ISSN 2320 - 2602
Volume 13 No. 2, February 2024
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst011322024.pdf
https://doi.org/10.30534/ijacst/2024/011322024

A literature survey on public blockchain technology for Cryptocurrency

Mayya Madhu Sudhan[1], Mohammed Shoaib[2], Mohith S Shetty[3], Pratheek Pramod Shetty[4], Dr. Bramha Prakash H P[5]
[1]Alva's Institute of Engineering and Technology, India, madhusudhanmayya@gmail.com
[2]Alva's Institute of Engineering and Technology, India, shoaib121344@gmail.com
[3]Alva's Institute of Engineering and Technology, India, mohitshetty89@gmail.com
[4]Alva's Institute of Engineering and Technology, India, pratheekpramodshetty@gmail.com
[5]Alva's Institute of Engineering and Technology, India, drbrahmap@aiet.org.in

Received Date : December 28 , 2023 Accepted Date : January 16, 2024 Published Date : February 07, 2024

ABSTRACT

Blockchain and cryptocurrencies have emerged as revolutionary technologies that have garnered substantial interest in the past few years. A blockchain functions as a distributed and transparent ledger, facilitating secure transactions without the requirement of intermediaries. Digital assets like Bitcoin and Ethereum are examples of cryptocurrencies, leveraging blockchain technology to enable secure and unrestricted transactions. These innovations have the potential to revolutionize industries such as finance, supply chain management, and healthcare. However, challenges such as regulatory concerns and scalability issues must be addressed for their widespread adoption. Overall, blockchain and cryptocurrencies offer new opportunities for innovation and financial inclusion.

Key words: Decentralized, transparent ledger, powers crypto currencies, scalability, comparative framework.

1. INTRODUCTION

A decentralized public ledger called blockchain, a revolutionary technology, securely maintains records over a network of connected computers [1]. Thanks to its ability to offer security, immutability, and transparency, blockchain has gained worldwide acceptance and acknowledgment [1]. By eliminating intermediaries and providing a tamper-resistant platform, blockchain fosters efficiency and trust across various industries. The rise of cryptocurrencies like Bitcoin, which seek to establish a decentralized environment where transactions and data are not under the jurisdiction of a single central authority, is evidence of their success [2]. The decentralized structure of blockchain has triggered a significant transformation in the perception of trust, paving the way for diverse applications beyond the realm of digital currency.

Blockchain technology's quick growth has been driven by its capacity to find workable solutions to persistent issues that were previously impractical [4]. The adoption of blockchain technology in international payments and financial transactions has revolutionized the way we engage in business. This innovative solution enables faster and more secure transactions, reduces costs, and enhances transparency [1]. Experts predict that blockchain's impact on the global economy will be remarkable, with an estimated commercial value of $176 billion by 2025 and an astonishing $3.1 trillion by 2030 [1]. The understanding that blockchain technology has the power to revolutionize businesses by simplifying procedures, boosting security, and encouraging dependence on a decentralized way is what is driving this rise.

The variety of blockchain implementations contributes to the ecosystem's expansion [3]. While Bitcoin remains the most renowned and extensively utilized blockchain, numerous other implementations exist to cater to various functions, handling strategies, and performance requirements [2],[3]. Constructing applications based on blockchain necessitates meticulous consideration of crucial technological features and configurations to ensure optimal system quality [4]. A framework has been established to assist decision-makers in choosing the best blockchain technology for their unique requirements by examining current industry products, technical forums, scientific literature, and real-world use cases [4]. This framework equips software architects, developers, tool selectors, and policymakers to decide on the best course of action after evaluating various blockchain solutions and their suitability for achieving desired results.

2. BACKGROUND

Blockchain technology is the foundational technology that powers cryptocurrencies. It offers a safe and open system for logging and verifying transactions. Each transaction is added to a block that is encrypted and connected to earlier blocks in a chain-like structure [1]. With the help of this distributed ledger technology, fraud and manipulation are prevented because everyone in the network has access to the same data. Blockchain is a decentralized technology, meaning no one organization has authority over the network, making it immune to censorship and hacker efforts.

Digital or virtual currencies that only exist in electronic form include Bitcoin, Ethereum, and Litecoin. Powerful computing systems execute complex calculations in a procedure referred to as mining, aiming to authenticate and incorporate transactions into the blockchain [5]. Cryptocurrencies offer various advantages compared to traditional currency, enabling fast and secure peer-to-peer transactions while eliminating the need for intermediaries such as financial institutions.

Additionally, as cryptocurrencies are unrestricted by the constraints of conventional banking institutions, they may be utilized for international payments.

The decentralized nature of cryptocurrencies, which implies that no government or central body controls or regulates them, is one of their distinguishing characteristics [2],[6]. The decentralization of financial affairs and possessions has granted individuals increased autonomy, enabling them to exert greater control. Nevertheless, this advancement presents challenges, including price fluctuations and concerns regarding regulations [1],[5]. Governments worldwide are actively working on establishing frameworks to regulate cryptocurrencies, combat tax evasion, and address issues related to money laundering, as these aspects are still under development.

More than only financial transactions are impacted by blockchain and cryptocurrencies. Due to its increased transparency, security, and efficiency, blockchain technology has the potential to revolutionize several sectors [3]. Supply chain management, digital identity management, and the utilization of decentralized apps (DApps) are among the potential applications for it [3],[4],[6]. Conversely, cryptocurrencies have gained significant traction as investment instruments, leading to the expansion of a thriving network of exchanges, wallets, and supplementary services [5],[6].

In general, the adoption of blockchain technology and digital currencies has revolutionized the approach for conducting financial transactions. It has opened up new opportunities for safe and decentralized systems, giving people and organizations the capacity to manage their financial dealings in a worldwide environment [2],[4],[5].

3. COMPARATIVE FRAMEWORK FOR BLOCK-CHAIN IMPLEMENTATIONS

A comparative framework for blockchain implementations involves evaluating different factors to assess and compare the strengths and weaknesses of various blockchain platforms [4]. Key considerations include the consensus mechanism, scalability, security, governance model, interoperability, sustainability, and adoption. These factors help stakeholders determine which blockchain implementation aligns best with their specific needs and goals. By conducting an analysis of these factors, individuals can make well-informed choices regarding the blockchain solution that best suits their specific use case [4]. Consequently, these characteristics play a crucial role in promoting the acceptance and integration of blockchain technology.

3.1 Consistency

Various approaches have been employed to ensure the secure association of a transaction with the blockchain, thereby guaranteeing strong consistency [2],[5]. One method involves waiting for a specific number of blocks to be generated (e.g., 6 blocks for Bitcoin or 12 blocks for Ethereum) after the transaction to establish its strong consistency with the blockchain [2],[5]. Another approach is to introduce a checkpoint within the blockchain, enabling all participants to accept transactions as valid and irreversible up to that checkpoint [2],[5]. Unlike multi-transaction block-based systems, alternative distributed ledger implementations such as DAG can significantly reduce confirmation times, as transactions propagate independently within seconds [3]. Consequently, consistency becomes reliant on the time required for confirmation, determined by the block production rate (BPR) specific to each implementation and set during the design phase [3]. Confirmation times can vary from seconds to minutes and hours, while block production speeds range from 10 minutes or more, 1 to 10 minutes, and even seconds [1],[4].

3.2 Performance and Scalability

To ensure authenticity and privacy in healthcare applications, user authentication becomes more complex, especially when integrating sensor networks [1],[5]. In the field of medical applications, sensor networks can be classified into three primary categories: implantable, wearable, and embedded. Implantable devices refer to medical devices that are placed inside the human body. Wearable technology, on the other hand, is designed to be worn on or in close proximity to the human body [4]. Embedded systems utilize environmental sensors for integration with the surroundings [4]. These networks serve various purposes, including locating individuals, comprehensive monitoring of patients' health conditions, and evaluating body posture [1],[5]. Environmental sensors incorporated into the environment continuously monitor a person's physical state, providing valuable data for ongoing health diagnostics [3]. This network of sensors can collect information related to fitness, well-being, and energy consumption [3]. Given the significance of user data security and privacy, healthcare applications require careful attention to user authentication, which becomes more complex when integrating sensor networks.

3.3 Security

The immutability of the blockchain is a significant attribute that safeguards the authenticity and confidentiality of data after it has been verified by all participating nodes. Any potential weaknesses or loopholes that can be manipulated by individuals with malicious intent are commonly known as security issues [2]. Currently, the most reliable solutions are based on Proof of Work (PoW) [2]. Nevertheless, there exists a potential risk of a 51 percent attack, wherein an individual or organization gains full control over a majority of the network's computational power and can manipulate it accordingly [5]. Other consensus protocols like Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) may offer enhanced scalability and performance, but they come at the expense of reduced security, as they typically allow up to one-third (33%) of untrusted nodes [4].

Alternatively, incorporating additional algorithms such as Byzantine Fault Tolerance (e.g., the BFT Ripple Consensus protocol) can augment security by tolerating up to two-thirds (2/3) of unauthorized nodes [3],[6]. However, these protocols entail supplementary prerequisites, including the necessity for participating nodes to possess knowledge of one another.

Consequently, the choice of consensus protocol and ledger implementation carries security implications.

3.4 Decentralization

Wireless Sensor Networks (WSNs) In theory, the concept of blockchain relies on a decentralized network without a central authority, enabling distributed recording, storage, and updating of data. However, it should be noted that certain blockchains may exhibit varying degrees of centralization [3]. In the scenario of a public and permissionless blockchain, no individual central authority or group holds greater power than others (as observed in the case of Bitcoin) [3]. Furthermore, all participants possess the privilege to verify transactions [3]. On the other hand, Consortium or Permissioned Blockchains grant specific permissions to a limited number of nodes for transaction validation (as observed in PoS and DPoS-based blockchains like EOS) [2],[6]. In contrast, fully private blockchains adopt a centralized structure with decision-making and validation control vested in a designated entity (such as Ripple and its Ripple Consensus Protocol) [2],[6]. Permissioned blockchains offer advantages such as increased speed, energy efficiency, and ease of implementation, but they introduce a certain level of centralization [3]. Hence, the degree of decentralization is influenced by the chosen consensus protocol and ledger implementation [3].

4. CASE STUDY: EXPLORING THE CONCEPT OF A DECENTRALIZED UBER

Blockchain technology has the potential to revolutionize the operations of companies like Uber. But how would a decentralized Uber function? Instead of relying on a centralized organization as a middleman, individuals looking for rides would attach relevant metadata, such as their preferences and requirements, to their blockchain-based profiles. This information could include location data and driver ratings, among other details. When someone requests a ride, the blockchain can utilize this metadata to filter and match potential drivers, directing the request to the most suitable driver available [4]. Subsequently, transactions between the driver and passenger can be processed through a peer-to-peer network, eliminating the need for a centralized intermediary.

5. HOW BLOCKCHAIN WILL SOLVE THIS PROBLEM

Imagine a decentralized transaction, the driver would open the app and every available driver within a certain radius would be traceable. The passenger specifies the destination, and all drivers would have the opportunity to bid for a job. The passenger selects the driver (based on price, reputation, pickup time, etc.) and a smart contract is created linking driver and passenger [1]. The fare is held by a smart contract and held until the driver takes the passenger to the Destination. Once the terms of the smart contract are met, the driver gets paid and both parties have the opportunity to review each other's experiences.

6. UBER BLOCKCHAIN PLATFORM COULD HAVE THE FOLLOWING BENEFITS

The implementation of the Uber Blockchain Platform could potentially yield the following advantages.

6.1 Cost Reduction

The blockchain decentralized platform reduces the need for intermediaries, which lowers transaction fees and operational costs. The direct connection between passengers and drivers eliminates the additional costs incurred through multiple intermediaries [6].

6.2 Safety and security standards

Smart Contracts enforce safety standards for drivers, generate accurate scores and prevent them from engaging in criminal activities.

Generating accurate ratings and preventing their involvement in criminal activities. By empowering riders to acquire comprehensive information about individual service providers, their safety and security can be enhanced, enabling them to make well-informed decisions [3],[4].

6.3 Environmentally Cleaner

Decentralized ridesharing facilitated by blockchain leads to a more efficient use of vehicles, reducing the number of cars on the road. Fewer cars contribute to a pollution-free environment and decrease the negative effects of metal and plastic consumption [6].

Since people will be able to share the ride seamlessly, fewer cards might be required, decreasing the metal and plastic amount that has various harmful effects [3]. It will help the world move towards a cleaner approach with every car removed from the road due to decentralized ridesharing platform.

6.4 Economic Opportunity

With the approach of a decentralized car-sharing platform, anyone can earn income using their personal vehicle. The removal of service fees due to the elimination of intermediaries can increase business opportunities for everyone with a smartphone and a safe modern vehicle [4],[6].

Blockchain holds a promising future in the coming years. Since a cab company like Uber is an integral part of the current public transportation system, the blockchain comes as a solution by decentralizing every operation and eradicating the need for a third party [2].

7.CONCLUSION

This paper offers a concise and pragmatic introduction to the fundamental principles underlying blockchain technology and proposes potential use cases that could be of interest [4]. Moreover, the article acknowledges the potential presence of innovative applications that remain unexplored but could hold considerable significance for the field. Nonetheless, it is imperative to thoroughly assess the benefits of utilizing

blockchain technology for these specific instances, considering the potential drawbacks such as inefficiency or high costs. In scenarios where blockchains align with industry requirements and applications, there is a possibility that publicly available or commercially-enabled chains could offer additional information and advantages.

REFERENCES

[1] Blockchain Revolution: How The Technology Behind Bitcoin And Other Cryptocurrencies Is Changing The World By Don And Alex Tapscott

[2] Michael Bacina, "Smart contracts and cotracts disputes and State of the DApps", 2018 https://www.stateofthedapps.com/stats

[3] Martin Garriga ,Alan Derenzis, Maximilliano Arias, Blockchain and cryptocurrency: A framework of the main Architectural Drivers.

[4] Brian A Scriber. 2018. A Framework for Determining Blockchain Applicability. IEEE Software 35, 4 (2018).

[5] Shailak Jani, "Growth of cryptocurrency in India: Its Challenges and Potential Impact Law", April 2016.

[6] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). https://bitcoin.org/bitcoin.pdf