Literature Survey of Blockexchange

Shahanas M S, Shejina N M, Dr G.Kiruthiga

[1] *Student, Dept. of Computer science and Engineering, IES College of Engineering, Kerala, India*
[2] *Assistant professor, Dept. of Computer science Engineering, IES College of Engineering, Kerala, India*
[3] *Associate professor, Dept. of Computer science Engineering, IES College of Engineering, Kerala, India*

ABSTRACT

The fast expansion of cryptocurrencies and Blockchain technology has recently altered the banking system and given rise to a new crypto-economy. Although Bitcoin is its most well-known application, a blockchain has several uses outside of cryptocurrencies. Blockchain technology supports a variety of industries, including cryptocurrency trading, anti-money laundering tracking systems, healthcare, real estate, supply chain monitoring, and logistics monitoring. This technology enhances security and reduces transaction fees because there are no middlemen. The study established that blockchain is a relatively new technology and that nodes in the network can exchange data independently of one another. To add transaction records to the public ledger and to verify a cryptocurrency transaction, mining was necessary. In cryptocurrencies, which are peer-to-peer digital trading platforms, cryptography is employed to generate and distribute units of currency. The ability to trade money without relying on a centralized authority is advantageous for users of cryptocurrency exchanges. Ethereum is the first blockchain platform for building smart contracts. It supports complex and personalised smart contracts with the help of the Ethereum virtual computer, a Turing-complete virtual machine. Decentralized apps can now be used without the use of a trusted third party thanks to smart contracts, which are computer protocols that automate the negotiation and enforcement of agreements amongst several unreliable parties. This study discusses the fundamentals of blockchain technology, its applications, problems, prospects, and advantages and disadva ntages of the system. Blockchain transaction information for Bitcoin and Ethereum is covered, as well as the general concepts of mining, cryptocurrencies, and smart contracts. Include a discussion on blockchain application implementation.

Keyword: - *Blockchain, Bitcoin, Mining, Cryptocurrency, Ethereum, Smart Contract*

1. INTRODUCTION

The blockchain has been around for more than ten years and is a system where a distributed database records every transaction that takes place in a peer-to-peer network. It is viewed as a distributed computing paradigm that effectively resolves the trust in a centralized party issue. As a result, multiple nodes work together in a blockchain network to secure and maintain a set of shared transaction records in a distributed manner without depending on any third parties. The first proposed cryptocurrency that used the blockchain as a distributed infrastructure technology was announced by Satoshi Nakamoto in 2008 with the introduction of Bitcoin [1]. Without a centralized regulator, it enabled users to securely transmit virtual money called "bitcoins." The crucial component of this deal is mining. Only those genuine transactions will add to the blocks after being validated by miners with powerful graphics cards. These blocks were all linked together in a chain. There are several mining algorithms used by different blockchains. A consensus algorithm based on proofs is known as proof-of-work (PoW). The fundamental idea behind the consensus technique is to identify and decide which node will be given the authority to add a new block to the chain by demonstrating sufficient proof of its effort.

2. LITERATURE SURVEY

Review, purchase and personal history success of internet marketplaces depends heavily on trust. Customers are apprehensive of market middlemen because they believe they are being opportunistic [2]. The online marketplace revealed that purchasers' perceptions of risk were equally important factors [3].

Satoshi Nakamoto advocated a trustless method for electronic commerce. He began with the customary architecture of digitally signed coins, which offers good ownership control but falls short without a method to prevent double spending. He proposed a peer-to-peer network employing proof-of-work to keep a public history of transactions that, assuming honest nodes hold the majority of CPU power, quickly becomes computationally difficult for an attacker to alter. The network's unstructured nature makes it robust. Nodes operate without much cooperation at once. Since messages are just required to be delivered with the greatest effort and are not directed to specific locations, they do not need to be recognized. Nodes are free to join and leave the network as they like, trusting the proof-of-work chain as evidence of what occurred while they were away. They cast their votes using their CPU power, extending legal blocks when they agree with them and refusing to work on invalid blocks. This consensus technique can be used to enforce any necessary rules and incentives[1].

Ahmad Afif Mortan discovered blockchain's design, algorithm, and operation in the paper[4]. The blockchain technology is a strong platform to transfer money without relying on a centralized authority. A fully-fledged Turing-incomplete programming language is Bitcoin. Complex algorithms cannot be executed in this language. He aware that the characteristics of blockchain, such as immutability, decentralization, transparency, and auditability, increase the security and tamper-proofs of transactions. Blockchain is essentially a series of blocks that uses a public ledger to store all committed transactions. When fresh blocks are added to the chain, it continues to expand. Digital signatures, cryptographic hashes, and distributed consensus algorithms are some of the essential te chnologies that make it possible for blockchain to operate in a decentralized setting. There is no need for any intermediaries to check or verify any of the transactions because they all happen decentralized. Other problems with blockchain include interoperability, privacy, energy use, egotistic mining, security, and regulatory policy.

The lack of a standardized protocol for corporate adoption and integration of blockchain-based solutions gives rise to the interoperability problem. Even though the blockchain claims to be extremely secure since users only conduct transactions using digital signatures associated with public-private key encryption, privacy leaks may still occur within the system. Additionally, the user's actual IP address can be found. Serious issues are also being raised with consensus procedures like proof-of-work (PoW) and proof-of-stake (PoS). For instance, PoW is renowned for using a significant amount of electrical energy since miners compete to create blocks by resolving challenging mathematical riddles. In PoS, the wealthy get steadily wealthier because the likelihood of getting a block depends on the stake size of the miners. Selfish mining, where miners might profit more than their fair share by keeping their blocks private, is another disadvantage of blockchain technology. Blockchain technology is susceptible to 51 percent attacks, in which a single node gains control of the majority of a network and abuses it. Furthermore, because of the uncertainties surrounding prospective governmental laws, it is thought that blockchain technology may not reach its zenith or the anticipated broad adoption by stakeholders.

According to Gavin Wood, the creator of Ethereum and Ethcore, the Ethereum project's goal was to make it easier for people to transact with one another without the use of established trust frameworks. His objective was to create a system that interacts with total trust in the results [5]. Ethereum was consequently made. Both carry out the same functions. Each of them used a different consensus algorithm. The two types of accounts available for Ethereum are Externally Owned Accounts (EOA) and Contract Accounts (CA). EOA is necessary to join in the Ethereum network and communicates with the blockchain using transactions, whereas CA represents a smart contract (SC).

An open-source blockchain technology hosted by the Linux Foundation called Hyperledger was compared to Ethereum by Pongnumkul et al. They measured the following performance criteria: I)Time spent deploying transactions, II) Transaction execution time, latency, and completion time. Maximum Concurrent Throughput and VI Transactions. The results showed that Hyperledger Ethereum could handle more but had a higher throughput. Simultaneously transactions Due to this, Ethereum becomes even an appropriate framework for creating scalable applications. The use of Ethereum's own money in applications Developers can design ecommerce utilizing its framework. Ethereum-based applications cryptocurrency, ether.

On order to establish software measures, Toneli et al. analysed the features of over 12,000 smart contracts. They discovered that, in general, the ranges of smart contracts metrics are more constrained than those of similar metrics in conventional software systems. They looked at metrics for events, mapping, modifiers, contracts, functions, lines, comments, bytecode, and cyclomatic complexity in software. The following metrics are specific to smart contracts and cannot be tracked for non-decentralized applications: calls to or from other addresses, calls inside a single smart contract, gas consumption, cryptocurrency trades, and bytecode/ABI metrics [6].

Focusing on the advantages and difficulties of smartcontracts, Shafaq Naheed Khan. Conventional contracts and blockchain technology integrate the terms of agreements between two or more parties, but smart contracts perform better than traditional contracts since they automatically implement agreements in a distributed environment when certain circumstances are met. Without the aid of a reliable third party, smart contracts enable, carry out, and enforce agreements between unreliable parties. Smart contracts are executable codes that operate on top of the blockchain. Smart contracts allowed for network automation and the conversion of paper contracts into digital ones. By using automated transactions that were not under the control of a central authority, smart contracts, as opposed to traditional contracts, allowed users to formalize their agreements and trust relationships. Smart contracts allowed for network automation and the conversion of paper contracts into digital ones. By using automated transactions that were not under the control of a central authority, smart contracts, as opposed to traditional contracts, allowed users to formalize their agreements and trust relationships. A smart contract's security refers to its ability to withstand attacks from malicious users that want to profit from contract security weaknesses or take advantage of a lack of reliable data feed to inject false data. In this study, the major topics that were investigated were dependable data feeding, transactional privacy, and vulnerability detection.

Bitcoin and other cryptocurrencies were discussed by Ridhanshi Bhatia. Based on their characteristics, he compares various cryptocurrency types. The position paper indicates that Ethereum continues to be in demand in the digital market due to the added feature of smart contracts built in it after discussing numerous parameters based on several digital currencies, including Bitcoin, Litecoin, Ethereum, Bitcoin Cash, and Ripple. This feature enables trading of stock, property, and money without the need for a legal representative, advisor, or other service provider. The central man is entirely gone. According to the author, when new technologies emerge with innovative and clever features in the digital market, bitcoin's future is in grave danger and its usage is declining daily. As it seems to be a bright future, there are certain contribute in the stable future of the blockchain technology [8] such as Electronic Contracts, Internet of things, Anti- fake platform.

On the Ethereum blockchain, R. Vishnu Prasad spoke about a decentralized marketplace application[7]. He explained the operation of transactions on the Ethereum network. The Truffle development framework was used to create the application. An Ethereum smart contract that was later moved to the Ethereum network housed the application's capabilities. The web3.js API was used to send the user's input to the Ethereum network after being read through a web interface. The application was found to have an average gas consumption of 4.6 wei and a transaction runtime of 3.8 seconds. The application's contract formation times were demonstrated to be under a second. According to his findings, selling through the program is less expensive than current online and offline choices.

Tiago Fernandez-Caraméser[9] discussed Blockchain can provide the Internet of Things (IoT) with a platform for sharing reliable information that defies non-collaborative organizational structures. In addition to outlining key BIoT application possibilities in industries including healthcare, logistics, smart cities, and energy management, this assessment analysed the state-of-the-art of blockchain technologies. These IoT applications have unique technological needs that differ from cryptocurrency implementations in a number of ways, such as the necessity for a particular design or energy efficiency in devices with limited resources. Additionally, it included a comprehensive analysis of the most important factors involved in an optimised BIoT design, such as its architecture, the necessary cryptographic algorithms, or the consensus mechanisms. T. M. Fernández-Caramés, P. Fraga-Lamas: Review on the Use of Blockchain for the IoT. Additionally, certain suggestions were made with the intention of advising future BIoT researchers and developers on some of the problems that must be solved before releasing the BIoT applications of the next generation.

More qualitative metrics, such as structural interoperability, support for Turing-complete operations, support for user identification and authentication, cost-effectiveness, and scalability across large populations, are listed by Vanderbilt University researchers in their study of a healthcare-specific application [10]. Others offered security patterns for freshly developed smart contracts that contrasted various security features, such as checkseffects-interaction, emergency stop, speed bump rate, limit mutex, and balance limit[11].

A blockchain voting mechanism was implemented by Diva K. She explained the entire workings and benefits of the system and also made comparisons with the current system. Because unsecured ballots are never used, blockvoting offers greater security than ID proof, and biometric identity is the most secure form of authentication, according to the researcher's findings. Additionally, blockchain offers storage-level voting security. By enabling you to construct a centralized hierarchical vote distribution without having to wait for results, online voting saves time and money. It takes place instantly. Full service setup and management is quicker and simpler because time is saved. in order to free up time for other activities. It is challenging to damage the system's credibility because it is a decentralized voting tool[12].

3. CONCLUSIONS

In this study, we discovered that a decentralized application can offer improved security and simple transactions without the use of middlemen. A fantastic technology for decentralized applications was pioneered by Santoshi Nakamoto. Over time, individuals discovered other blockchains with Turing complete language that were similar to his. It is promising to build a competitive Dapp on the promising Ethereum platform with a straightforward user interface since it will develop technology expertise and have the potential to compete in a just-emerging market. Because the rules of the system are predetermined by the smart contract, vendors cannot be subjected to discrimination by the system thanks to the use of such contracts. We also have transparent system rules that can be independently verified by the public. Additionally, the audit process is made simpler by the transaction data being kept on the blockchain. This essay also discussed several blockchain implementation and applications.

4. REFERENCES

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electroniccash system, 2008.

[2] Pavlou, P. A., & Gefen, D. “Building effective online marketplaces with institution-based trust.” Information Systems Research, 15(1), 37-59, 2004.

[3] Gimun Kim, Hoonyoung Koo, “The causal relationship between risk and trust in the online marketplace: A bidirectional perspective” Computers in Human Behavior Volume 55, Part B, February 2016, pp. 1020-1029.

[4] A survey of blockchain from theperspectives of applications, challenges, and opportunities AA Monrat, O SChelen,K Andersson – IEEE Access, 2019 – ieeexplore.ieee.org

[5] Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014. Reference 3(Font-10, justify)

[6] Blockchain smart contract:Applications,challenges and future trends SN Khan, F Loukil, C Ghedira-Guegan,2021- spinger.

[7] A decentralized marketplace application on the ethereum blockchain VP Ranganthan, R Dantu, A Paul… - 2018 IEEE 4th …, 2018 - ieeexplore.ieee.org

[8] A decentralized marketplace application on the ethereum blockchainVP Ranganthan, R Dantu, A Paul… - 2018 IEEE 4th …, 2018 - ieeexplore.ieee.org

[9] Peng Zhang, Michael Walker, Jules White, Douglas C. Schmidt, Vanderbilt University “Metrics for Assessing Blockchain-based Healthcare Decentralized Apps”, IEEE 2018

[10] Maximilian Wöhrer and Uwe Zdun, University of Vienna “Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity

[11] A Review on the Use of Blockchain for the Internet of ThingsTM Fernández-Caramés, P Fraga-Lamas - Ieee Access, 2018 - ieeexplore.ieee.org

[12] Blockvoting: An Online Voting System Using Block ChainK Divya, K Usha - 2022 International Conference on Innovative 2022 - ieeexplore.ieee.org