International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 10 | Oct 2021 www.irjet.net p-ISSN: 2395-0072

Overview of Blockchain Technology & Its Impact on Education Sector

Avishkar Hongekar[1], Anand Jaju[2], Prajwal Bhargade[3], Neel Acharya[4], Prof. Atul Pawar[5]

[1-5]*Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Maharashtra, India*

Abstract - *A Cryptocurrencies have seen a massive surge in popularity and there is one innovative technology behind these cryptocurrencies which is known as Blockchain. A blockchain is a peer-to-peer network of computers known as nodes that communicate with one another. Blockchain is a distributed network that enables fast reliable transactions by recording transaction details in the blockchain after being validated by validators. For these purposes, different consensus algorithms are used some of them are discussed in this paper. Not only cryptocurrency but blockchain technology has also a role in various finance and non-finance sector. In this paper, we will also discuss how blockchain technology can be implemented in the education sector for the benefit of learners and to increase the quality of the learning process The properties of a blockchain such as immutability, security, provenance, and peer-executed smart contracts could bring a new level of security, trust, and transparency to e-learning. In this paper, we will discuss what is blockchain, the types of blockchains, what is block and its structure, algorithms related to blockchains, and a short overview of how this technology will impact the education sector in upcoming years.*

Key Words: Blockchains, hash, mining, Merkle tree, block, consensus algorithms, PoW, PoS, SHA-256, PoV, education, e-learning

1.INTRODUCTION

Generally, there are two major types of systems which are distributed and centralized. Blockchains follow distributed approach where several nodes are connected to each other without a central control node.[1] Blockchain is the technology behind bitcoin and other cryptocurrencies. Blockchain is an open ledger where all transactions are recorded and everyone is connected to each other. Blockchain implements a unique P2P (peer to peer) distributed network that stores, verify transactions by the peers present in the network. One of the benefits of blockchain technology is that once a transaction is added to the blockchain, it is difficult to update, remove, or tamper with it. For transactions to be led effectively they should be affirmed by blockchain. It is done through consensus algorithms.

2. TYPES OF BLOCKCHAINS

2.1 Permissionless Blockchain: - Bitcoin is one example of this type of blockchain. Anyone can use it, can run a node, mining software. This can be done as long as they are following the rules of the blockchain. These types of blockchain are open and transparent. Anyone can review it at any time. They are also known as public blockchains. Most of the digital currencies in the market are included in this type. e.g., bitcoin & lite coin.

2.2 Permissioned Blockchain: - They are also known as private blockchain. It is a closed ecosystem where people can't readily join the blockchain network. They need permission to do tasks in the network. It belongs to a private individual or an organization a central authority manages all permissions. The consensus mechanism may be the same as public blockchain or some other maybe used. e.g., Ripple, Quorum.

2.3 Consortium or Federated Blockchain: - In this type power wasted on an individual entity is removed. Instead of providing authority to a single organization, power is transferred to a group of persons or individuals that establish consortiums or federations. e.g., Quorum, Hyperledger, Corda.

3. STRUCTURE OF A BLOCK

Blockchain refers to a continuous chain of blocks that are linked to each other. In this blocks data related to blockchain networks like transaction details is stored. Basically, a block is a data storing file which acts like a page of record book.

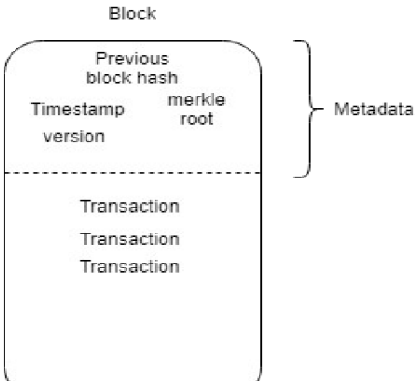

Fig -1: Block in Blockchain

• Version- It is the current version of a particular block.

• The Previous block's hash – We know that every block in a blockchain is cryptographically tied to the next block. The preceding block hash is utilized for this reason. The previous block hash field corresponds to the previous block's hash value field.

• Timestamp - The time at which a particular block is created.

• Transaction – It contains all the information related to transactions such as transaction date, time, total amount, From-To details, etc.

• Merkle root and Merkle tree – Merkle root is a cryptographic hash of the entire block's transactions. The transactions in a block are maintained in a data structure known as a Merkle tree. This tree is constructed by hashing pairs of nodes in a tree until only one hash remains, known as the Merkle root. [3].

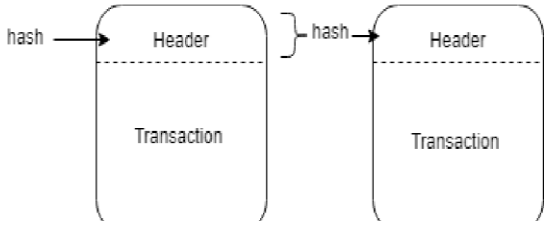

Fig -2: Linked blocks in Blockchain

4. BLOCKCHAIN ALGORITHMS

Consensus algorithms are a group decision-making procedure in which members of the group create and support the choice that is best for the rest of them. It is a type of resolution in which individuals must support the majority decision, whether they agree with it or not. This section examines several proposed blockchain consensus algorithms.

A. Proof of Work (PoW)

Proof of Work algorithm is applied to confirm transactions and add new blocks to the blockchain [4]. This algorithm is the first successful decentralized blockchain consensus algorithm. Miners compete against one another in Proof of Work to complete exchanges on the system and get paid. When a miner solves the hash for a block, it is added to the Blockchain. PoW is used in Bitcoin, Ethereum, Litecoin, ZCash, Monero, and many other blockchains.

In PoW, all transactions are proven with the help of complicated mathematical calculations. Miners solve the problem, form a new block, and confirm the transaction [6].

As proof of work, several approaches are utilized for various types of cryptocurrencies. Bitcoin, for example, employs the SHA-256 cryptographic method [5]. Litecoin utilizes a similar method known as scrypt [5], whereas Ethereum employs the Ethash algorithm [5].

B. Proof of Stake (PoS)

Proof of work (Pow) selects a block signer based on the computing effort of miners in solving mathematical problems [7]. However, there is one critical issue to address: energy waste. Proof of Stake (PoS) is used to address this issue. The main notion is that nodes with more stake will have more opportunities to add blocks to the network [7]. PoS nodes existing on a network stake some amount of bitcoin to become candidates to validate the new block and earn a reward from it. The node that will validate the new block is then chosen by an algorithm from a pool of candidates. Such selection method combines the amount of stake (the quantity of cryptocurrencies) with other criteria (such as coin-age based selection and the randomization process) to ensure that the selection is fair to everyone on the network. [8].

Coin-age or Validator Time based selection method [8]:

The method keeps track of how long each validator candidate node remains a validator. The older the node, the more likely it will become the new validator.

Random Selection Method [8]:

The validator is picked using a mix of 'lowest hash value' and 'highest stake'. The node with the best weighted combination of these becomes the new validator.

The advantages of PoS are:

1) Energy Efficient – As all the nodes in network are not competing to become a validator lot of energy is saved.

2) Decentralization - The amount staked determines the amount of reward. As a result, there is no advantage to joining a mining pool, favoring decentralization.

3) Security- A individual attempting to hack a network will need to acquire 51% of the stakes (which is pretty expensive). This results in a secure network.

Proof of Work	Proof of Stake
It consumes huge energy as many nodes compete for mining.	Energy efficient
Computation resources are required in large amount.	Very less requirement of the resources
Block reward for miner after successful mining of a block.	No block reward; forger takes transaction fees.
Centralized miners dominate a blockchain.	No centralization of forging resources
Miners must divide their resources to work on a spin-off chain in order to avoid the 'Nothing at stake' concern.	The 'nothing at stake' issue might result in repeated incentive payments to forgers. To circumvent this, PoS blockchains require extra security constraints.

Table -1: Proof of Work Vs Proof of Stake

C. Data Encryption Algorithms

This method handles the step-by-step procedure for data storage and blockchain formation, as well as the encryption and decryption process via a hash function and concurrent data storage in nodes.

Encryption of Data [9] - Cryptographic data encryption ensures data confidentiality, integrity, and authentication. A public and private key is assigned to each node in the network. A private key should never be revealed. The length of the key is determined by the method used, which can be SHA256, SHA384, or SHA512. A public key is information that is freely accessible to all nodes in the network. The data is encrypted before being transmitted to the nodes.

Data Mining and Generation of Blocks [9]: - The data present in the blockchain network is cryptographically linked using algorithms such as SHA1, SHA384, SHA256, and SHA512 [8].

D. SHA-256 Algorithm

SHA-256 was the first cryptographic hashing algorithm to be utilized for transaction verification on a blockchain network using a Proof of Work consensus method. In essence, SHA-256 allows a Proof of Work network in which computers compete to solve a difficult arithmetic problem. When one computer discovers a solution, it broadcasts it to the other computers on the peer-to-peer network. This validates their work to the other machines who were attempting to solve the same issue, as each computer on the network independently checks the solution. If the solution is proved to be correct, the miner who discovered it gets rewarded. The competition is then restarted when a fresh problem is provided. In blockchain, the SHA-256 algorithm is used to generate a consistent hash of 256 bits every time. This algorithm is also used in encryption technologies.

SHA (Secure Hash Algorithm) 256 is a cryptographic hash, similar to a text or data file signature. For a text, SHA-256 creates a nearly unique 256-bit (32-byte) signature. A hash is not the same as encryption (It cannot be decrypted back to the original text). It is a 'one-way' cryptographic function that is the same size regardless of the size of the source text.

Let's take one example of the SHA-256 algorithm with the help of 'Merkle tree'. As we know all transactions inside a block are stored in the Merkle tree. For this SHA-256 hashing algorithm is used [10].

Now, consider a block with four transactions

const tP ="Hello"

const tQ ="is this a college"

const tR ="close the gate"

const tS ="do you know this"

Now for constructing a Merkle tree we start from the bottom and go up until a single Merkle root is left. So now taking a single transaction and double hashing them.

const sha256 = require('js-sha256'). sha256

const hP = sha256(sha256(tP))

const hQ = sha256(sha256(tQ))

const hR = sha256(sha256(tR))

const hS = sha256(sha256(tS))

This hashing of the data will produce some output and now pairing together hP and hQ:

const hPQ = sha256(sha256(hP + hQ))

Pairing together hR and hS

const hRS = sha256(sha256(hR + hS))

Now the final step pairing hPQ and hRS

const PQRS = sha256(sha256(hPQ + hRS))

This is our Merkle root [10].

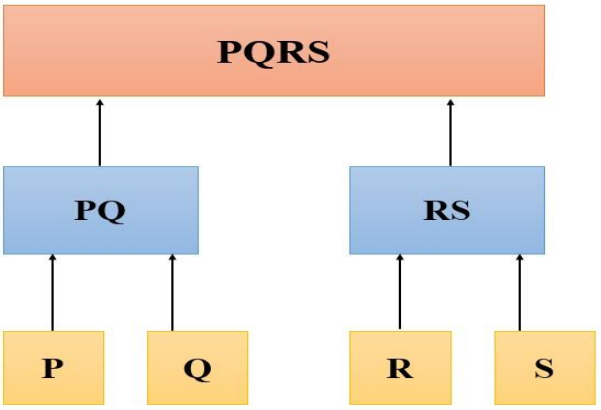

Fig. -3: Merkle Tree

Some other examples of cryptographic hash functions are SHA 1, MD5, KECCAK (used by Ethereum).

E. Secure Shading Algorithm [12]

ELASTICO is a permission-less or open blockchain agreement method that is scalable. The transaction rate grows linearly with the amount of computing required in the mining operation. It means that as computing power increases, more transaction blocks are handled. The aim is to split a network into tiny groups known as committees. Each committee handles a certain number of transactions,

and the entire method is parallelized. Only if the answer meets the constraint function is it accepted. The outcomes (shards) of all committees are combined in the final committee. To validate the algorithm, several security characteristics that emphasize its security strength are defined [12].

F. Proof of Trust algorithm for crowdsourcing [13]:

This algorithm is suggested for crowdsourcing services. The validators for a transaction are chosen based on the trust levels of the nodes. The 'Shamirs secret sharing algorithm' and 'RAFT leader election' are utilized in the selecting procedure. This algorithm is broken into four stages. The Raft leader election method is used in Phase 1 to select a leader. A voting method is used to choose transaction validators in phase 2. In step 3, the transactions are validated. In the last stage, transactions were validated, collected, and linked to the blockchain. The suggested algorithm design is evaluated based on the following properties: validity, scalability, fairness, performance, and agreement. This article also discusses attack possibilities. The results show that PoT outperforms other alternative consensus algorithms in terms of performance, accuracy, and scalability [13].

G. PoPF: Proof of Participation and Fee [14]:

JCLedger is a blockchain-based solution for JointCloud, a cloud-specific service platform. This article covers the PoPF consensus method, which has been suggested for JCLedger (Proof of Participation and Fees). The computing expense of PoW makes it impossible for JCLedger to implement it. To that end, a novel consensus technique is presented that uses significantly less computer power. The mining candidates are chosen based on two factors: the cost paid by the participation and the number of times the participant appeared as an accountant. The approach was empirically validated by the authors using simulation in the distribution of accountants [23].

H. Proof of Vote (PoV) [15]:

In this work, it is argued that the Proof of Vote (POV) consensus method is more efficient than the Proof of Work (POW) consensus algorithm (PoW). A voting method is used to verify the blocks. A consortium network model defines four roles in total. There are four types of users: commissioner, butler candidate, butler, and regular user. This algorithm has demonstrated the best performance in terms of energy usage [15].

I. The Digital Signature and Currency Trading Algorithm [16]

This algorithm is divided into two parts:

1) Signature algorithm

2) Verification algorithm

The signature algorithm creates a digital signature on the message or data. The signature key is generally in charge of this signature. The signature algorithm or signature key is kept secret and is under the signer's control. The verification algorithm is used to validate the digital signature of the message or data, and the message may be successfully validated based on the signature. The verification algorithm is often controlled by the verification key, but both the method and the verification key are public, so anybody who wants to verify the signature may do so very easily.

Transaction Authentication Process [16]: The order's validity may be confirmed by comparing the two summaries. The receiver can certify that the order is genuine if the signature and verification procedure match or are confirmed.

5. BLOCKCHAIN IN THE EDUCATION SECTOR

Cryptocurrency is one of the most significant and interesting innovations of the last century. Millions of investors are drawn to the notion of decentralized virtual money, which allows for quick and anonymous transactions. Bitcoin, on the other hand, is not simply an asset, but a complete system that has the potential to alter the social activities of all sectors. The technology is known as blockchain, and it is a mechanism that has already been utilized in the health and finance areas. Blockchain will be used in more sectors. The education industry is unquestionably one of them [17].

Today, we see advances in artificial intelligence, intelligent classrooms, and distance learning enabled by cutting-edge technology. Blockchain is expected to become a component of schools in the next years.

According to the literature articles and studies that have been published thus far, the education area will profit from the functionality given by the blockchain; nevertheless, adoption of the technology in education is still in its early phases.

Some blockchain-based systems have progressed from the prototype stage to commercial solutions, with some of them being utilized in diplomas. MIT, UT Austin, and the University of Nicosia (Cyprus) are examples of institutions that award digital certificates to students [18].

Knowledge Media Institute (KMI) a University in the UK, Europe is one of the universities to implement blockchain in education. They have created an Ethereum based platform used in learning process for academic activities, which is called as Open Blockchain [19]. They use Micro credentials (badges) which are allocated for courses available on their platform. Badges are portable, verifiable, and digital badges which can be students' skills, achievements, degrees, certifications, or any other type of credentials.

How might blockchain technology be utilized in education? Let us examine the potential repercussions of this technology as well as the potential benefits it may provide to the learning process.

1) Decentralized resource sharing in education

2) Increase student enthusiasm in online learning systems.

3) Limit the situation of forging diplomas

4) Eliminate the concerns about plagiarism in educational materials.

5) Reduce the educational industry's investment expenses.

5.1 Benefits of Blockchain on Education

1)Decentralization:

As blockchain is a peer-to-peer network, it improves fault tolerance by eliminating single points of failure [18]. Furthermore, nodes inside a network are not need to rely on some central administration to carry out their respective tasks.

2)Reliability:

All the data stored in the blockchain is immutable and distributed. Any participant may validate the data's validity and ensure that it has not been tampered with [18].

3)Scalability:

A large number of entities can access data, learning materials and process information stored in blockchain simultaneously.

4)Increased transparency of assessments [20]:

If blockchain is implemented in the education process due to its features like transparency, immutability, security the assessment process will be much simplified and fair enough.

5)Security:

All the information such as transaction details, degrees are secured in the blockchain, based on some cryptographic protocols. Due to immutability, transparency degree records are more secured.

6) Well-supported personalization [20]:

If all the courses offered by a particular university are stored on a blockchain, learners can choose courses as per their requirements. Due to this flexibility in curriculum design and a diverse set of learning outcomes will be available for learners.

7)Reduction in investment cost, administrative costs, and bureaucracy for the universities adopting blockchain-based solutions.

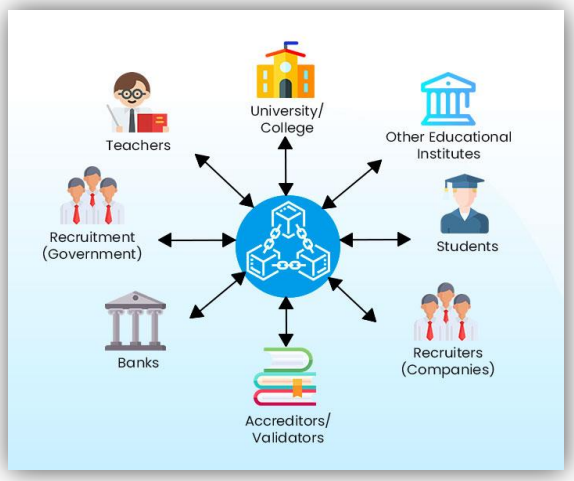

Fig. -4: Blockchain in Education

5.2 Limitations

1)Human factors:

Considering Blockchain technology is still in its early phases in the education sector, various activities, such as the quality of information or content given, and interactions with learners, are still constrained by human actors.

2) Immature technology [20]:

As the technology is not developed yet completely to use in the learning process, we can't be dependent completely on this technology at such early stages. Still, some universities are moving from prototype stages towards implementation of actual products.

3) Variety of assessment factors:

In the majority of blockchain-based e-learning systems that have been established, the learner is still in charge of his work, which is evaluated and the findings are outputted. However, numerous real-world assessment situations, including as real-time assessments, practical assignments, projects, presentations, and interviews, are also essential variables in determining a learner's whole set of learning outcomes. These evaluation criteria have yet to be incorporated in those e-learning systems.

4) Regulatory and Governance barriers [20]:

The majority of the proposed solutions can help to create a global, open, and flexible marketplace for curriculum customization. However, they do not address

higher education laws, economics, or other difficulties that exist across different educational systems.

5)Public awareness:

For the growth of this technology in the education field people should be aware of what features this technology provides rather than the conventional education process. Most of the people don't understand properties such as immutability, security, peer-to-peer concepts, and consensus. The upcoming platforms or applications should have a good user interface for consumers to demonstrate the concepts and advantages through animations, videos, and precise explanations in a simple way.

6. CONCLUSION AND FUTURE WORK

Nowadays Blockchain which is main technology behind bitcoin is not only used in the finance, health sector but it has many cross-industry applications. In the future, many more industries will adopt blockchain and one important sector among them is 'Education'. Through this paper, we have given an overall idea behind blockchain technology and how it works. We have also discussed some algorithms used in blockchain. Later we move on to the use of blockchain in the education field. Because of the benefits provided by this technology, several blockchain-based learning platforms have been created and are being utilized for the learning process in several colleges. Although there are many more benefits to using blockchain in education, we have provided a basic understanding and use examples of this technology in education. This study subject is still in its early stages, and there are many other topics that need to be investigated further before blockchain technology can be completely implemented in education.

Our paper is limited to the overall structure of blockchain technology and how we can implement it in education. For future work, many more algorithms related to the blockchain can be studied. Comparison of different consensus algorithms can be done with respect to some parameters. In depth study of different learning, platforms launched based on blockchain will provide further clarification of the proposed advantages and will give a clear understanding of real-time usage of blockchain in the learning process. Also, smart contracts and their applications can be explored further as they are not mentioned in this article. To analyses consensus algorithms, experiments must be conducted properly, as well as learning platforms can be tested based on different conditions or parameters. As a result, the choice to use blockchain in this sector must be considered with caution.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash,2008

[2] Dhiren Patel, Jay Bothra, Vasudev Patel,” Blockchain exhumed”, IEEE 2017.

[3] Blockchain: what is in a block? URL: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo

[4] Johansen, Stefan K. “A Comprehensive Literature Review on the Blockchain Technology as a Technological Enabler for Innovation.”, Mannheim University, Department of Information Systems, Version: 2.

[5] "Types of Cryptocurrencies Hashing Algorithms - Bitcoinlion.Com". Bitcoin Lion - Your Gate to Cryptocurrency, 2018, http://www.bitcoinlion.com/cryptocurrency-mining-hash-algorithms/. Accessed 5 Aug 2018.

[6] https://changelly.com/blog/proof-of-work/

[7] E. Garcia Ribera, “Design and implementation of a proof-of-stake consensus algorithm for blockchain,” B.S. thesis, Universitat Polite`cnica de Catalunya, 2018

[8] https://www.geeksforgeeks.org/proof-of-stake-pos-in-blockchain/

[9] Steven R. Weller, U. Asfia, S. Sutavani, “Secure Energy Market against Cyber Attacks using Blockchain”, International Conference on Control, Decision and Information Technologies (CoDIT’19)

[10] Janvi Dattani, Harsh Sheth, “Overview of Blockchain Technology”, Asian Journal of Convergence in Technology.

[11]https://blokchainnetwork.com/how-does-blockchain-work/

[12] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016, pp. 17–30.

[13] Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," IEEE Transactions on Services Computing, 2018

[14] X. Fu, H. Wang, P. Shi, and H. Mi, “Popf: A consensus algorithm for jcledger,” in Service-Oriented System Engineering (SOSE), 2018 IEEE Symposium on. IEEE, 2018, pp. 204–209.

[15] Li, H. Li, H. Hou, K. Li, and Y. Chen, “Proof of vote: A high performance consensus protocol based on vote mechanism & consortium blockchain,” in High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems

(HPCC/Smart City/DSS), 2017 IEEE 19th International Conference on. IEEE, 2017, pp. 466– 473.

[16] Xiaoyan Gong, Sheping Zha, "Research on the Application of Cryptography on the Blockchain", Journal of physics, California.

[17] https://www.sotatek.com/how-does-blockchain-help-to-improve-education-sector/#2_Increase_students_interest_in_online_education_platforms

[18] Cristina Turcu1, Cornel Turcu1, Iuliana Chiuchişan1, "Blockchain and its Potential in Education", Ştefan cel Mare University of Suceava 13, University Street, Suceava, RO-720229, ROMANIA

[19] Lemoie, Kerri (2017). Innovations in Open Badges & Blockchain.

[20] Tsz Yiu Lam & Brijesh Dongol (2020): A blockchain-enabled e-learning platform, Interactive Learning Environments, DOI: 10.1080/10494820.2020.1716022