International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-7, Issue-4,2020 Regular Edition E-ISSN: 2349-7084

Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain)

Dr. M. R. Arun[1*] , Prof. M. R. Sheeba[2], Prof. F. Shabina Fred Rishma[3]

Associate Professor, ECE, PBR Visvodaya Institute of Technology and Science , Nellore, India[1]
Assistant Professor& RS, CSE, Manonmaniam Sundaranar University, Tirunelveli, India[2]
Assistant Professor, CSE, Cape Institute of Technology, Levinjipuram, India[3].

e-mail: mrarunresearch@gmail.com, sheebasjustus@gmail.com, fredrishma@gmail.com

Corresponding Author: mrarunresearch@gmail.com

Available online at: http://www.ijcert.org

Received: 26/04./2020, Revised: 29/04/2020, Accepted: 1/May/2020, Published: 08/May/2020

Abstract:- With the rapid advancement in technological innovation, block Chain has become one of the hottest transformative techniques in the internet domain in recent times. As considered to be a decentralized, distributed and highly encrypted technology in data transfer, the blockchain has restored the trust for secured business transactions by the sophisticated cryptographic algorithm. Here the protocol validates that all nodes are merely synchronized with one another, thus providing security, anonymity, and data integrity without the requirement of any other third party intrusion. Block chain technology which is also known as DLT (Distributed Ledger Technology) that is a great platform for non-physical money transaction such as bitcoin and other online crypto currencies. It is seen as emerging foundational security-based technology having enormous potential across different sectors. Blockchain as a decentralized mode useful for a peer-to-peer network without the essential of any central or controlling authority server. This will, in general, reduce transaction costs, improved security, and execute the financial transaction in real-time. Block chain is significant and not the same as of now existing techniques. Since it empowers disseminated, independent decreases grating in business exchanges with safety and shares decentralized records, this paper gives a discussion on the comparative analysis of block chain technology with other existing technologies.

Keywords: Block Chain, Peer-to-peer, Bitcoin, Hashgraph, DAG, Holochain, Cryptography, Cyber security, DLT, Cryptocurrency

1. Introduction

In recent days we are supposed to hear a new technology that is used in cryptocurrency to maintain security in transactions. The cryptocurrency, which is the digital currency system that enables international monetary transactions between two end-users without the requirement for another intermediate transaction agency [1]. In the financial sector, it has achieved huge prominence in the world economy. Bitcoin is an open-source first mere application of blockchain technology. It is just a

decentralized digital currency, appeared on 3rd January 2009. To say about block chains, they are databases that stores data in terms of Blocks. In total contrast, with customary (SQL or NoSQL) databases of the client-server network that are controlled by single-point access, and it requires central administrator [2]. Blockchains are more reliable and secure than relational databases in some ways, and less secure in others.

Block chain is a decentralized and incorruptible distributed ledger technology, where blocks contain a bundle of transaction data that are affixed together by cryptographic hash. Blockchain network often consists of thousands of nodes. Each node is acting as another admin that is used to support the network [3]. Here each node validates and verifies the new increases to the block chain record and is proficient in entering new blocks of data into the distributed database technology. All entire participating nodes authenticate transactions that are represented online as a "Block" that originates from a node, and a set of information exchanges are added entirely into a block by a general "mining" hub. Any mining hub with extreme computational power solves a cryptographic mathematical puzzle. It can generate as well as broadcast a new block to every mining node in the network.

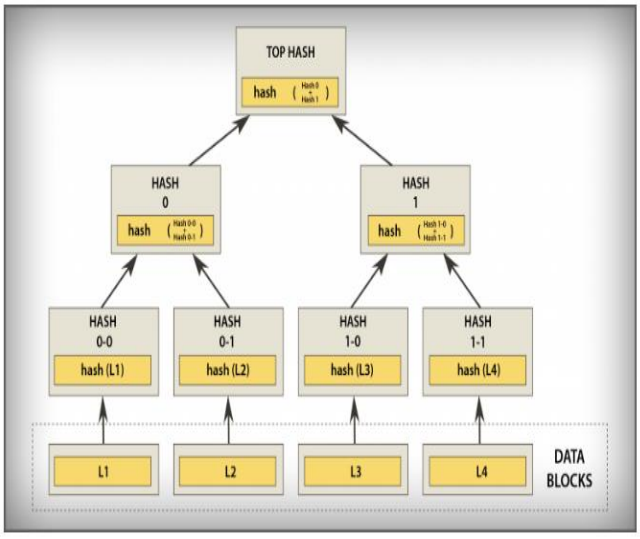

Figure 1: Block Hash Tree Structure

Block Hash = SHA2562(Hash of Prev Block|| Nonce||Tx Data Hash||Time||ver||Target value)

Here Target value is the considerable trouble level set by the network that requires the corresponding hash to be not exactly or equivalent to this value. Participating node retrieves, verifies, validates, and saves it as a new block, and hence there will be no master copy. Each block contains the value of timestamp, header details and the hash of the preceding block in the recent block, forming a sequence of blocks connected to each other in the form of the linked list, which is termed to be the blockchain [4]. If the preceding hashed block content is changed, the hash of preceding block also changes, therefore the hash pointer of the present block changes and this continues forever. This helps to detect easily if any changes occurred.

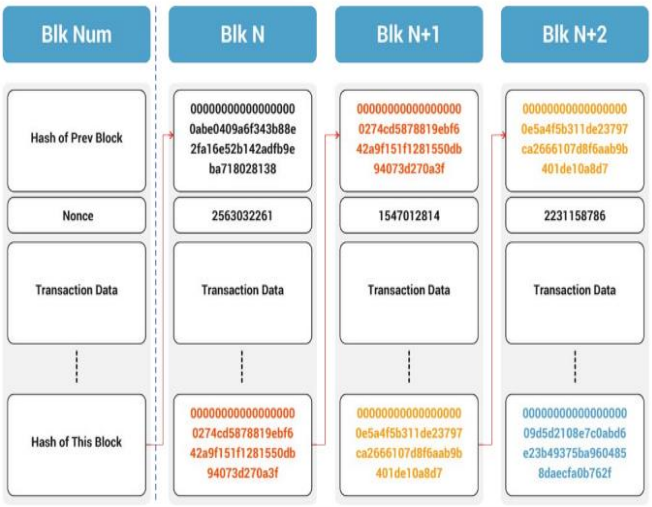

Figure 2: Block Hash Calculations

2. Block Chain Features

The features of block chain technology emphasize the security aspects in the data transmission process.

2.1 Decentralisation

Block chains are decentralized technology in nature meaning that no central authority or group that makes the system more secure. Everybody in the peer-to-peerr network has the distributed ledger copy data with them, so no one can carry out modification by their own and can track the data if they want to. These basic features of block chain allow trustworthy towards transparency and increased security.

2.2 Peer-to-Peer Network

Block chain specifically uses peer-to-peer (P-2-P) infrastructure network overlay on the Internet. Each node communicates with a set of neighbour nodes, each of which communicates with their neighbour nodes and so on. Any node can join and leave the network freely [5]. The transactions and blocks are communicated on the bitcoin P-2-P network and each receiving node forwards it to other neighbour nodes. Nodes that save a copy of entire block chain are called Full Nodes. SPV (simple payment verification) nodes checks the payments using only block headers. Mining nodes which generates blocks.

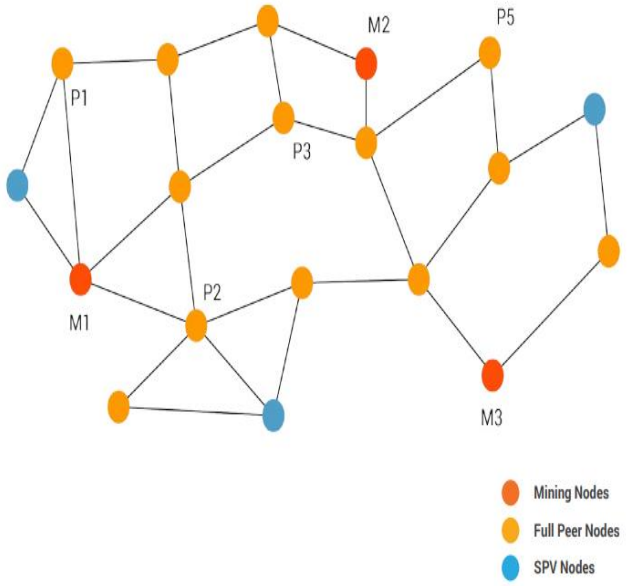

Figure 3: Peer-to-Peer Network

2.3. Immutable

The immutability property refers to the truth that any data/information, once written on the block chain's distributed ledger, cannot be changed. Sending an email is the best example of an immutability feature. Once anyone sends an email to a group of people that cannot revert it back. One possible way is, that the corresponding person have to ask each individual recipients to delete the email which is pretty tedious and time-consuming. This is the manner by which unchanging nature works. Once the blocks of data has been handled, it cannot be adjusted or modified later. In the event of block chain technology, if someone tries to modify the information of one block, then they'll have to modify the whole block chain following it as each block by defaults stores the hash value of its earlier block. Therefore change in one hash block will prompt to alter in all the accompanying mathematical hashes. It is exponentially more difficult for someone to modify all the hashing algorithm as it involves a great deal of computational capacity to do as such [6]. Consequently, the information put away in a block chain is more secure and so not susceptible to hack attacks happen due to immutability.

2.3 Tamper-Proof

With the peculiar property of immutability which is inbuilt in block chains, it ends up simpler to identify changes of any information. Blockchains is considered to be tamper-proof media transaction so that any alter in even one solitary block can be recognized and solve the problems smoothly. Hence there are two key ways of detecting, namely, blocks and hashes. Each cryptographic hash function related to a block is unique. You can think of it as like an advanced unique finger impression of a block. Any modification in the data will lead to modify in the cryptographic hash function. Since the hash function of one block is connected together to next hashed block, for hackers to make any changes, he/she will have to change hashes of the considerable number of blocks after that block, which is very muddled to do.

3. Traditional Databases

Traditional data management software has been mostly used globally by businesses across the world, practically in all industrial sectors for nearly around 40 years. These monolithic systems that operates with only one central server (main authority) that allows its users or its administrators to alter the existing data within the database tables. This increases failure and numerous performance-related issues. This central server is made up of administrators, who are the full privileges over giving access and granting permission authority figures within the system. A solitary administrator can give access or authorizations to another client, without the need of endorsement or accord from different administrators. With sufficient permissions, there are more chances to modify the information freely that are warehoused on the centralized server [7].

Traditional servers keep track of information up-to-date at a point in time. When information is updated or altered by someone, subsequent users will only see the newly updated latest version of the database records. There is no recorded archive of previous history of transactions or changes made, that leaves no trace of what has been modified or who has changed which particular table in a

database. Traditional databases use client-server network architecture [8]. Here, a client (also known as a user) can alter information, which is stored on a unified server. Control of the database stays with an assigned authority, which verifies a client's login credentials before giving access to the database. Since this authorization specialist is in charge of organization of the database, if the security of the expert is undermined, the information can be modified, or even erased by programmers.

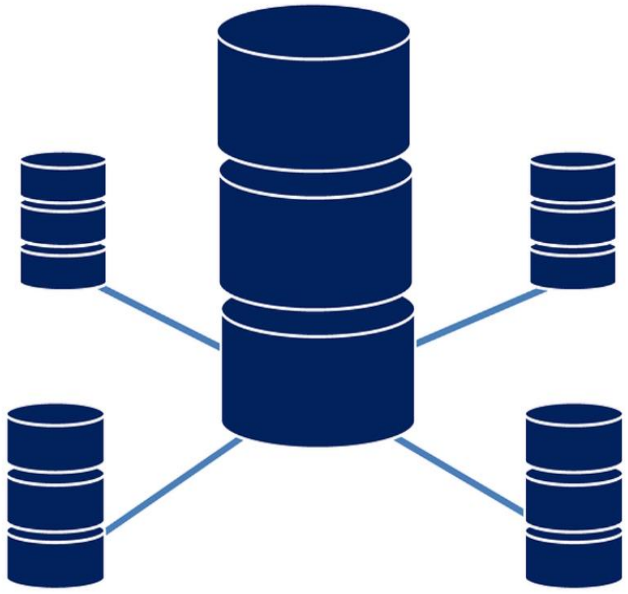

Figure 4: Traditional Databases / Client – Server Architecture

4. Other Existing Technologies

4.1. Directed Acyclic Graph (Dag)

DAG is an alternate technique that will defeat block chain issues. It has been touted as the next significant iteration of block chain technology. It has shown its potential to turn into the distributed ledger architecture of choice in the digital currency industry. Introductory version of Bitcoin was Block chain 1.0. Next the decentralized application Ethereum (Open Source) is Block chain 2.0 and Block chain 3.0 would be DAG [9].

4.2 Directed Acyclic Graph Structure

To reiterate, a DAG structure looks progressively like a web of individual transactions associated together with "edges" or, associated transactions moving forward in the same direction [10]. This differs totally from the design of block chain structure that groups' operations altogether in hashed blocks with chain formation. With the concept of DAG, transactions verify each other, the need for miners to secure the network is gradually eliminated, and so, fees are significantly dropped, with some DAG successfully testing feel less environments[11]. This is where DAG has the tremendous potential to knock the wind out of block chain's sails. Quick, adaptable, on-chain transaction exchanges are a blend of factors that block chain innovation still struggles to complete. However, DAG has demonstrated technologically that these things are possible in a manner that the block chain can't contend with. Most of the DAG projects have tested and it has the capability to process thousands of transactions per second successfully [12].

Another most important factor is the DAG that eliminates the requirement for miners to secure the network, as every transaction checks subsequent transactions. By doing this, the mining procedure, which is incredibly energy intensive, is totally eliminated, making DAG a more financially cordial light weight distributed record for transactions.

4.3 Directed Acyclic Graph vs Block chain

A DAG model works uniquely in contrast to a block chain [13]. A typical block chain expects miners to look after blocks, however, a DAG wouldn't require either verification of-work or blocks [14].

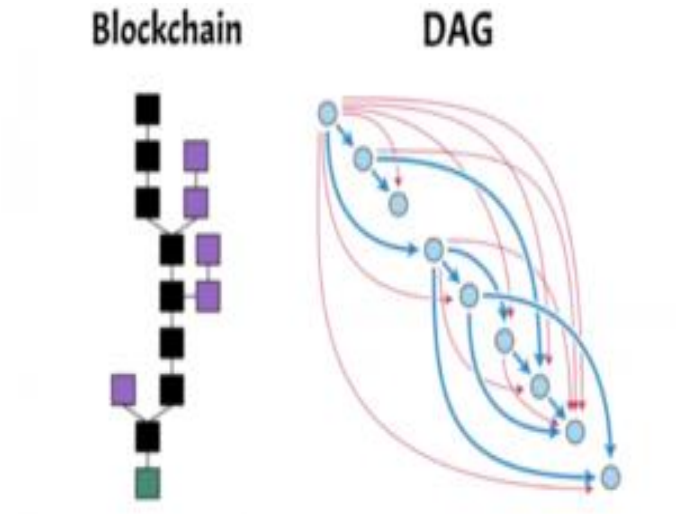

Figure 5. Block chain vs DAG

4.4 Quick Transactions

Because of its block less nature, the transactions run straight forwardly into the DAG networks. The entire process is lot quicker than those of block chains based on PoW and PoS.

4.5 No Mining Involved

There are no miners on DAG networks. The approval of transactions goes straight forwardly to the transactions themselves [15]. For clients, this means transactions go through almost in a fraction of seconds.

4.6 Friendly to Small Payments

With the headway of DAG, we're taking a gander at a future where advanced and least transaction expense chains are conceivable. That implies clients can send micro-payments without overwhelming charges like Bitcoin [16].

4.6 Hash Graph

Hash graph is a technique where multiple transactions are stored on the ledger with in the same timestamp [17]. Here all of the transactions are merely stored in parallel structure. Every record present on the ledger is referred as "Event"

4.7 Working

Hash graph uses a Gossip protocol to relay the information about a transaction. Once a specific transaction occurs, the neighbouring nodes they started sharing that information with the rest of other nodes, and after few time period, all the nodes came to know about the happened transaction [18]. With the help of "Virtual Voting" protocol, all the nodes validates themselves with corresponds to the transaction and then added itself to the ledger.

4.8. Holo Chain

Holo chain is a different kind of DLT that moves on from the data-centric structure to agent-centric structure.

4.9 Working

In this structure, every node present on the network has their own ledger that they maintain [19]. There isn't any global validation process, but the Holo chain network maintains a set of rules called the "DNA" to verify each individual's ledger.

5. Block chain vs Hash graph vs DAG vs Holo chain

The descriptive and functional variations among different technologies are illustrated. To add sense to the technology the mutual comparative differences among various cryptographic technologies which are in web applications to ensure safety and security of data transmission were tabulated below [7] [9] [19] in table 1

Table 1: Comparison among Block chain, Hash graph, DAG, Holo chain

Categories	Block chain	Hash graph	DAG	Holo chain
Mining	Participants have the ability to mint new tokens via different consensus mechanism	Nodes create consensus through Virtual Voting	The previous transaction validates the succeeding to achieve consensus	Nodes run on individual chains hence miners not needed to validate transaction
Efficiency (Transactions per second)	Highly limited in terms of scalability and TPS (3-4)	high scalability and high TPS (>250,000)	scalability and TPS are high (500-800)	limitless scalability and TPS
Data structure	Data structured in blocks validated by miners in the ecosystem	Virtual voting and Gossip validated by the majority	Data structure follow DAG transaction is independent	Data distributed among nodes no problem of N/W congestion

Validation of transactions	Miners have the power to postpone a transaction or cancel it entirely	Validation of operations is done as per consensus	Validation of transaction-based two previous transactions	Nodes by its own maintain ledgers hence no need of miners
Time of launch	Public usage in 2008	public usage in August 24 2018	In Nov 9th 2015	released on May 26, 2018
Applications	Bitcoin Ethereum	Swirlds NOIA	NXT Tangle ByteBall	Holochain
Copyright	Open Source	Patented	Open Source	Open Source
Validation Time	Order of minutes	Order of seconds	Order of seconds	Order of minutes
Privacy	Low	High	Low	Low
Security	High	High	High	High

6. Conclusion

This paper compares the features of different cryptographic technologies with existing block chain technology. Here comparison is carried out between block chain, hash graph, DAG and Holo chain. For the purpose of comparisons initially first part of the paper is elaborated with detailed description of each methods existing earlier along with the recent block chain technology. Then at the end the manuscript is filed with the tabulation of the comparison and differences among the different methods. To carry out the tabulation various features and highlights taken are mining, data structure, efficiency, launched time, copyright, validation time, privacy, security, validation of transaction and applications. Block chain could become obsolete among the distributed ledger technology. Block chain was completely ruling the monetary system and demerits in the alpha version of the technology were eradicated by advance and alternate method launched associate to the applications.

7. References

[1] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies", *IEEE Communications Survey Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[2] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem", *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982

[3] D. Kraft, "Difficulty control for block chain-based consensus systems", *Peer-to-Peer Networking and Applications*, vol. 9, no. 2, pp. 397–413, 2016

[4] Yuee, X., Wang, H., Jin, D., Li, M., & Jiang, W., "Healthcare data gateways: found healthcare intelligence on block chain with novel privacy risk control", *Journal of medical systems*, vol. 40, no. 10, pp. 218, 2016.

[5] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Dist Block Net: A Distributed Block chains-Based Secure SDN Architecture for IoT Networks," *IEEE Communication Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[6] K. Fan, Y. Ren, Y.Wang, H. Li, and Y. Yang, "Block chain-based efficient privacy preserving and data sharing scheme of content-centric networking 5G," *IET Communication*, vol. 12, no. 5, pp. 527–532, Mar. 2018.

[7] G. Karame, S. Capkun, "Block chain security and privacy", *IEEE Security Privacy*, vol. 16, no. 4, pp. 11-12, Jul. 2018.

[8] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, S. Mehraeen, " Cyber security enhancement of power trading within the networked micro grids based on block chain and directed acyclic graph approach", *IEEE Transaction Industrial Application*, vol. 55, no. 6, pp. 7300-7309, Nov. 2019.

[9] F. M. Beni, I. Podnar Arko, "Distributed Ledger Technology: Block chain Compared to Directed Acyclic Graph", *2018 IEEE*

38th International Conference on Distributed Computing Systems (ICDCS), pp. 1569-1570, 2018

[10] T. T. Kuo, H. E. Kim, L. Ohno-Machado, "Block chain distributed ledger technologies for biomedical and health care applications", *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211-1220, 2017.

[11] C. Fan, H. Khazaei, Y. Chen, P. Musilek, "Towards a scalable DAG-based distributed ledger for smart communities", *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, pp. 177-182, Apr. 2019.

[12] B. Lee and J.-H. Lee, "Block chain-based secure firmware update for embedded devices in an Internet of Things environment," *Journal Supercomputing*, vol. 73, no. 3, pp. 1152–1167, Mar 2017.

[13] O. Novo, "Block chain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet Things Journal*, vol. 5, no. 2, pp. 1184– 1195, Apr. 2018.

[14] C. Yang, X. Chen, and Y. Xiang, "Block chain-based publicly verifiable data deletion scheme for cloud storage," *Journal Network Computing Application*, vol. 103, pp. 185–193, Feb 2018.

[15] N. Kshetri, "Block chain's roles in strengthening cyber security and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.

[16] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A Block chain Based Privacy-Preserving Incentive Mechanism in Crowd sensing Applications," *IEEE Access*, vol. 6, pp. 17 545–17 556, 2018.

[17] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Block chain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," *IEEE Internet Things Journal*, vol. 4, no. 6, pp. 1832–1843, Dec 2017.

[18] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," *IEEE Communication Magazine*, vol. 55, no. 12, pp. 119–125, Dec 2017.

[19] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the block chain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, July 2018.

