BLOCK CHAIN TECHNOLOGY IS A FUTURE OF SECURE ONLINE TRANSACTION

Laxmi Shankar Awasthi[1], Karuna Shankar Awasthi[1], and Anand Kumar Rai[2*]

[1]Deptt. of Computer Science, Lucknow Public College of Professional Studies, Lucknow.
[2]Deptt. of Computer Science, Mumtaz Post Graduate College, Lucknow.

[*]Corresponding Author: anandrai07@gmail.com

ABSTRACT: Blockchain technology is revolutionary. It will make life easier and safer, change the way personal information is stored and how to make better transactions and services. Blockchain technology creates a permanent and consistent record of everything that is done. This is a secure system, which we plan to use the current secure online trading system. The online payment gateway is prone to hackers where the attacker can disrupt the network, thus causing financial loss. To record a transaction, we use proof of a function algorithm that deactivates the computer for the attacker to change. Digital signatures provide part of the solution to ensure the security and integrity of blockchain data.

KEYWORDS: Blocks, Blockchain, Block time, Block fork, Hash.

INTRODUCTION: A blockchain is an emergent list of records, called blocks, linked together using cryptography it is also described as "reliable and completely independent peer-to-peer data storage" distributed on a network of participants often called nodes. Each block contains a cryptographic hash of the previous block, timestamp, and transaction data (usually represented as a Merkle tree). A timestamp confirms that the transaction data was present when the block was published to enter its hash. As each block contains information about the previous block, they form a series, with each additional block reinforcing those before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be replaced by replacement without changing all of the following blocks. Blockchains are usually managed by a peer-to-peer network to be used as a publicly distributed platform, where nodes collectively follow the process of communicating and validating new blocks. Although blockchain records are as flexible as forks are possible, blockchains can be considered as secure in design and serve as an example of a highly distributed Byzantine computer program with high tolerance. The blockchain was developed by a person (or group of people) Satoshi Nakamoto in 2008 to act as a public transaction logger for cryptocurrency bitcoin. [**1**] Satoshi Nakamoto's identity is still unknown. The introduction of the bitcoin blockchain has made it the first digital currency to solve the problem of spending money twice without the need for a trusted authority or a central server. The bitcoin design has promoted other applications [**1**] [**2**] and blockchains that are publicly read and widely used by cryptocurrensets. The blockchain is considered a form of payment train. Private blockchains have been proposed for commercial use but Computer world has called for the marketing of such privately held blocks without the appropriate security model "snake oil". However, some have argued that allowed blockchains, if carefully designed, could be allocated more power and therefore more secure than doing without permission.

LITERATURE REVIEW: Cryptographer David Chaum first proposed a blockchain law in his 1982 book “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups. Scott Stornetta. They wanted to use a system where the time stamps of the texts were not disturbed. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle Trees into this project, which improved their performance by allowing several text certificates to be collected in one block[**3**][**4**][**5**]. The first blockchain was invented by a man (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto has improved the design in a significant way using a method similar to Hashcash to create timelines without having to be signed by a reliable team and introducing a complex parameter to stabilize the rate by which the blocks are placed in the chain. The design was launched the following year by Nakamoto as a major component of the cryptocurrency bitcoin, where it serves as a public logger of all network activity [**2**][**6**]. In August 2014, the file size of the bitcoin blockchain, which contained records of everything done on the network, reached 20 GB (gigabytes). By January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. Lower size exceeded 200 GB by early 2020. The words block and series were used separately in Satoshi Nakamoto's first paper, but became known as a single word, blockchain, in 2016. According to Accenture, the widespread use of innovation theory suggests that blockchains achieved a 13.5% acquisition rate within financial services in 2016, thus reaching the first phase of subscribers. Industrial trading groups have joined the creation of the Global Blockchain Forum in 2016, which is an initiative of the Chamber of Digital Commerce. In May 2018, Gartner found that only 1% of CIOs exhibited any type of blockchain acquisition within their organizations, and only 8% of CIOs had a short period of "planning or [considering] active blockchain testing". In 2019 Gartner reported that 5% of CIOs believe blockchain technology is ‘changing the game’ in their business [**5**]. A blockchain is a distributed, and often public, digital book containing records called blocks that are used to record transactions on multiple computers so that any block involved can be changed backwards, without changing all of the following blocks. This allows participants to verify and evaluate transactions independently and low cost. The blockchain website is managed independently using a peer-to-peer network and a distributed timestamp server. The design of blockchain facilitates robust performance where participants' uncertainty regarding data security is minimal. The blockchain is defined as the exchange rate protocol. The blockchain can retain title rights because, when properly designed to provide information on an exchange agreement, it provides a record that enforces the offer and acceptance [7].

ARCHITECTURE OF BLOCK CHAIN:

BLOCKS: Blocks hold collections of valid transactions that are missed and placed on the Merkle tree. In Figure 1, the blockchain structure is shown. Each block inserts a cryptographic hash of the previous block into the blockchain, which links the two. Connected blocks form a series. This repetition process ensures the integrity of the previous block, all the way back to the original block, and known as the genesis block. To ensure the integrity of the block and the data contained in it, the block is usually signed digitally [**3**][**4**][**8**]. Sometimes different blocks can be made at the same time, forming a temporary fork. In addition to secure hash-based history, any blockchain has a specific algorithm for inserting different versions of history so that a person with high scores can be selected over others. Blocks that are not selected for chain placement are called orphan blocks. Peer-supported peer-to-peer database has different types of history from time to time. They maintain only the highest quality database known to them. Whenever a peer gets a high scoring type (usually an older version with one new block added) they extend or rewrite their details and pass on their peers' progress. There is no absolute guarantee that any particular entry will remain a good version of history forever. Blockchains are built to add points to new blocks on older blocks and are encouraged to stretch with new blocks rather than override old blocks. Therefore, the chances of replacement are greatly reduced as more blocks are built on top of them, eventually becoming much lower. For example, bitcoin uses a performance verification system, in which a chain with highly accumulated evidence of performance is considered appropriate by the network. There are many methods that can be used to show a sufficient level of calculation. Within the blockchain computation is done more efficiently than in the traditional and divided system.

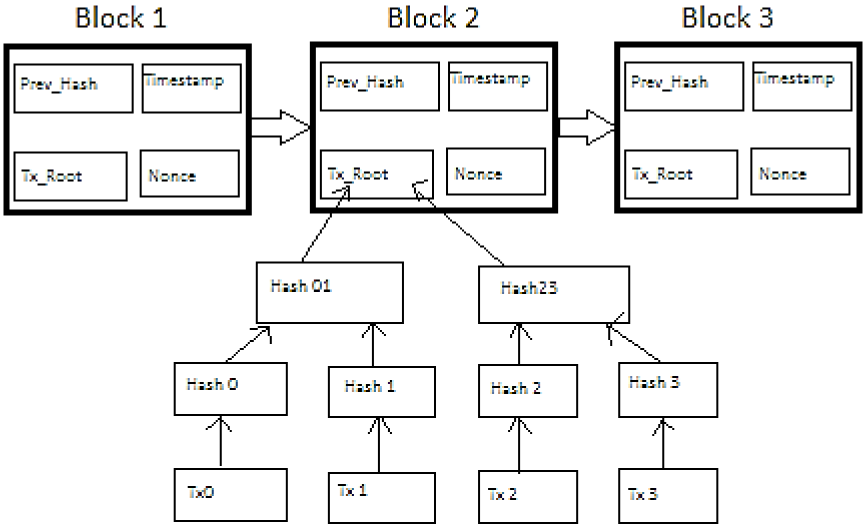

Figure 1. Block Chain Architecture

BLOCK TIME: Block time is the average time it takes for a network to produce a single block in a blockchain. Some blockchains create a new block every five seconds. At the time of block completion, the entered data is verified. In cryptocurrency, this happens when transactions occur, so a short block period means a quick transaction. Ethereum blocking time is set to be between 14 and 15 seconds, while bitcoin is within 10 minutes [**3**][**4**].

HARD FORKS: The hard fork is a change in the law so that software that guarantees according to the old rules will see the blocks produced according to the new rules as invalid. If there is a hard fork, all nodes are intended to operate according to the new rules that need to be upgraded for their software. If one group of nodes continues to use the old software while the other nodes use the new software, it may be permanently cracked. For example, Ethereum is having a hard time “finalizing” investors in the DAO, who were hacked to exploit the vulnerability of its code. In this case, the fork led to a split in the creation of Ethereum and Ethereum Classic chains. In 2014 the Nxt community was asked to consider a heavy fork that could lead to the recovery of blockchain records to reduce the effects of the 50 million NXT theft on large cryptocurrency exchanges. The proposal for a heavy fork was rejected, and some of the funds were obtained after negotiations with the payment of a ransom. Alternatively, to prevent permanent fragmentation, most nodes using the new software can revert to the old rules, as happened with bitcoin split on 12 March 2013. The latest hard-working example was made with Bitcoin in 2017, which led to the fragmentation that created Bitcoin Cash. Network fragmentation is caused by disagreements over how to maximize transactions per second to meet demand.

DECENTRALIZATION: By storing data throughout the peer network, the blockchain eliminates many of the risks that come with centralized data. [**7**] The intermediate blockchain can use the communication message to transmit and distribute the network. One risk of a lack of judicial separation in a so-called "51% attack" area where the middle business can gain control over more than half of the network and can use that particular blockchain record at will, allowing double spending. Peer-to-peer blockchain networks do not have the average risk points that computer crackers can use; similarly, it has no central place for failure. Blockchain security methods include the use of public key cryptography. The public key (long, random number series) is a blockchain address. The value tokens sent across the network are recorded as that address. A private key is like a password that gives its owner access to their digital assets or other means of communication and various skills that blockchains currently support. Data stored in a blockchain is generally considered to be invalid [**9**][**10**]. Every node in a distributed system has a copy of the blockchain. Data quality is maintained by high duplication of database and computer trust. No "official" copy is included and no user is "trusted" more than any other. Transactions are broadcast online using software. Messages are sent with the best effort. Mining domains secure transactions, insert them into the building blocks, and then distribute the completed block to other nodes. Block chains use various time-saving schemes, such as proof of work, to make a serial change. Other methods of consensus include the validation of the pole. The growth of shared blockchain growth carries with it the risk of merger because the computer resources needed to process large amounts of data are more expensive.

OPENNESS: Open blockchains are easier to use than other traditional ownership records, which, while open to the public, still require physical access to view. Because all original blockchains were not authorized, controversy has arisen over the definition of blockchain. The issue in this ongoing debate is whether a confidential system with guaranteed and authorized (authorized) certificates by the middle authority should be regarded as a blockchain. Sponsors of approved or secret chains claim that the word "blockchain" can be used in any data structure that encloses data in blocks with a timestamp. These blockchains serve as a distributed version of multiversion multi-currency management (MVCC) for databases. Just as MVCC prevents two transactions from simultaneously converting one item into a database, blockchains prevent two transactions from using a single result in a blockchain. Nikolai Hampton of Computerworld said that "many in-house blockchain solutions will not be just complex information details," and "without a clear security model, related blockchains should be considered suspicious [**3**][**9**]."

BLOCKCHAIN ANALYSIS: Analysis of public blockchains has become increasingly important with the popularity of bitcoin, Ethereum, litecoin and other cryptocurrensets. The blockchain, if public, provides anyone who wants access to the screening and analysis of chain data, provided it is provided to an experienced person. The process of understanding and accessing the crypto movement has been a problem for many cryptocurrency, crypto-exchanges and banks. The reason for this is the suspicion of a blockchain-enabled cryptocurrensets that enable the illicit trade in the black market for drugs, weapons, money laundering etc. A common belief has been that cryptocurrency is confidential and unaccountable, which has led many leaders to use it for illegal purposes. This is changing and now specialized technology companies are providing blockchain tracking services, making crypto exchanges, law enforcement and banks better aware of what is happening with crypto currencies and fiat crypto trading. These developments, some say, have led criminals to prioritize the use of new cryptos such as Monero. The question is about public access to blockchain data and personal privacy of the same data. It is an important issue in cryptocurrency and ultimately in the blockchain [**3**][**5**][**11**].

CONCLUSION AND FUTURE TREND: In this study we have emphasized on blockchain secure online transactions. Undoubtedly we can claim that blockchain is a secure technology for the online secure transactions. Hackers can never create any trouble. For the implementation of this technology in the interest of general public secure banking transaction, few more research are needed regarding the hardware resource. In future blockchain is the only way for online secure banking or sensitive data transactions.

REFERENCES:

1. Ahn, J.-w., Chang, M. D., Kokku, R., and Watson, P. (2018). “Blockchain for Open Scientific Research”. Patent Number: 20180323980, Armonk, NY.

2. Abraham, I., and Mahlkhi, D. (2017). The blockchain consensus layer and BFT. Bull. EATCS 123, 1–22. Available online.

3. Arnold, L., Brennecke, M., Camus, P., Fridgen, G., Guggenberger, T., Radszuwill, S., et al. (2019). “Blockchain and initial coin offerings: blockchain's implications for crowdfunding,” in Business Transformation Through Blockchain, eds H. Treiblmaier and R. Beck (Cham: Palgrave Macmillan), 233–272. doi: 10.1007/978-3-319-98911-2_8.

4. Aste, T., Tasca, P., and Di Matteo, T. (2017). “Blockchain technologies: the foreseeable impact on society and industry”. Computer 50, 18–28. doi: 10.1109/MC.2017.3571064.

5. Bartling, S., and Friesike, S. (2014). “Towards another scientific revolution,” in Opening Science, Chapter 1, eds S. Bartling and S. Friesike (Cham: Springer), 3–15. doi: 10.1007/978-3-319-00026-8_1.

6. Abeyratne, S., and Monfared, R. (2016). Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. 5, 1–10. doi: 10.15623/ijret.2016.0509001.

7. Ali, M., Nelson, J., Blankstein, A., Shea, R., and Freedman, M. J. (2019). The Blockstack Decentralized Computing Network. Available online at: https://blockstack.org/whitepaper.pdf.

8. Altunay, M., Avery, P., Blackburn, K., Bockelman, B., Ernst, M., Fraser, D., et al. (2011). A science driven production cyberinfrastructure–the open science grid. J. Grid Comput. 9, 201–218. doi: 10.1007/s10723-010-9176-6.

9. Benčić, F. M., and Podnar Žarko, I. (2018). “Distributed ledger technology: blockchain compared to directed acyclic graph,” in 2018 IEEE 38th International Conference on Distributed Computing Systems.

10. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., et al. (2014). “Zerocash: decentralized anonymous payments from bitcoin,” in 2014 IEEE Symposium on Security and Privacy (San Jose, CA), 459–474. doi: 10.1109/SP.2014.36.

11. Ihle, C., and Sanchez, O. (2018). “Smart contract-based role management on the blockchain,” in Business Information Systems Workshops, eds W. Abramowicz and A. Paschke (Berlin: Springer International Publishing), 335–343. doi: 10.1007/978-3-030-04849-5_30.