BLOCKCHAIN BASED PAYMENT METHOD FOR SECURE TRANSACTION

Prof. Jayshri Mankar[1], Mr. Abhishek Ingle[2], Mr. Shivam Gade[3], Mr. Kshitij Bramhne[4]

[1] *Guide, Computer Engineering Department, Genba Sopanrao Moze College of Engineering, Balewadi, Pune, India*
[2,3,4] *Students, Computer Engineering Department, Genba Sopanrao Moze College of Engineering, Balewadi, Pune, India*

ABSTRACT

There was no mechanism in place before Bitcoin that allowed any two willing parties to conduct transactions without the intervention of a third party. To prevent fraud, third parties were brought into the process. As a result, enlisting a third party resulted in additional transaction fees, which is a disadvantage of the current online transaction system. Due to the ease with which digital tokens can be reproduced and the inability of transaction parties to verify the digital currency's legitimacy, double-spending is a problem with digital currencies. Bitcoin has a process in place to prevent double-counting and ensure that each transaction is genuine. Bitcoin is a cryptocurrency that is built on encryption, blockchain, and a peer-to-peer electronic cash system. Because there are no prerequisites, the Bitcoin network is rapidly expanding. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and re-join the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Keyword : - *Digital Currency , Electronic Cash, Proof-of-work.*

1. INTRODUCTION

In the past decade, with the popularity of digital cryptocurrencies, e.g., Bitcoin, blockchain technology has attracted tremendous attention from both academia and industry. The blockchain was first proposed in to serve as a crypto-currency transaction ledger, and is currently widely adopted for a large number of crypto-currencies, such as Ethereum, Ripple and EOS The blockchain technology guarantees the tamper-proof ledger, transparent transactions, and trustless but secure trading's in a decentralized network. Thus, the blockchain network is recently applied in a wide range of scenarios far beyond crypto-currencies, such as Internet of Things (IoT) healthcare and insurance In general, blockchain is a distributed public data-ledger maintained by achieving the consensus among a number of nodes in a Peer-to-Peer (P2P) network. More specifically, the verified transaction data is stored in a chain of blocks, i.e., a basic data structure of blockchain, and the chain grows in an append-only manner with all new verified blocks to it. This process involves several operations such as verifying transactions, disseminating blocks, and attaching blocks to the blockchain

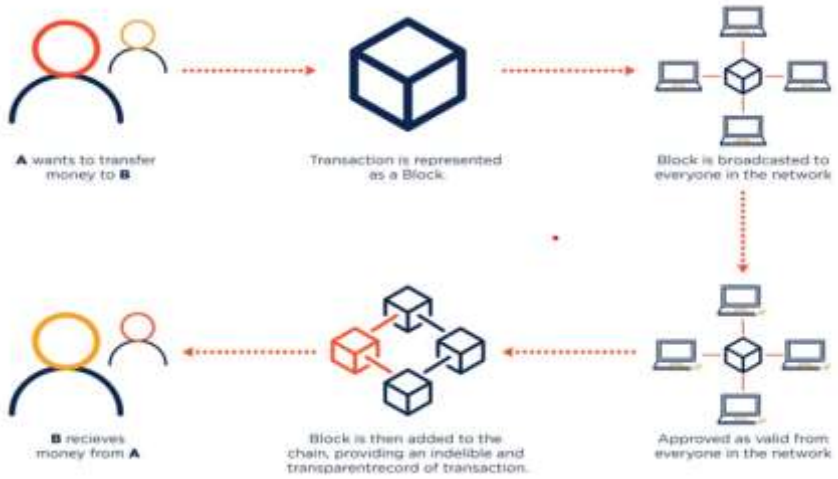


Chart : Working of Blockchain

2. LITERATURE SURVEY

Dourado, Eli & Brito, Jerry. (2014) in their article „Cryptocurrency‟ discusses about problems that have plagued digital cash in the past and the technical advance that makes cryptocurrency possible. It discusses about problem of double payment and Byzantine Generals Problem. The study concludes that Cryptocurrency is an impressive technical achievement, but it remains a monetary experiment. Even if cryptocurrencies survive, they may not fully displace fiat currencies.

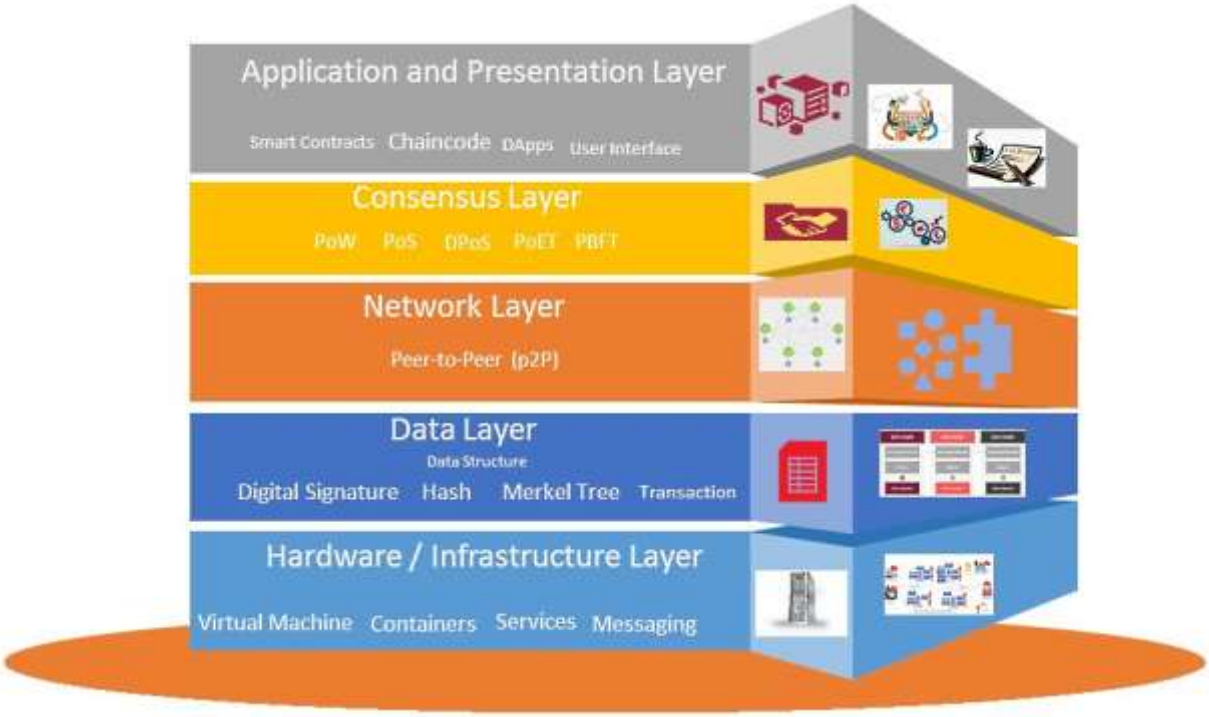
Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) in their study „Where Is Current Research on Blockchain Technology? Systematic Review‟ analyses challenges and future directions regarding Blockchain technology from the technical perspective. The results show that focus in over 80% of the papers is on Bitcoin system and less than 20% deals with other Blockchain applications including e.g., smart contracts and licensing. The majority of research is focusing on revealing and improving limitations of Blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness. Many other Blockchain scalability related challenges including throughput and latency have been left unstudied.

Chiu, Jonathan, Koeppl, Thorsten. (2017) in their study _The Economics of CryptocurrenciesBitcoin and Beyond. (2017)‘ analyses how well can a cryptocurrency serve as a means of payment? The study examines optimal design of cryptocurrencies and assess quantitatively how well such currencies can support bilateral trade. The challenge for cryptocurrencies is to overcome double-spending by relying on competition to update the blockchain (costly mining) and by delaying settlement. The study estimate that the current Bitcoin scheme generates a large welfare loss of 1.4% of consumption. This welfare loss can be lowered substantially to 0.08% by adopting an optimal design that reduces mining and relies exclusively on money growth rather than transaction fees to finance mining rewards. The study also point out that cryptocurrencies can potentially challenge retail payment systems provided scaling limitations can be addressed.

Foley, Sean and Karlsen, Jonathan R. and PutniņsTalis J (2018) in their paper _Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?‘ reports that approximately one-quarter of bitcoin users and one-half of bitcoin transactions are associated with illegal activity. Around $72 billion of illegal activity per year involves bitcoin, which is close to the scale of the US and European markets for illegal drugs. The illegal share of bitcoin activity declines with mainstream interest in bitcoin and with the emergence of more opaque cryptocurrencies. The techniques developed in this paper have applications in cryptocurrency surveillance. Our findings suggest that cryptocurrencies are transforming the way black markets operate by enabling —black e-commerce

3. ARCHITECTURE OF BLOCKCHAIN

1) DATA LAYER: The data layer, which encompasses the entire blockchain, is the lowest tier. It keeps track of a connected network of blocks. Version, Time stamp, Merkle root, Difficulty target, Nonce, and Previous hash are all included in each block. The block architecture is split into two parts: the block head and the block body. The Merkle tree is calculated using the history of validated transactions in the block body. The block head contains the hash of the previous block, the time stamp, the software version, and the remaining entities, such as the difficulty goal, nonce, and the Merkle root, which are used to effectively and safely verify transactions.
2) NETWORK LAYER: The network layer, which is the second lowest tier, has two primary goals: broadcasting and transaction verification. Blockchain networks are peer-to-peer networks with equal privileges for all nodes. Newly created transactions are broadcast to all network peers, who use a predetermined protocol to verify them. The transaction is transmitted to other nodes and a block is added to the data if verification is successful.
3) CONSENSUS LAYER: the consensus layer consists of a number of protocols that are used to verify any changes made to the blockchain. Because all nodes in an open peer-to-peer network are masters, they agree on a standard mechanism for validating new transactions. Bitcoin utilises proof of work (PoW), whereas Binance and DASH use proof of stake (PoS), which reduces the amount of electricity used in PoW. DPoS is used by Tezos and EOS (Delegated Proof of Stake). PBFT is used by Zilliga. Proof of bandwidth [19], ripple [20], tendermint [21], stellar [22], Proof of Capacity, Proof of Importance, Proof of Ownership, and Proof of Activity are some of the less well-known algorithms. Section IV contains a full examination of some of these consensus algorithms. For public blockchain systems, PoW, DPoS, and PoA are commonly used.
4) CONTRACT LAYER: The contract layer is in charge of using programmable smart contracts to defend participant rights. Two or more participants sign these smart contracts cryptographically. Certain contract norms are agreed upon by both parties. It is kept on the blockchain system and is self-triggered for each node to verify the transaction. A high-level programming language is used to programme the rules. Non-Turing complete language is used to implement Bitcoin's contract. Ethereum, on the other hand, makes use of Turing complete language platforms. Solidity is a common choice for smart contract implementation in many blockchains. Solidity is Turing complete, which means it can handle loops and other complex features. Solidity is also used to programme Ethereum smart contracts, which are then translated to bytecode using EVM (Ethereum Virtual Machine). Bugs in smart contracts should not be introduced.
5) APPLICATION LAYER: It is the highest level. It saves the user interface for using the blockchain network. Any network change is visible at the application layer. Web-based applications are available for several blockchain platforms. Different applications, such as intellectual property, IoT, and so on, can be designed based on business logic.



4. COMPARISION IN METHODOLOGY

Property	Public	Private	Federated
Consensus	• Costly PoW	• Light PoW	• Light PoW
Mechanism	• All miners	• Centralised organisation	• Leader node set
Identity	• (Pseudo) Anonymous	• Identified users	• Identified users
Anonymity	• Malicious?	• Trusted	• Trusted
Protocol & Efficiency	• Low efficiency	• High efficiency	• High efficiency
Consumption	• High energy	• Low energy	• Low energy
Immutability	• Almost impossible	• Collusion attacks	• Collusion attacks
Ownership &	• Public	• Centralised	• Semi-Centralised
Management	• Permissionless	• Permissioned whitelist	• Permissioned nodes

Transaction Approval	• Order of minutes	• Order of milliseconds	• Order of milliseconds

Software has evolved from a technology tool for solving specific problems to an industry that is omnipresent in most of today's corporate activities over the previous 60 years. Software engineering is defined as "the use of a systematic, disciplined, quantifiable methodology to the development, operation, and maintenance of software; that is, the application of engineering to software," according to IEEE Standard 610.12 [10]. The Software Engineering Body of Knowledge (SWEBOK) provides a complete description of the core SE Knowledge Areas (KAs) , which are also taken into account in this research. Software requirements, software process, software testing, software quality, software maintenance, software configuration management, and engineering management are examples of knowledge areas.

4. CONCLUSIONS

Blockchain is a powerful tool for resolving complex issues quickly. Its ability to provide security in an open environment makes it attractive for usage in a variety of other fields, including health care, IoT applications, and finance. E-commerce retailers and delivery partners can use consortium blockchains to avoid fraud during transit by continuously updating package positions on the blockchain. One of the most innovative potential uses of blockchain could be to avoid fraud in chit funds, which are used to save money in Indian society. It can also serve as a ledger for disadvantaged farmers to share resources. We give a state-of-the-art survey of blockchain technology in this study. We began by discussing the background, classification, architecture, and several sorts of consensus.

5. ACKNOWLEDGEMENT

It is an our Great Pleasure to express our special thanks of gratitude to all our Authors and Professors for their contribution in our project for analysis and reporting of our work, also we would like to thanks them who supported for important intellectual content and also for article drafting and revising it.

6. REFERENCES

[1]. Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System." March 2009.

[2]. Ridhanshi Bhatia, Praveen Kumar, Shilpi Bansal and Seema Rawat. "BLOCKCHAIN –THE TECHNOLOGY OF CRYPTO CURRENCIES." In ICACCE-2018.

[3]. XIAO FAN LIU, XIN-JIAN JIANG2, SI-HAO LIU AND CHI KONG TSE. "Knowledge Discovery in Cryptocurrency Transactions: A Survey".
In Digital Object Identifier 10.1109/ACCESS.2021.3062652.

[4]. Vaibhav Shakya, PVGN Pavan Kumar, Lakshay Tewari and Pronika. "Blockchain based Cryptocurrency Scope in India." IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2. (ICICCS 2021)

[5] FAIJAN AKHTAR, JIAN PING LI, MD BELAL BIN HEYAT, SYED LUQMAN QUADRI, SHAIK SOHAIL AHMED, XIAO YUN, AMIN UL HAQ. "POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN DIGITAL CURRENCY: A REVIEW." 978-1-7281-4242-5/19/$31.00 ©2019 IEEE.

[6] Suman Ghimire and Dr. Henry Selvaraj. "A Survey on Bitcoin Cryptocurrency and its Mining."978-1-5386-7834-3/18/$31.00 ©2018 IEEE.

[7] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks.
"A Brief Survey of Cryptocurrency Systems." white paper 2016.

[8] Jae Min Kim, Jae Won Lee, Kyungsoo Lee and Junho Huh. "Proof of Phone:A Low-cost Blockchain Platform"
Self-published.

[9] Yong Yuan and Fei-Yue Wang. "Blockchain and Cryptocurrencies: Model, Techniques, and Applications"
2168-2216-2018 IEEE.

[10] Wenzheng Li and Mingsheng He. "Comparative Analysis of Bitcoin, Ethereum, and Libra