Crimson Publishers
Wings to the Research

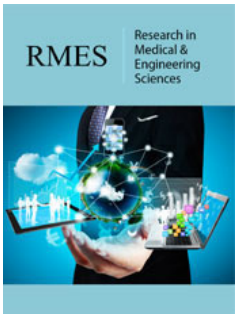
Mini Review

Bitcoin and Blockchain Technology and Some Perspectives on its Future- A Mini Review

Chetna* and Shikha

Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, India

ISSN: 2576-8816



***Corresponding author:** Chetna, Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India

Submission: July 12, 2022

Published: August 22, 2022

Volume 9 - Issue 5

How to cite this article: Chetna, Shikha. Bitcoin and Blockchain Technology and Some Perspectives on its Future- A Mini Review. Res Med Eng Sci. 9(5). RMES.000725. 2022. DOI: 10.31031/RMES.2022.09.000725

Abstract

A digital money built on cryptographic principles that has gained popularity recently is referred to as a cryptocurrency. Bitcoin is a decentralised cryptocurrency that records all transactions on a distributed, append-only public ledger called a blockchain. The incentive-compatible Proof-of-Work (PoW)-based decentralized consensus procedure, which is upheld by nodes in the network known as miners, is essential to the security of bitcoin. As the market continues to rise, interest in Bitcoin appears to be increasing. The underlying concepts of Bitcoins and Blockchains are the same, as is briefly addressed in this review. Blockchain is a breakthrough technology that has multiple implementations, ranging from smart contracts to cryptocurrencies, and is discussed in several studies as a potential solution to a number of problems.

Keywords: Blockchain; Bitcoin; Blockchain security; Bitcoin security; Bitcoin attacks; Security threats; User privacy

Introduction

Blockchain has recently been a pioneer in trustworthy computing in an open network infrastructure that does not require a central authority, symbolising the beginning of an era. It offers a unique system for data storage, operation execution, service provision, and trust building. Blockchain is well-known for being a digital revolution in privacy and cybersecurity, with uses ranging from globally distributed monetary systems like Bitcoin to Internet of Things-enabled smart grids and smart contracts, among others [1]. The review will start off by talking about blockchain and how it applies to digital exchanges for Bitcoin.

What is blockchain?

A linked list is created by connecting a network of blocks, which is referred to as a "blockchain" in this context. A block head and a block body are the two essential components of any block. Information regarding the block's and chain's management is contained in the block header. The block body, on the other hand, includes a transaction list [2].

A blockchain is a decentralised database used for information management that keeps track of a constantly changing collection of transaction logs by arranging them in a block-by-block hierarchy. The blockchain network is constructed and maintained using a peer-to-peer (P2P) underpinning technology, and it is protected by the wise and widespread application of crowdsourcing and encryption. The value of the blockchain economy was $211 billion as of January 2020. The three layers that make up a blockchain's fundamental structure are its main P2P networks, its database, and its numerous applications [3].

Blockchain's potential applications go far beyond monetary assets and electronic currency. Blockchain was initially created as the fundamental architecture of Bitcoin, the first decentralised cryptocurrency that has grown to incredible heights since its 2009

introduction. It acts as the decentralised ledger for the Bitcoin system, recording and confirming each bitcoin in the Bitcoin P2P network environment worldwide to allay worries about digital media, such as double spending etc.

Future aspects

This survey study focuses on bitcoin as a generalizable blockchain-based application, as well as blockchain architecture and cryptographic protocols. Regardless of geographical limitations or reliable intermediaries, blockchain can significantly change how transactions and payments are handled globally. It has great potential for creating a global, reasonably priced, and secure communications network for the rest of the world's businesses.

Many aspects of all Bitcoin technologies, such predicting the success of machine learning and artificial intelligence operations, may yet be untapped. This section covers numerous noteworthy accomplishments as well as potential strategic research efforts. The corporate and scientific fields have shown a lot of interest in Blockchain technology during the past ten years [4]. A crucial strategic path for consensus algorithms is the switch from POW to numerical algorithms like POS. Another exciting potential for the future is that brand-new cryptocurrencies like NEM and EOS may encourage companies to develop blockchain applications based on novel protocols.

Before blockchain to become a widely useful technology, some current challenges must be overcome. To start, blockchain technology needs to be more flexible to get beyond the limitations of poor performance, lag, and continually rising memory requirements. For instance, it must look at ways to use the high throughput of multicore and group systems to significantly increase the efficiency of money transfers. Today's powerful node organizations may be able to combat resource inefficiency and dominance by studying how to control connection sizes by deleting extraneous blocks without compromising authenticity [5].

The cost-effective deployment of enhanced smart contracts is a much more pressing problem that the research community needs to address. The investment community will eventually have to deal with the environmental ramifications of numerous nodes contributing to agreements that, if left unattended, might trigger a serious global environmental crisis.

Microsoft and Intel have formally joined to promote enterprise blockchain, and the partnership maintains that dependability, confidentiality, and governance challenges must be handled for corporate block chain technology to prosper. In a distributed network between two blockchain- based parties, blockchain technology has produced completely unbiased reputation management and artificial intelligence (AI) empowers robots to make wise decisions on par with humans and, in some circumstances, more quickly. The combined strengths of AI and bitcoin hold great promise for developing apps in a variety of industries. A great fit for very lucrative applications would result from trust in bitcoin, as well as artificial intelligence decision-making in hospitals and driverless cars, for instance. Future applications for this technology could include energy trading, tracking the life cycle of automobiles, electric cities, and the usage of Bitcoin for tax collection [6].

Conclusion

This mini review's goal was to give readers a broad overview of current blockchain and bitcoin usage strategies, defences, and efficiency. Due to its primary attributes of decentralisation, durability, anonymity, and data authenticity, blockchain has demonstrated its potential to fundamentally alter traditional businesses.

Although Bitcoin is the first effective virtual currency implementation known to exist, it is still in its infancy, and its creators are constantly working to lessen its vulnerability. New and creative assaults will start to appear as more people start utilising bitcoin. Attacks like ">50%" and "Selfish-mining" have the potential to make the Bitcoin mining process unreliable.

All users accept Bitcoin's protocols because it is a decentralised cryptocurrency, and a community of participants must agree before any changes to the protocol set can be made (approximately 80 percent). Therefore, it seems difficult to implement advanced Bitcoin protocol security. Due to these factors, Bitcoin continues to be a very problematic cryptocurrency for many customers. Now, efforts are being made to lessen the risks that emerge throughout the mining process. The user education and a change in user mindset are still necessary because the Bitcoin cryptocurrency payment system and blockchain financial statements are still in their early phases.

References

1. Conti M, Sandeep Kumar E, Lal C, Ruj S (2017) A survey on security and privacy issues of bitcoin. IEEE Communications Surveys and Tutorials 20(4): 3416-3452.
2. Zhang R, Xue R, Liu L (2020) Security and privacy on blockchain. ACM Comput Surv 52(3): 1-34.
3. Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, et al. (2013) A fistful of bitcoins: characterizing payments among men with no names. Communications of the ACM 59(4): 86-93.
4. Feng Q, He D, Zeadally S, Khan MK, Kumar N (2019) A survey on privacy protection in blockchain system. J Netw Comput Appl 126: 45-58.
5. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA (2015) SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. 2015 IEEE Symposium on Security and Privacy, San Jose, California, USA, pp. 104-121.
6. Zaghloul E, Li T, Mutka MW, Ren J (2020) Bitcoin and blockchain: security and privacy. IEEE Internet Things J 7(10): 10288-10313.