduces security vulnerabilities and risks associated with transaction reversibility. In response, we propose a novel, fully peer-to-peer electronic cash system that enables direct payments between parties, bypassing the need for intermediaries. Our system employs cryptographic proof to ensure transaction security and mitigate the risk of double spending. Transactions are timestamped and incorporated into a chain of proof-of-work, creating an immutable transaction record. This approach enhances security, eliminates the necessity for extensive documentation, and reduces costs. By harnessing the power of blockchain technology and peer-to-peer networks, our solution aims to transform online transactions, rendering them secure, efficient, and decentralized.

**Index Terms** - Block Chain, decentralization, peer to peer, Security, Proof-of-work, Transactions, Cryptography, Ledger, Distributed Network, Consensus, Smart Contracts.

## I. INTRODUCTION

In today's online payment systems, we often rely on banks and other financial institutions to handle our transactions. While this setup generally works well, it does come with some downsides. For example, it can leave our transactions vulnerable to security breaches and other issues that might affect whether or not a transaction can be reversed. To address these concerns, we're proposing a new way of handling online payments—a system that allows people to pay each other directly, without the need for banks or other middlemen.

Our system uses advanced technology to ensure that transactions are secure and that the risk of double spending is minimized. Each transaction is time-stamped and recorded in a way that makes it nearly impossible to alter. This not only makes transactions more secure but also simplifies the process and reduces costs. Our system is based on blockchain technology and peer-to-peer networks, which means that transactions can be processed quickly and efficiently, without the need for a central authority. We believe that this approach has the potential to transform online transactions, making them more secure, efficient, and accessible to everyone.

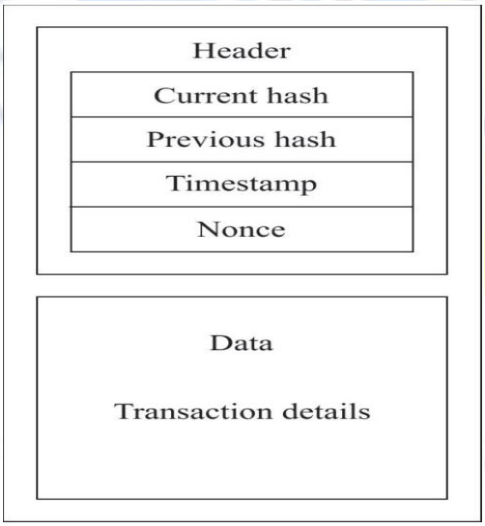


Fig.1 Structure of a Block

## II. LITERATURE SURVEY

**2.1 Decentralized Consensus for Edge-Centric IoT: A Survey** - This survey paper by Qinghua Lu et al. provides an overview of decentralized consensus mechanisms for the Internet of Things (IoT). It discusses various consensus algorithms and their suitability for edge-centric IoT environments.

**2.2 A Survey of Blockchain Consensus Mechanisms** - This survey by Arshpreet Kaur et al. provides an overview of consensus mechanisms used in blockchain systems. It discusses various algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT).

**2.3 Blockchain Technology: Principles and Applications** - This book by Marc Pilkington provides a comprehensive overview of blockchain technology, covering its principles, applications, and potential impact on various industries.

**2.4 Blockchain-Based Electronic Voting Systems: A Survey** - This survey by Marcin Andrychowicz et al. discusses the use of blockchain technology for electronic voting systems. It provides an overview of existing systems and their challenges.

**2.5 Decentralized Applications: Harnessing Bitcoin's Blockchain Technology** - This book by Siraj Raval explores the concept of decentralized applications (DApps) and how they can be built using blockchain technology.

**Blockchain: Blueprint for a New Economy** - This book by Melanie Swan provides an in-depth look at blockchain technology and its potential to disrupt various industries, including finance, healthcare, and supply chain management.

## III. ARCHITECTURE AND WORK FLOW

The electronic payment system based on blockchain technology operates through a network of peers, each participant possessing a unique identifier and cryptographic key pair for transaction signing. Transactions are initiated when a peer wishes to transfer coins to another peer. This process involves compiling transaction details such as sender, recipient, and amount, which are then signed with the sender's private key. Validation of transactions is conducted by other peers in the network, who verify the transaction's signature, check the sender's coin balance, and ensure the transaction is not a double spend. Valid transactions are added to a pool of pending transactions, from which miners select transactions to include in a new block. Miners compete to solve a proof-of-work puzzle, with the first miner to solve it adding a new block to the blockchain. Other miners verify the new block by confirming the proof-of-work and validating the transactions, after which the block is appended to their copy of the blockchain. This process ensures consensus among network nodes, making it computationally challenging for malicious nodes to manipulate the blockchain. The decentralized nature of the system is maintained through peer-to-peer networking, which facilitates the broadcasting of transactions and blocks. Security measures, such as SHA-256 hashing and cryptographic signing, ensure the integrity and authenticity of transactions, making the system secure, transparent, and resistant to fraud.

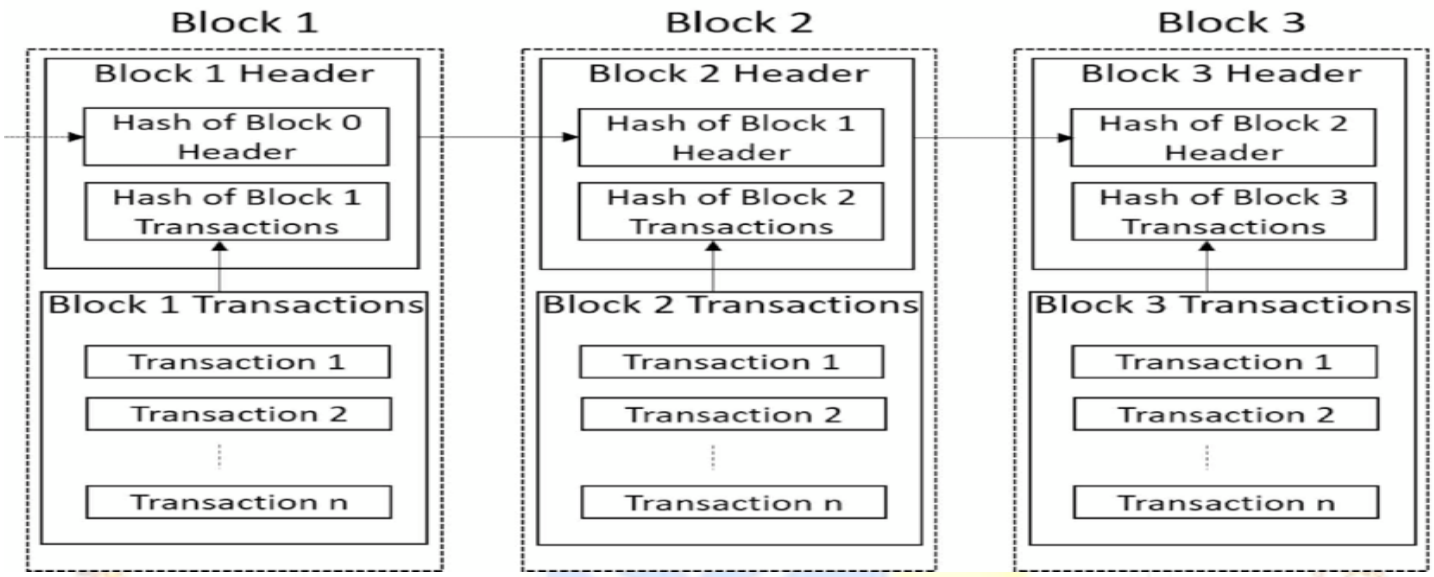


Fig.2 Architecture of block chain

In the context of the electronic payment system based on blockchain technology, the primary algorithm required is SHA-256 (Secure Hash Algorithm 256-bit). This algorithm serves several critical functions within the system:

**Hashing Transactions:** SHA-256 is used to hash each transaction. This process creates a unique, fixed-size output that serves as a digital fingerprint for the transaction. The hash ensures the transaction's integrity and provides a way to verify its authenticity.

**Generating Cryptographic Keys:** Public and private keys used for cryptographic operations, such as signing transactions, are generated using SHA-256. The algorithm ensures that the keys are generated securely and are resistant to attacks.

**Securing the Blockchain:** SHA-256 is a fundamental component of the proof-of-work algorithm, which is used to secure the blockchain. Miners compete to solve a cryptographic puzzle based on SHA-256, and the first miner to solve it adds a new block to the blockchain. This process ensures that adding new blocks is computationally intensive, making the blockchain resistant to tampering and fraud.

The SHA-256 algorithm processes input data in 512-bit blocks to produce a 256-bit hash value. Here's a simplified mathematical representation of how SHA-256 works, using a transaction T as an example:

1. **Padding:** The input message (transaction T) is padded to a length that is a multiple of 512 bits. Padding includes a single '1' bit followed by '0' bits and the length of the original message in binary (padded to 64 bits).
2. **Message Block Splitting:** The padded message is divided into blocks of 512 bits each.
3. **Initial Hash Values:** SHA-256 uses eight initial hash values (H0 to H7), which are 32-bit words derived from the fractional parts of the square roots of the first 8 prime numbers.
4. **Message Schedule:** For each message block, a message schedule array (W[0..63]) of 32-bit words is created. The first 16 words are filled with the 32-bit words of the block, and the remaining 48 words are calculated based on a formula using the previous words.
5. **Compression Function (Ch):** The compression function is applied to each message block, updating the hash values.
6. **Final Hash:** After processing all blocks, the final hash value is the concatenation of the updated hash values H0 to H7.

Mathematically, the SHA-256 algorithm can be represented as follows (simplified for illustration

**Padding:**

Let M be the padded message.
Let L be the length of the original message in bits.
M = original message || 1 || 0^k || L, where k is the number of '0' bits needed for padding.

**Message Block Splitting:**

M is split into blocks M[0], M[1], ..., M[n].

**Initial Hash Values:**

H0 = 0x6a09e667
H1 = 0xbb67ae85
H2 = 0x3c6ef372
H3 = 0xa54ff53a
H4 = 0x510e527f
H5 = 0x9b05688c
H6 = 0x1f83d9ab
H7 = 0x5be0cd19

**Compression Function (Ch):**

For each block M[i], update the hash values:
Calculate the message schedule array W[0..63].
Initialize working variables a, b, c, d, e, f, g, h with the initial hash values.
Perform 64 rounds of operations using bitwise functions, addition modulo 2^32, and logical functions.

**Final Hash:**

The final hash value is the concatenation of the updated hash values H0 to H7 after processing all blocks.

After the SHA-256 algorithm processes transactions and blocks in a blockchain, the Proof of Work (PoW) algorithm is implemented to enhance the blockchain's security and facilitate consensus among network participants. PoW works as follows:
The Proof of Work (PoW) algorithm is a consensus mechanism used in blockchain networks to achieve agreement on the state of the blockchain. In the context of your project, which aims to create a purely peer-to-peer electronic cash system, PoW plays a crucial role in securing the network and preventing double-spending.
Here's how PoW works, along with some mathematical representations:
**Mining**: In PoW, participants in the network, known as miners, compete to solve a computationally intensive puzzle. The first miner to solve the puzzle gets the right to add a new block to the blockchain and is rewarded with newly minted coins and transaction fees.
**Puzzle**: The puzzle that miners solve is typically a hash puzzle. Miners are required to find a hash value that meets certain criteria, such as being lower than a target value. The hash function used, such as SHA-256, ensures that finding a valid hash value requires significant computational effort.
**Difficulty**: The difficulty of the puzzle is adjusted regularly to ensure that new blocks are added to the blockchain at a roughly constant rate, regardless of changes in the total computational power of the network.
Mathematically, the PoW algorithm can be represented as follows:
Let H be a hash function (e.g., SHA-256).
Let D be the current difficulty level.
Let N be the nonce, a number that miners increment in their attempts to find a valid hash.
Let T be the target value that a valid hash must be less than.
Let M be the message or block data that is being hashed.
The goal of the miner is to find a nonce N such that:
$H(M \| N) < T$,
where || denotes concatenation. This inequality is checked by hashing the concatenation of the message M and the nonce N and comparing the result to the target value T. By requiring miners to expend computational effort to find a valid hash, PoW ensures that adding new blocks to the blockchain is resource-intensive, making it economically infeasible for an attacker to manipulate the blockchain.
After the Proof of Work (PoW) algorithm secures the blockchain and establishes consensus on transaction order, the final step involves adding the validated block to the blockchain. This process begins with the successful miner broadcasting the new block to other network nodes for verification. Each node independently validates the block by checking the PoW solution and verifying the transactions. If the majority of nodes reach a consensus that the block is valid, it is added to the blockchain, ensuring all nodes have a consistent view of the ledger. This cycle of mining, validating, and adding blocks continues, ensuring the blockchain's integrity and security. Miners are incentivized to participate through rewards of newly minted coins and transaction fees, ensuring the network's ongoing operation and security without the need for a central authority.

## IV. CONCLUSIONS

Our proposed system revolutionizes electronic transactions by eliminating the need for trust. We began by establishing a framework where coins are represented by digital signatures, ensuring secure ownership control. However, to address the critical issue of double-spending, we introduced a novel approach. Through a peer-to-peer network utilizing proof-of-work, we create a public transaction history that is virtually immutable. This system becomes increasingly difficult for malicious actors to alter, as long as honest nodes collectively control the majority of the network's computational power. This network operates seamlessly with minimal coordination among nodes, making it highly robust. Nodes within the network remain anonymous, as messages are distributed without specific routing, relying solely on best-effort delivery. This unstructured simplicity ensures the system's efficiency and resilience, paving the way for a more secure and reliable electronic payment ecosystem.

## V. REFERENCES

[1] Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.
[2] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
[3] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.
[4] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In IEEE International Congress on Big Data (Big Data Congress) (pp. 557-564). IEEE.
[5] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
[6] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
[7] Casey, M. J., & Vigna, P. (2018). The Truth Machine: The Blockchain and the Future of Everything. St. Martin's Press.
[8] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.
[9] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance. CRC Press.
[10] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, 14(4), 352-375.
[11] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smo lander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PloS one, 11(10), e0163477.