International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206292

Comprehensive Study of Blockchain Technology- Architecture, Consensus and Future Trends

Shreya Joshi[1], Bhavyaa[1], Suhani Gupta[1], Mrs. Lalita Luthra[2]

[1]Department of Computer Science and Engineering, Dr. Akhilesh Das Gupta Institute of Technology and Management (affiliated to Guru Gobind Singh Indraprastha University), New Delhi, India

[2]Assistant Professor, Department of Computer Science and Engineering, Dr. Akhilesh Das Gupta Institute of Technology and Management (affiliated to Guru Gobind Singh Indraprastha University), New Delhi, India

ABSTRACT

Blockchain is considered to be a disruptive core technology. Although many researchers have realized the importance of blockchain, but the research of it is still emerging. It is the record-keeping technology behind bitcoin and is one of the hottest and fastest growing skills in the IT sector today. It serves as an immutable ledger which allows transactions to take place in a decentralized man Blockchain-based applications are rising up, covering numerous fields including finance, healthcare, product management, Internet of Things (IoT), and many more. However, there are still some challenges of blockchain technology such as scalability and security problems which need to be overcome. This paper comprises of a comprehensive study of Blockchain technology. We have included here a deep dive into how blockchains work, its architecture, consensus and various applications. Furthermore, technical challenges are briefly listed.

Keywords: Blockchain, Decentralization, Consensus, Scalability.

I. INTRODUCTION

The idea of Blockchain technology was described in the early 1990s when research scientists Stuart Haber and W. Scott Stornetta introduced a computationally practical solution for time-stamping digital documents so that they could not be backdated or tempered with [10].

The system used a cryptographically secured chain of blocks to store time stamped documents [10]. Here comes the buzz word 'Cryptocurrency'. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 169 billion dollars in 2019 [5]. Bitcoin white paper was authored by Satoshi Nakamoto; whose identity still remains a mystery. Bitcoin has been behind the birth of over a thousand different cryptocurrencies and many more blockchain projects as well. The specially designed data storage structure of bitcoins allows transactions to happen without any third party. Blockchains come under the wider category of 'distributed ledgers '. "*The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.*" [3]. Putting in simplest terms., Blockchain is a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles which is called chain [7]. The blockchain network doesn't have any central authority.

Now differentiating between blockchain and blockchain technologies, Blockchain Technologies are the rules or standards for how a ledger is created and maintained [2]. Blockchain is put to use in various financial services such as digital assets, remittance and online payment. Moreover, it can be applied to fields such as smart contracts, public services, Internet of Things (IoT), reputation systems and security services as well. Those fields favor blockchain in multiple ways. Transaction cannot be tampered once it is stored into the blockchain.

Though blockchain technologies bring us more reliable and convenient services, the security issues and challenges behind this grounbreaking technique is also an important topic that we need to concern.

In this paper we will have a quick study about what blockchain is, its architecture, consensus algorithms, different application in blockchain and what service do they offer, at the end, we shall talk about the security issues and those challenges we need to overcome and then the paper is concluded.

II. THE CONCEPT OF BLOCKCHAIN

The blockchain technology is composed of six key elements:

1) Decentralize

Blockchain doesn't require a central authority. Distributed consensus enables a blockchain to represent a single version of truth that is agreed upon by all parties.

2) Transparent

The data's record by blockchain system is transparent to each node (user), it is also transparent on update the data, that is why blockchain can be trusted.

3) Open Source

Everyone has the access to all the records. If the user wants they can access all the records from the time blockchain was created.

4) Autonomy

Each node on the blockchain system can transfer or update data safely, with the objective to trust form single person to the whole system, so that no one can intervene it [6].

5) Immutable

Records once added into the blockchain are immutable. There is a possibility of withdrawing the changes but this is considered almost impossible to do as it will require an unaffordable amount of computing resources.

6) Anonymity

Blockchain technologies solved the trust problem between node to node, i.e. it ensures the anonymity of the users who have initiated the transaction and the receivers of the transaction.

A. How Blockchain works

The main working process of a blockchain is as follows:

1) A node starts a transaction by signing it with its private key [4].
2) The transaction is promoted by using the much needed Gossip protocol to peers, which authenticates the transaction based on pre-set criteria [4].
3) All receiving nodes in the network execute consensus algorithms, usually PoW (Proof of work) and PoS (Proof of Stake) on the new block.
4) The block is then added to each node in the network.

B. The Structure of Blockchain

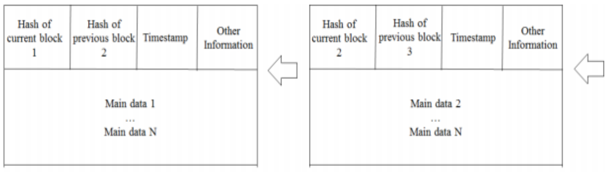

Figure 1: The structure of block chain

A typical structure of a blockchain contains 'n' number of transactions. A typical block has four attributes: Previous Hash, Transaction details, Nonce and the Hash of the block itself.

Previous hash stores the hash value of the previous block in the blockchain. This is how you are able to link one block to another and create a chain of blocks. Transaction details field contains the details about the various transactions that are to be taken place.

Nonce is the random value that is used to variate the hash value, which is a hex value that has both numbers and letters. A hash is always unique. Any change to the nonce, transaction details or the previous hash will completely change the outcome of the hashing function.

That is why altering a single block will require to change the hash of all the blocks which will require great computational power and is therefore impossible. Another important element in the blockchain is the Node. A node in a blockchain network can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain [4]. This is done by following a consensus protocol, most commonly PoW (Proof of Work).

III.HOW TO GET CONSENSUS

Consensus is the procedure of agreement among distrusting nodes on a final state of data [4]. In order to achieve consensus different consensus algorithms are used.

Consensus algorithms are at the core of the blockchain architecture. They make sure that the latest block has been added to the chain correctly.

A. Proof of Work (PoW)

The Proof of Work consensus algorithm involves solving a computational challenging puzzle in order to create new blocks in the Bitcoin blockchain [14].

As the name suggests for authenticating a transaction a node should publicly prove that it did a definite amount of work. Node has to exhibit proof of its work and this is obtained by solving a complex cryptographic puzzle [16].

In order to make our digital monetary system to work, the recipient of a transaction must be able to assert that:

1) The originator of the transaction is in possession of the funds that are being transferred and he has also obtained the funds by valid means [17].
2) As an outcome of the transaction the recipient will be known to be in possession of the funds being transferred and the sender will not be able to present himself as being in possession of the funds any more [17].

B. Proof of Stake (PoS)

Proof of stake (PoS) is a consensus algorithm by which a blockchain network aims to achieve distributed consensus.

This concept states that a person can authenticate block transactions on the basis of how many coins he or she holds [11].

Before proof of stake, the most accepted way to achieve distributed consensus was through Proof-of-Work (which was implemented in Bitcoin). But Proof-of-Work is quite energy (electrical energy in mining a bitcoin) intensive [12]. This algorithm deploys a pseudo-random election process to choose a node to become the validator of the next block, on the basis of a combination of factors which could include the staking age, randomization, and the node's wealth [10]. paragraphs must be indented. All paragraphs must be justified, i.e. both left justified and right-justified.

IV. NEW TRENDS

From the entire scenario it is evident that Blockchain system will improvise the work system in many industries and Government agencies along with time and efforts.

As the employees become skilled this highly beneficial technology would be massively in demand in traditional business cultures.

A. Blockchain adoption will grow

Apart from cryptocurrency, blockchain technology has been used in other sectors, for example:

1) In voting, food quality check, shipping, etc.
2) Big brands like Walmart, IBM and Amazon have plans to benefit from this.
3) Industrial fields in supply chain, medical data, and administration are planning to blockchain in order to streamline processes
4) In the 3D printing space, blockchain has allowed firms to manage data, identify provenance, and eased out auditing and validity.
5) The gemstone industry uses blockchain to ensure a stone provenance and authenticity (to avoid conflict mining).
6) Blockchain has also paved its way in resolving climate change issues, carbon emissions and food wastage.

Various other applications of the technology are already in use at a small scale.

B. Serial entrepreneurs will get on board

Serial entrepreneurs are those who have established startups and have work culture including the blockchain space, and more will continue to do so in 2020.

This is the era in which entrepreneurs will solve problems innovatively.

E.g.: -A man visions to bring out the world's first professional fantasy football league by using the blockchain to ensure glasslike authentic game.

And ideas like these make us look forward to more brilliant applications of the blockchain in the year ahead.

C. Blockchain app used to track COVID-19 cases

A Canada based company is putting efforts to fight the coronavirus pandemic in Latin America using the blockchain technology. Emerge, a Toronto based startup is launching an app called Civitas. This software program could link with locals' government ID numbers with unique blockchain records, which allows authorities to decide whether they are eligible to leave their homes. On the other hand if the citizens report that they are experiencing symptoms of coronavirus, the app could help in determining which days are safest for them to go out for essentials like food and medicine.

D. Blockchain will be used for identification

Blockchain is used to increase security which includes personal identification as online frauds and cyberattacks are common nowadays. This can be for online shopping where the retailer needs to ensure a consumer's identity and at the same time safeguarding any personal information gathered, in compliance with regulations such as GDPR. A startup called, "Shopin" has handled this problem by creating a universal shopper profile using blockchain technology [15].

E. Blockchain will beef up IoT

Blockchain technology will enhance the Internet of Things (IoT) where apps must run anywhere by building trust, decreasing costs, reducing risk and speeding up transactions. It has been estimated that 20 percent of all IoT deployments will have at least basic level of blockchain services enabled [15].

F. Blockchain will speed up AI

In Artificial Intelligence (AI), work speed is directly proportional to the access to bigger volume of data and here is where blockchain works as a catalyst in the process as it checks for data verification in a faster and reliable way, thereby vastly improving the performance of the AI.

G. The number of blockchain jobs will explode

Trends show that the demand for blockchain developers and project managers is very high and it will explode in 2020, as more organizations realize the benefit of blockchain, and start adopting it and building apps on it. Blockchain is relevant for not only coders but also for product managers and tech architects looking at product development and architecting solutions.

H. Blockchain based Digital court

An announcement was held on April 6, 2020*, in which* a group of researchers from Japan devised a blockchain-based mechanism which helped in performing legal functions in the "digital court". Explaining the mechanism, the University of Tokyo said that "On suspected violation of some agreement, those involved post their opinions to this digital court. The court then algorithmically aggregates the parties' opinions and judges who breached their agreement. If the digital court concludes that a party violated the agreement, the party is fined by withholding a deposit made during the initial agreement." However, it has received criticism for its decentralized nature.

V. CHALLENGES

As every technology brings challenges along with its benefits so is the case with Blockchain. Some major challenges are described below:

A. Scalability

As the amount of transactions are increasing day by day, the blockchain becomes bulky. Each node has to store all transactions to validate them on the blockchain because they have to check if the current transaction provenance is unspent or not. The original block size constraint and the time interval taken to generate a new one are the reasons why the Bitcoin blockchain can only process around 7 transactions per second, which can't meet the pace of processing millions of transactions smoothly.

B. Privacy Leakage

Users carry out their transactions with their private key and public key without any real identity exposure. However, blockchain cannot guarantee the transactional security fully as the amounts and balances for every public key are easily accessible and can be linked to user's information.

C. Selfish Mining

Even little hashing is enough to make the blockchain network a way to cheat as the selfish miners don't broadcast their mined blocks and the private way is only accessible to people if certain conditions are fulfilled. As the private branch is longer than the current public chain, selfish miners keep the private ones and make revenue while honest miners simply waste their resources.

D. Decentralisation

This challenge involves the level of decentralisation that is involved with the bitcoin blockchain. Although it does not apply to all of the ledger technologies distributed all across the globe, it is yet important to emphasise. In fact, the power of Bitcoin itself lies in the fact that it was designed to be decentralised, due to which not one centralised stakeholder could control the network. However, today the mining pools control a majority of Bitcoin's collective hash rate. Surprisingly six mining pools together control over 75% of the total mining power. This centralisation of validating transactions is just yet another logical consequence of how the Bitcoin protocol was developed, as it rewards economies of scale. This does not have to be a problem, as long as the mining pools can be trusted and have an incentive to do the right thing [5].

Blockchain technology definitely offers organisations to renovate their work culture and processes in order to be efficient, transparent and authentic with their data and working. However, there are cons of the technology along with pros and this concludes that more research is required to rule out as many challenges as possible.

VI.CONCLUSION

Blockchain has become one of the hottest trends in the recent years. Its key characteristics like decentralization, anonymity, and immutability have transformed the industries and has led its applications soar high. In this paper we gave an overview of the key characteristics of blockchain, its structure and how it works. We have then discussed the consensus algorithms and various applications and future trends of blockchain in depth. Blockchain is going to boom up in the coming years. It is not only giving birth to new technological advances but also creating new job opportunities for the people. Though blockchain technologies have great potential we still have to remain cautious of certain issues of scalability and security it has.

VII. REFERENCES

[1]. Tapscott Don and Tapscott Alex, 2016, Blockchain Revolution, Penguin, Westminster, 432 pp

[2]. Lewis Antony, 2018, The Basics of Bitcoins and Blockchains, Mango Media, Miami, 408 pp

[3]. Laurence Tiana, 2017, Blockchain for Dummies, Wiley, New Jersey, 236 pp

[4]. Bashir Imran, 2018, Mastering Blockchain, Ingram, Tennessee, 656 pp

[5]. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus and Future Trends" in proceedings if IEEE International Congress on Big Data (Big Data Congress), 2017

[6]. Iuon-Chang Lin, and Tzu-Chun Liao, "A survey of Blockchain Security Issues and Challenges", International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017

[7]. Ameer rosic, March 1, 2019, What is Blockchain? A step-by- step guide for beginners,https://blockgeeks.com/guides/what-is-blockchain-technology/

[8]. Gareth Jenkinson, Oct 31, 2019, A brief History of Blockchain: 10 years of High and Low, https://cointelegraph.com/news/a-brief-history-of-bitcoin-10-years-of-highs-and-lows

[9]. Ameer Rosic, April 2019, What is Bitcoin? The most Comprehensive step-by-step guide, https://blockgeeks.com/guides/what-is-bitcoin/

[10]. History of Blockchain, https://www.binance.vision/blockchain/history-of-blockchain

[11]. ake Frankenfield, Aug 11,2019, Proof of Stake(PoS), https://www.investopedia.com/terms/p/proof-stake-pos.asp

[12]. Parikshit Hooda, Proof of Stake in Blockchain, https://www.geeksforgeeks.org/proof-of-stake-pos-in-blockchain/

[13]. Jake Frankenfield, Aug 11,2019, Proof of Work, Jul 30,2018, https://www.investopedia.com/terms/p/proof-work.asp

[14]. Parikshit Hooda, Proof of Work(PoW) Consensus, https://www.geeksforgeeks.org/proof-of-work-pow-consensus/

[15]. Stuart Rauch, December 2019, 7 Trends in Blockchain for 2019, https://www.simplilearn.com/blockchain-trends-article

[16]. Ravindra T, December 28,2019, Blockchain Consensus Algorithm: Proof of Work (PoW), https://www.cisin.com/coffee-break/technology/blockchain-consensus-algorithm-proof-of-work-pow.html

[17]. Aleksandr Bulkin, May 3, 2016, Explaining Blockchain, https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845

Cite this article as :

Shreya Joshi, Bhavyaa, Suhani Gupta, Mrs. Lalita Luthra, "Comprehensive Study of Blockchain Technology - Architecture, Consensus and Future Trends", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 319-325, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT206292
Journal URL : http://ijsrcseit.com/CSEIT206292