RESEARCH ARTICLE

ADHYAYAN Volume 13, Issue 2, 2023 Print ISSN: 2249-1066 Online ISSN: 2455-8656

The Literature Review of Blockchain and Its Applications

Gopal Mishra*, Yachika Dixit

School of Management Sciences Lucknow, Uttar Pradesh, India.

Abstract

Blockchain has been viewed as a breakthrough and an innovative technology due to its privacy, security, immutability, and data integrity characteristics. This technology enables cryptographically secure and anonymous financial transactions among the user nodes of the network enabling the transactions to be validated and approved by all the users in a transparent environment. It is a revolutionary technology that earned its emerging popularity through the usage of digital cryptocurrencies. Even though blockchain holds a promising scope of development in the online transaction system, it is prone to severalsecurity and vulnerability issues. In this paper, blockchain methodology, literature review, its applications, and security issues are discussed which might shed some lighton blockchain enthusiasts and researchers.

Keywords: Blockchain, decentralized, distributed, ledger, security, anonymity.

Adhyayan: A Journal of Management Sciences (2023); DOI: 10.21567/adhyayan.v13i2.02

Introduction

Blockchain technology is a peer-to-peer architecture network. It is decentralized and comprised of a series of blocks recognized, which is why blockchain. After the initial concept derived and implemented by Satoshi Nakamoto in Bitcoin, Blockchain has become a topic of interest among the research (Nakamoto, *et al*., 2008; Blockchain, 2019). Moreover, its characteristics have expanded its applicability to a greater extent. It is also referred to as distributed ledger technology, which preserves the calculation of all the nodes in each of them. Since the ledger is shared; reliability is not a concern in the network. Moreover, the blocks include hash code, which is a unique and unchangeable value derived using the complex mathematical hash function. For this reason, immutability is ensured (V. P. *et al*., 2018). Among other characteristics, transparency is ensured by the reasons mentioned above. As the transaction does not happen in the traditional way as in with individual real user ID and address, there are several scopes to make both the sender and the receiver anonymous. The absence of central authority makes the whole system autonomous to some extent (Joshi, *et al*., 2018). These reasons have made the concept of blockchain as an emerging technology to be implemented in various fields.

Various Types of Blockchain: Blockchain is the foundation of the digital cryptocurrency, Bitcoin. It has raised its sheer importance in the digital world by holding its critical character traits of decentralization, immutability, anonymity, and suitability for the e-money transaction process. There are primarily four types of blockchains to be considered.

Corresponding Author: Gopal Mishra, School of Management Sciences Lucknow, Uttar Pradesh, India, e-mail: gopal@smslucknow.ac.in

How to cite this article: Mishra, G., Dixit, Y. (2023). The Literature Review of Blockchain and Its Applications. Adhyayan: A Journal of Management Sciences, 13(2):6-10.

Source of support: Nil

Conflict of interest: None

Public Blockchains

A public blockchain is an open-source, decentralized blockchain with no restriction of users that can participate in the network. No individual entity has control over the network instead anyone can join the network and read/write/audit the blockchain with no order for processing the transactions (What are the Different, 2019). Public blockchains, by their design, are ideal for protecting user anonymity. Since this type of blockchain is publicly accessible to all users, the decisions here are made by several consensus algorithms such as Proof of Work (POW), Proof of Stake (POS), and many more (Different Types of Blockchains, 2017). Moreover, the public blockchain platform maintains an incentive mechanism predefined in the protocol through some gaming theory, that is, the participants in the network are economically rewarded for maintaining the best of behaviors and honesty in the system (Shermin, 2019). Public Blockchain platforms include Bitcoin, Ethereum, Litecoin, etc.

Private Blockchains

Private blockchain restricts the users who can participate and make a transaction in the network. A group of individuals or organizations that are permitted to enter the network holds control of the blockchain network. Thus a private blockchain from the very beginning has user identity to some extent for determining their respective tasks in the networks and their controlling access such as reading/writing/auditing of specific information in the blockchain. The design of the private blockchain, in contrast to the public blockchain, is more centralized, so the decisions are made by an in-charge who assigns several rights to the participants in the network (Different Types of Blockchains, 2017). However, the centralized architecture of a private blockchain makes it more prone to security breaches. Organizations or corporations that need scalability, privacy protection for data, and regulatory standards for state compliance employ the private blockchain (Shermin, 2019). Thus, blocks of information are accessible to particular members in the network who meet predetermined conditions for internally evaluating and confirming the transactions. Private blockchain platforms include Hyperledger, Hashgraph, Corda, and many others.

Consortium/Federated Blockchains

A consortium blockchain is a partially decentralized blockchain, which means it lies in between a public and a private blockchain. Consortium blockchain partially exhibits the properties of both public and private blockchains, but it retains most of the characteristics of a private blockchain. Unlike a private blockchain, the network of a Consortium blockchain is operated by a group of entities (Joshi, *et al*., 2018). As opposed to a public blockchain, a consortium blockchain prevents access to the network and only permits users to get access with the network administrators' consent. This type of blockchain is often referred to as a "semi-private" blockchain since the authority of the network is given in advance to selectively predefined nodes based on several consensus algorithms. Generally, it is used in business organizations having several business partners. Examples of consortium platforms include R3, Corda, etc.

Hybrid Blockchains

A hybrid blockchain is a combination of both the public blockchain and the private blockchain. It combines the advantages characteristics of each blockchain, respectively, that is, a hybrid blockchain inhibits the privacy benefits of a private blockchain and transparency benefits of a public blockchain according to necessity. The patented Interchain ability gave rise to the hybrid nature of the blockchain enabling the hybrid blockchain to have multiple chain networks of blockchains (What are the Different, 2019). The hybrid blockchain is not entirely open to everyone; certain restrictions are posted while allowing participants to enter the hybrid blockchain network. This hybrid characteristic of this platform gives organizations properly controlled access of their data in the network thus making the system more flexible and secure without compromising privacy. Even though the hybrid blockchain is controlled by a group of individuals, the transactions made are kept private and yet can be verified whenever needed. This upholds the immutability of the transactions (Hybrid Blockchain, 2018). Hybrid blockchain platforms include Dragonchain.

Methodology

Blockchain technology works by creating an environment that is secure and transparent for the financial transactions of virtual values such as Bitcoin. Hash codes of each block keep records safe in the blockchain. This is mainly because irrespective of the size of the information or document, the mathematical hash function provides a hash code of the same length for each block. So, attempting to change a block of information would generate a completely new hash value (How Blockchain Technology Works, 2019). A network that is open to everyone and concurrently maintains user anonymity undoubtedly raises trust issues regarding the participants. So, to build trust the participants need to go through several consensus algorithms such as Proof of Work and Proof of Stake. Bitcoin is a digital cryptocurrency that uses blockchain technology, the first of its kind (Amaba, *et al*., 2017). It is a digital store of value that enables peer-to-peer transactions over the Internet without the intervention of a third party. The blockchain network is a decentralized structure that consists of scattered nodes (computers) that inspect and validate the authenticity of any new transactions that attempt to take place. This collective agreement is done through several consensus models by the process of mining. The process of mining demonstrates that each node trying to add a new transaction has gone through and solved the complex computational puzzle through extensive work and deserves to get a reward in return for their service. For the validation of a transaction, the network must confirm the following conditions:

The sender account holds sufficient Bitcoin balance that it intends to transfer. The amount intended to transfer has not already been sent to some other recipient. Once a transaction has been validated and agreed upon by all the nodes, it then gets added to the digital ledger and protected using cryptography that uses a public key that is accessible to all the other nodes and a private key that must be kept secret (Wachal, 2019). To maintain the transactions using digital currency in the blockchain network, we need to have an understanding of the digital wallet which is used to store, send, and receive digital currency. A digital wallet or a cryptocurrency wallet is a string of letters and numbers forming a public address associated with each block in the blockchain. This public address is used whenever a transaction takes place; that is, the Bitcoin currency is assigned to the public address of the specific wallet. However, to prove the ownership of the public address there is a private key associated with the wallet that serves as the user's digital signature that is used to confirm the processing of any transaction. The user's public key is the shortened version of his private key generated through complex and advanced mathematical algorithms (Baliga, 2017).

For example, let us consider someone is trying to send you some digital currency such as Bitcoin, as the transaction is being processed, the private key in your wallet should match the crucial public address of your wallet that the currency has been assigned to. If both these keys match, then the digital currency amount is transferred to the public address of your wallet.

Block Structure

Main Data: Blocks will contain transaction data. This transaction data depends on the usage factor of the blockchain, that is, the relevant services for which the blockchain is implemented. For financial institutions like banks, financial transaction data will be stored. Timestamp: The timestamp will also exist in the blocks. Here, the timestamp refers to the date and time when a particular block is generated. Hash: The hash corresponding to each block is a unique identifier that is generated using a cryptographic hash algorithm such as SHA-256. The current block's hash and the previous block's hash are stored in the block. Hashes make the blocks immutable. Hashes are generated using the Merkle tree function. It is stored in the header of the block. Merkle tree root hash It consists of all the hash values relating to every transaction that took place in a block and performs a mathematical hash calculation generating a 64-character code (Salah, 2018). The hash of the Merkle tree root of all the transactions in the block is stored for effective processing and easier verifying of data within a short time. Nonce A nonce is a randomly generated 4-byte number that can be used once in a cryptographic transaction process. During the mining process in a proof-of-work algorithm, the nonce is used as a counter that the miners are trying to solve in order to generate a new block. The aim is to calculate a hash value less than a given target value, which depends on the difficulty of the complex mathematical problem.

Application of Blockchain

blockchain application can be applied to many sectors in Bangladesh. It either uplifts the existing process or creates new technologies. It will change our lives and protect us from fraud, thief, or any crime. Blockchain provides a secure way of sending digital assent without even knowing third parties. In many sectors, we can use blockchain. Some of the sectors are:

Healthcare

Security of Personal information like health data is very important for everyone. These health related information are very valuable as pharmacy companies thrive on these data. Most of the time these data are kept on a hospital server and not in a secure environment too. To prevent health data from falling on the wrong hands and to prevent misuse of these data public blockchain can be used where health data can on be seen by the doctors if the owner of the data i.e. the patient permits it (Lin and Liao, 2017). Building a system like this will ensure proper security for these data.

Equity Crowdfunding

Getting money from a crowd or supporters of a company/product in exchange of equity/shares in that company is known as equity crowdfunding. As people from different backgrounds participate in these crowdfunding and they follow different rules and regulations, it becomes very tough to maintain policies. Also, not all people will trust the party that is handling all the transactions thus affecting the total amount of money generated. To maintain a fair ground among fundraisers and investors blockchain technology can

Table 1: Some of the attacks and their details

S. No.	*Name of the Organization/Groups*	*Details of 51% attack*
1	Ghash.io	Exceeded 50% in 2014. Later nodes voluntarily dropped to preserve the integrity
2	Krypton and Shift	Etherium-based blockchain was attacked in August 2016
3	Bitcoin Gold	Attacked during August 2018, Stole 18 Million dollar worth of Bitcoin Gold

be used. Blockchain will remove differences due to regulatory laws and bring all the parties together in a systematic way (Zhu & Zhou, (2016).

Banking

It needs to use blockchain in the tax sector. Blockchain can make a significant contribution in the tax sector. Our current tax collected system is not so trusted. Blockchain can change the whole system, the way our tax is collected. As blockchain provides accurate information, so if we use this in the tax sector then it will be beneficial for all the people. Sometimes people argue about paying taxes. They denied paying taxes and claim false information. Blockchain is an immutable system. It gives the real value of the system. When someone lying about paying tax, blockchain can immediately give the correct information about tax. As this is immutable people could change the information if they want. It is impossible to change the complete information, so when people lying about paying the tax they will be caught immediately. Blockchain can detect fraud easily. It can reduce VAT fraud (Zhu, & Zhou, 2016). Now, in the present system, tax authorities have to take information from taxpayers one by one. It is not only challenging but also not safe. It could not give real data. Nevertheless, if blockchain will used in tax system then it is not necessary to collect information from the taxpayer. Authorities can see the result in a computer, and that result will be real and genuine. Security of money is important for everyone. So people use banks to keep their cash safe. But even banks cannot provide absolute security. But, nowadays most of our money is not real money but rather a digital form of money. Digital things must be kept on a server somewhere operated by software. Just like any other software banks get hacked too. In the blink of an eye, money can vanish from a bank. Blockchain is used to prevent hackers from getting money from bank. A banking system totally based on Blockchain is very hard to hack and steal money. Banking based on Blockchain makes sure that even if a server gets hacked hackers cannot steal right away because they would also have to hack all the other servers that contain the same information as the hacked server.

Smart Power Grid

Blockchain is also used in a power grid to supply electrical power to customers. This eliminates fraud. Everyone's power consumption will be recorded in the blockchain ledger. Since everyone has the same ledger no one just claims they used less power than they actually have. Authority also cannot overcharge a customer.

Smart Delivery System

Making sure we get the right product we ordered online can be a tough job for distribution companies. Delivery relying on third parties can be easily hacked, a single point of failure. Once compromised attacker can procure an item that was intended for others. Blockchain can remedy this using smart (Table 1) (Salah, 2018). But using blockchain for every single item is not practical. There is no need to create a Blockchain system for grocery delivery instead we need one for very valuable items like gold, statues, documents etc. Smart contract-based Blockchain can make sure that the right person gets the

item. Secret code can be shared between seller and buyer. Once item reaches its destination previously shared secret code will complete the contract. This way both buyer and seller can make sure that the transaction was successfully completed.

Conclusion

The future of Blockchain predictively holds some significant advancements in technology. As the future scope, the foremost priority is to handle the several security issues that arise from different types of blockchain network such as private blockchain network which is often implemented by business organization and big enterprises.

The concept of private blockchain makes the network centralized thus making the network vulnerable to cyberattacks. Moreover, consensus algorithms such as PoW implemented in blockchain have several drawbacks. It requires an enormous amount of energy for the computation of hash. So trying to develop an improved consensus algorithm would result in a cost-effective and more efficient blockchain network (Saraswat, 2019).

References

Nakamoto, S., Bitcoin (2008). A Peer-to-Peer Electronic Cash System, www.bitcoin.org,

Blockchain Architecture Explained: How It Works and How to Build It MLS Dev. https://mlsdev.com/bl og/156. 2019.

V. P. Mrs. Harsha, G.R. Mrs. Kanchan, V.T. Malati (2018). A Study on Decentralized E-Voting System Using Blockchain Technology, International Research Journal of Engineering and Technology, Vol. 5(11), 48-53.

A. Prashanth Joshi, M. Han, Y. Wang, and Kennesaw (2018). A survey on security and privacy issues of blockchain technology, Mathematical Foundations of Computing, vol. 1(2), 121–147.

What are the Different Types of Blockchain (2019) https://dragonchain.com/blog/differences.

Different Types Of Blockchains In The Market and Why We Need Them,"CoinSutra - Bitcoin Community, 05-Dec-2017. [Online]. Available: https://coinsutra.com/different-typesblockchains/. [Accessed: 03-Jun-2019].

Shermin, V. (2019). Blockchains & Distributed Ledger Technologies. BlockchainHub. Accessed on: Apr 12, 2020.

"Hybrid Blockchain- The Best of Both Worlds," 101 Blockchains, (2018).

"How Blockchain Technology Works. Guide for Beginners," Cointelegraph. (2019).

D. B. Amaba, P. C. Leed, D. T. Ahram, D. A. Sargolzaei, D. J. Daniels, and D. S. Sargolzaei (2017). Blockchain Technology Innovations, p. 5.

M. Wachal, "What is a blockchain wallet? - SoftwareMill Tech Blog," Medium, 02-Apr-2019. [Online]. Available: https://blog.softwaremill.com/what-is-a-blockchain-walletbbb30fbf97f8. [Accessed: 15-Jun-2019]. "eCoinnomy - What is Blockchain?," e Coinnomy.

D. A. Baliga (2017), Understanding Blockchain Consensus Models.

I.-C. Lin and T.-C. Liao (2017). A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security, vol. 19(5), 653–659.

Zhu, H., & Zhou, Z. Z. (2016). Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. Financial innovation, 2(1), 1-11. https://www.allerin.com/blog/heres-why-the-tax-sectordesperately-needs-blockchain-now.

H. R. H. a. K. Salah, (2018), Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters," vol. 6, 46781-46793.

N. Saraswat (2019)"consensus-mechanisms-as-detailed-andconcise-as-possible-b3da79f85f6 6," hackernoon, https://hackernoon.com/consensus-mechanisms-as-detailedand-concise-as-possible-b 3da79f85f66.