IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BITCOIN: BLOCKCHAIN TECHNOLOGY

[1] Darshana Bhamare , [2] Kirti Randhe,[3] Reshma Sonar

[1] Asst. Prof. CSE Department,

[2] Asst. Prof AI&ML Department,[3] Asso.Prof AI&MLDepartment

[1,2,3] ISBM College of Engineering, Nande, Pune

I. ABSTRACT

In recent times, blockchain, the foundational technology powering Bitcoin, has attracted extensive attention as an immutable ledger enabling decentralized transactions. The proliferation of blockchain-based applications across diverse domains, such as finance, reputation systems, and IoT, has been remarkable. However, challenges related to scalability and security persist and demand resolution. This paper presents a comprehensive overview of both blockchain technology and Bitcoin's transformative impact. It begins by introducing blockchain architecture and various consensus algorithms utilized in different blockchains. Additionally, the paper outlines technical challenges and recent advancements in the field. Furthermore, we delve into the multifaceted outcomes and research directions inspired by Bitcoin's emergence as a billion- dollar economy. By combining insights from both blockchain and Bitcoin, this survey provides a holistic understanding of their significance and potential future trends.

Index Terms – Blockchain Technology, Bitcoin, Internet of Things (IoT), Data storage, internet.

II.INTRODUCTION

Bitcoin and blockchain technology have emerged as transformative forces, reshaping the landscape of computer science and information technology. The concept of decentralized money had long been a theoretical notion until 2008 when Satoshi Nakamoto's groundbreaking paper introduced Bitcoin and blockchain technology, making it a practical reality.

Despite the controversies surrounding Nakamoto's identity, there is no denying the revolutionary impact of their work. Users now have the freedom to explore and utilize this innovation in various ways. Some individuals are developing applications to address societal challenges, while others are investing in cryptocurrency projects or trading based on the market fluctuations.

This paper introduces blockchain and cryptocurrencies. It delves into the history of decentralized digital money solutionsbefore Bitcoin and then delves into the core functionalities of Bitcoin and Ethereum, which dominate the cryptocurrency market capitalization. As with any emerging technology, limitations and challenges have also surfaced, and we explore these in detail.

III. EARLY CONCEPTS OF DECENTRALIZED DIGITAL CURRENCIES

The concept of digital currency has been around for some time, but recent successful implementations have brought it to the forefront. Chaum presented an idea of untraceable electronic mail and anonymous correspondents based on public key cryptography [1]. Law et al. proposed electronic cash with public key cryptography for use with banks as central trust authorities [2].

Other researchers explored using computational power as an asset with actual value in the form of proof-of-work systems. For combatting junk mail, Dwork and Naor introduced a system requiring a computation of a hard pricing function [3]. The concepts of b-money, reusable proof-of-work, and bit gold also represented

ideas of using computational power as valuable assets [4] [5] [6].

Vishnumurthy et al. tackled the problem of resource sharing in P2P networks with the KARMA system, where nodes' contributions and consumptions affected their karma score [8]. However, these approaches either relied on trusted parties like banks or didn't entirely address the double-spending problem, particularly crucial in decentralized systems like cryptocurrencies [7].

Quorum systems were introduced as a potential solution, where voting by the majority of nodes in the network determinedthe control of information [9] [10]. Nonetheless, this approach remains susceptible to Sybil attacks, where hostile nodes manipulate peers with false information to gain control [11].

In summary, the journey of digital currency has seen several breakthroughs and challenges, with researchers continuouslyexploring new methods to improve security, trust, and decentralization in this evolving domain.

IV. BITCOIN AND BLOCKCHAIN TECHNOLOGY

A. Bitcoin essentials

In his renowned work, Satoshi Nakamoto provided a groundbreaking solution to the challenges faced by digital currency implementation, particularly the double-spending problem [12]. While Nakamoto's true identity remains speculative, it is known that he was actively involved in the Bitcoin project until 2010, after which he handed it over to the community for further development [7]. His proposed system featured a peer- to-peer distributed timestamp server, generating computational proof for the chronological order of transactions [12]. An electronic coin was defined as a chain of digital signatures, with each transaction consisting of a digitally signed hash of the previous transaction and the public key of the next owner (Fig. 1)[12]. The private key was used for transaction signing, while the public key served for verification, stored in a wallet that could be software, hardware, or online-based.

The Bitcoin ledger operates as a state transition system, comprising a state that represents the ownership status of all existing bitcoins and a state transition function in the form of transactions. The outcome of this function is a new state [13]. Through this process, the sender's and recipient's states are modified if the senderpossesses sufficient bitcoins to carry out the transaction; otherwise, an error occurs.

B. Bitcoin transactions

Each transaction in the blockchain is uniquely identified by its hash value, comprising a transaction identifieralong with sets of inputs and outputs [7]. Notably, each output of a transaction can only be used as an input once across the entire blockchain, preventing the double-spending problem within the network. Uniqueness is maintained through the concept of Unspent Transaction Outputs (UTXOs) for unreferenced outputs and Spent Transaction Outputs (STXOs) for previously referenced ones. Transactions can have multiple inputs, allowing the combination of smaller amounts of coins being transferred, and up to two outputs. These outputscan represent amounts sent to other parties or change sent back to the sender [12].

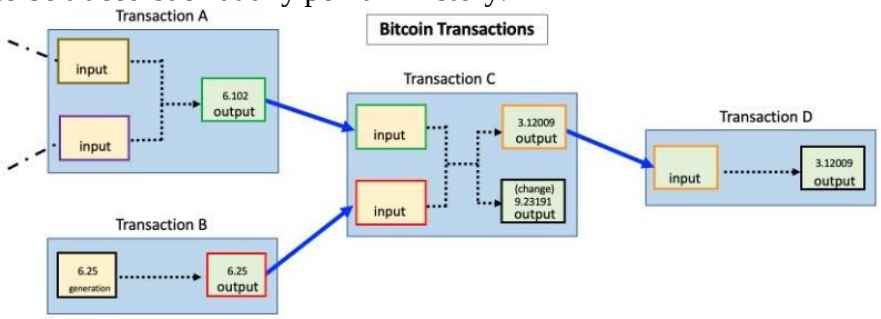
The Bitcoin distributed ledger contains records of all transactions and ownerships in the network. Every nodein the peer-to-peer network maintains a copy of this ledger [13]. When a user wants to send coins to another user, they announce the transaction publicly, and the network verifies its accuracy. However, some users may attempt to manipulate the network by issuing multiple transactions for the same coins (double-spending problem). Additionally, a user can set up multiple instances to confirm their initial intent, leading to a Sybil attack.

C. Proof-of-work and blockchain

In the Bitcoin network, potential issues are mitigated, if not entirely prevented, by requiring each node to provide proof-of-work when verifying transactions. This demand entails heavy computations to demonstrate their validity as network members. As long as the collective computational power of honest nodes surpassesthat of attackers, the system maintains consistency, ensuring legitimate transactions can occur [7], [12].

To declare a block in the blockchain, a set of transactions, the hash of the previous block, and a nonce are combined. A timestamp server creates a hash of the block and publicly announces it,

proving that the data inside the block existed at the time of hashing. The timestamp server also verifies that the block's timestamp is greater than that of the previous block in the chain and less than two hours into the future. These blocks are then linked together in a chain, forming the blockchain (Fig. 2) [12]. A key characteristic of the blockchain is its traceability, allowing transactions to be traced back at any point in history.



Bitcoin's proof-of-work hashing scheme is similar to Hashcash [14] and relies on the SHA-256 hash function[15]. The proof-of-work process involves incrementing a nonce in the block until the hash value begins with the required number of zero bits. Once completed, the computations cannot be undone without redoing the work. If a malicious attacker attempts to change a block, all subsequent blocks would have invalid hashes. To make alterations, the attacker would need to overcome the voting power of the majority of honest nodes,creating a race problem.

Transactions within a block are hashed in a Merkle tree [16], [17], a binary tree with multiple leaf nodes, and the root of the leaf nodes becomes a hash of its children. The Merkle tree is essential for long-term maintainability, as any inconsistency in the tree will be reflected somewhere in the chain [13]. This approach helps save storage space on nodes, as only the root hash included in the block header is kept. The current size of the Bitcoin blockchain is approximately 144.8 GB [18]. After transactions are included and verified in a block, all hashes in the tree, except the root hash, are discarded. This pruning process aids in reducing blockchain size and storage requirements.

D. Bitcoin network and mining

The first transaction in a block creates a new coin, owned by the block's creator, which incentivizes nodes to verify transactions and put coins into circulation since no central authority issues them. This transaction is called a coinbase transaction [12]. The network aims to produce one block approximately every ten minutes[13]. As computational power increases over time, the block time remains constant by gradually increasing the difficulty of generating new blocks.

In the Bitcoin network, new transactions are broadcasted to all nodes, which gather transactions into a block and work to find proof-of-work. Once found, the block is broadcasted to the network. Nodes only accept a block as valid if all transactions within it are correct and unspent. If accepted, the chain continues by creatingthe next block and adding the previous block's hash to it [12].

Nodes are rewarded for adding new blocks to the blockchain through mining [7]. Initially, the block reward was set to 50 coins (50 BTC) and halves every 210,000 blocks. This halving process will continue until the reward drops below one satoshi, which is the smallest unit of Bitcoin equal to 10-8 BTC [7].

In a distributed decentralized system, multiple nodes may broadcast the same block almost simultaneously but with different transactions, leading to a fork and network inconsistency. However, the network always follows the longest chain, and over time, a consensus is reached, invalidating the chains resulting from forks[7].

E. Bitcoin scalability problem

Bitcoin faces severe scalability challenges with its 1MB block size. This limited size allows for fewer than seven transactions per second (tps) [19]. In comparison, Visa's payment network achieved a rate of 47,000 tps during the 2013 holidays and currently processes hundreds of millions of transactions per day [20]. To achieve such throughput on the Bitcoin network with a 1MB block size, assuming each transaction is 300 bytes in size, it would require 8GB per Bitcoin

block every ten minutes, resulting in over 400TB of data per year [19]. This would centralize the network towards nodes with substantial storage capacities, contradictingthe decentralized nature of Bitcoin and blockchain.

To address this issue, various solutions have been proposed, leading to both soft and hard forks of Bitcoin. Asoft fork is a backward-compatible change that allows old software to recognize newly created blocks as valid. In contrast, a hard fork introduces a new rule to the network, making the old software incapable of recognizing new blocks [21]. These forks are part of the ongoing efforts to enhance Bitcoin's scalability andadapt to evolving needs.

V. CONCLUSION

Bitcoin stands as the most renowned and valuable cryptocurrency today. Built upon blockchain technology, it fosters a trust mechanism within a peer-to-peer network, driven by the consensus of the majority of nodes. This paper offers a concise historical overview of the initial phases of digital money implementation and the fundamental underpinnings of blockchain technology. Moreover, it delves into the most notable and widely embraced instantiation of blockchain, namelyBitcoin.

I. REFERENCES

[1] D. Chaum, “Untraceable electronic main, return addresses, and digital pseudonyms,” in Communications of the ACM,vol. 24, no. 2, pp. 84-88, February 1981

[2] L. Law, S. Sabett, and J. Solinas, “How to make a mint: the cryptography of anonymous electronic cash,” AmericanUniversity Law Review, vol. 46, no. 4, pp. 1131-1162, 1996

[3] C. Dwork and M. Naor, “Pricing via processing or combatting junk mail,” in 12th Annual International CryptologyConference, pp. 139- 147, 1992

[4] W. Dai, “B-money,” 1998, available at: http://www:weidai:com/bmoney

[5] H. Finney, “RPOW,” 2004, available at: http://nakamotoinstitute.org/finney/rpow/

[6] N. Szabo, “Bit Gold,” 2005, available at: http://unenumerated.blogspot.rs/2005/12/bit-gold.html

[7] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: a technical survey on decentralized digital currencies,” IEEECommunications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, March 2016

[8] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, “KARMA: A secure economic framework for peer-to-peerresourse sharing,” 1st Workshop on Economics of Peer-To-Peer Systems, 2003

[9] N. Szabo, “Secure property titles with owner authority,” 1998, available at: http://nakamotoinstitute.org/secure- property-titles/

[10] D. Malkhi and M. Reiter, “Byzantine quorum systems,” Distributed Computing, vol. 11, no. 4, pp. 203-213, 1998

[11] J. Douceur, “The Sybil attack,” in Proceedings of IPTPS '01 Revised Papers from the First International Workshopon Peer-to-Peer Systems, pp. 251-260, March 2002

[12] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” 2008, available at: https://bitcoin.org/bitcoin.pdf

[13] Ethereum Community, “A next-generation smart contract and decentralized application platform,” White Paper,available at: https://github.com/ethereum/wiki/wiki/White-Paper

[14] A. Back, “Hashcash – a denial of service counter-measure,” 2002, available at:http://www.hashcash.org/papers/hashcash.pdf

[15] D. Eastlake, 3rd and T. Hansen, “US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF),” RFC 6234 (Informational), May 2011, available at: http://www.ietf.org/rfc/rfc6234.txt

[16] R. Merkle, “A digital signature based on a conventional encryption function,” In: Pomerance C. (eds) Advances in Cryptology — CRYPTO ’87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg,pp. 369-378, 1987

[17] R. Merkle, “Protocols for public key cryptosystems,” in Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pp. 122- 133, April 1980

[18] Bitcoin Blockchain Size, https://charts.bitcoin.com/chart/blockchain-size

[19] J. Poon and T. Dryja, “The bitcoin lightning netwiork: scalable off-chain instant payments,”, 2016,

available at: https://lightning.network/lightning-network-paper.pdf

[20] M. Trillo, "Stress test prepares VisaNet for the most wonderful time of the year," 2013, available at: https://www.visa.com/blogarchives/us/2013/10/10/stress-test-preparesvisanet-for-the-most-wonderful-time-of-the- year/index.html

[21] A. Castor, "A short guide to Bitcoin forks," March 2017, available at: https://www.coindesk.com/short-guide- bitcoin-forks-explained/