JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Scrutiny on opportunities and challenges of block chain

Author: Parvathy Viswanath

Guest Lecturer, N.S.S. College, Ottapalam

Abstract

A block chain can be defined as a distributed technology that is associated with bitcoins and they can form a chain of blocks. Here each block contains information and data which are packed together and they are also verified. Blocks are validated and they are added to the chain in previous blocks. This technology is having numerous benefits like decentralization , anonymity , audibility and it has been used in many areas like financial services , risk management , Internet of things , cryptocurrency etc. This paper deals with both technological and application perspectives of block chain. Introduction to block chain consensus algorithms, technical challenges and some recent solutions to tackle these challenges area also discussed here.

Keywords: Block chain, cryptocurrency, bitcoin, consensus algorithm

1.Introduction

Block chain is the core mechanism for bitcoin and this method was first introduced in 2008 and it was implemented in 2009[1]. Block chain can be called as public ledger where all transactions are stored in blocks and later they are connected in a chain. In this chain, new blocks can be easily attached and so the chain grows .By this architecture some of the key characteristics such as decentralization, persistency and auditability can be attained.

This technology works with decentralized environment and this environment is also enabled by some of the supporting technologies like cryptographic hash, asymmetric cryptography based digital signature and some distributed consensus mechanisms. Block chain can greatly save cost and improve efficiency by the decentralization.

Block chain is also found to be a promising technology for the coming generation of systems. Some of the technologies that are being planned to get integrated to the block chain technology are smarts contracts [2], internet of things [3],reputation systems[4] and security services[5]. Apart from all these advantages, there are some challenges faced by block chain . Some of them are scalability as bitcoin block size was earlier limited to 1 Mb and when the block is mined in every 10 min , the whole network is restricted to a rate of 7 transactions per second and this considered as an disadvantage in high frequency trading. This lead to larger blocks in turn a larger storage space requirement but propagation in the network seems to be slow

Another challenge is that miner can achieve larger revenue by following some mining strategy like by hiding the mined blocks in order achieve more revenue in the future[6].This can hinder the block chain development. Even the privacy leakage can also happen even if public key cryptography is used [7] .

This paper includes the study of technical details of block chain like consensus algorithms, applications of block chain and even some future directions.

2. Architecture of block chain

As discussed before block chain is a sequence of blocks which keeps the details of transaction records[8].Each block points to the previous blocks by making use of reference which are usually a hash value of previous block often called as parent block. There are different types of blocks like uncle blocks and they are children of block's ancestors and those hashes can be also stored in ethereum block chain[9] . The block with no parent is called genesis block and it is the first block in the chain. In each block it contains block header and block body and block header contains block version , it indicated which set of block validations should be followed. Block header contains parent block hash which is of 256 bit which points to the previous block. It also contains merkle tree root hash , which is the hash value of all transactions in the block. Even the header of the block contains the timestamp along with nBits which is the hashing target in a compact format. A nonce field of length 4 byte is also present in the block header where the value starts with 0 and increases in every hash. Block chain mechanism uses a asymmetric cryptography mechanism to check each transactions carried out[10].

2.1 **Authentication in block chain**

Authentication is carried out by making use of key pairs- private key and public key. The private key is used here to sign each transactions. After signing each transactions these documents are moved through the whole networks and the datas are available to others by using public keys which is accessible to all users. This type of signature includes two phases- the signing phase and verification phase.

If a sender will first generate the hash value derived from the transaction to sign the transaction. Then the sender will encrypt the hash value by making use of the sender's private key .The original data is sent to the receiver along with the encrypted hash. At the receiver's side , the receiver will verify the transaction received by comparing the hash value received and the hash value generated at the receiver's side by performing the same hash function as sender's, The algorithm that is used in block chain for generating the digital signature is Elliptic curve digital signature algorithm[11]

3. Characteristics of Block chain

Persistency

Every transactions must be persistent as each transactions are confirmed before it is completely transferred in to the network. It is difficult to attacks these validated informations.

Anonymity

A user in the block chain can generate many addresses so that each user wont expose their individual identity. There is no central party in the block chain network to control this address creation. Due to this constraint block chain is not providing any guarantee for privacy preservation.

Decentralization

Each transaction in the block chain is carried between two peer and they are not authenticated by a central agency . This decentralization can reduce both development cost and operational cost of a central server.

4. Types of block chain

Block chain can be roughly categorized in to three types – Public block chain, private block chain and consortium blockchain[12].

Public block chain- In the perspective of consensus , in public block chain each node could take part in the consensus process and only those selected nodes are responsible for validating the blocks .Transaction in public block chain are visible to the public. As the transactions are stored in different nodes in the distributed network , it is very difficult to tamper all these transactions.

Private block chain-In the case of private block chains, transactions are controlled by one organization .The read permission will be decided by the organization that controls the communication. The stored information can be public or restricted depends on the organization that it controls.

Consortium block chain-It is similar to private block chains, the consortium can decide whether information regarding the transactions are to be stored in public or restricted. Consortium block chain could be reversed or tampered when compared to the private block chains

5.Consensus algorithms

As the block chain follows distributed ledger there is no central node that ensures ledgers on all nodes are same . Because of this nature there will be no trust between the nodes . For this purpose there should be some efficient algorithms to make data in different node consistent. There are many approaches in block chain in order to make it consensus.

In Bitcoin, Proof of work(PoW)[13] is the strategy used . Here come computations are carried out inorder to make the nodes and the transactions authenticated. In this method a hash value of the block header is calculated each time and we will check that this value is equal to smaller than a particular value shown in consensus algorithm. As block chain technology is a distributed ledger all nodes in the network have to calculate this hash value and this process is carried out by random nonces . Every node connected to a node must confirm the correctness of the value each time it is created. The collections of transactions used in the calculations is approved to be in the result and these approved results is denoted by new block in the block chain. Miner is the term used for the nodes that calculates hashes and the procedure that can be used are called as mining.

.

A lot of calculations are required in proof of work and these are carried out by miners and they require a lot of resources. In order compensate this loss there are some efficient protocols that support PoW and those have some important applications also. One of the example is used in Primecoin [14] where the protocol use only prime numbered blocks in the chain for different researches.

Another alternative approach to maintain the consistency between the block is proof of stake(PoS) .This approach is considered to be energy conservative and efficient space handling method. PoS requires the people to prove the ownership in the chain. It is believed that the people who are there in the block chain with more currencies will create less problems. As it is found that this selection is completely based on account balance , this type is considered as not that efficient. Many solutions were carried out to solve the issue. Some of the examples are Blockcoin[15], where the next generator is predicted by using some randomization. This method finds out the lowest hash value in connection with size of stake. One of another example is Peercoin[16], it uses age based selection criteria.

Here the cost of mining is almost zero there are chances for different types of attacks. Usually when a block chain technology follows PoW at the beginning will follow PoS later. Now Ethereum is moving it's step to move from Ethash[17] , which is a kind of PoW to Casper[18] which is of type PoS. Later to combine the advantages of both these techniques Proof of activity[19] was introduced.

Similar to POS , another method where the miners will get the priority to generate the blocks according to their stake and this method is called as Delegated Proof of stake . This method is considered to be more representative democratic. Stake holders will select their delegates inorder to validate a block. Another consensus algorithm was introduced that uses the trusted sub networks present inside a larger network and this algorithm was called as Ripple[20]. In this algorithm the networks are divided in to two client and server. Those nodes participates in the consensus process is called as server and those nodes transferring funds are called client nodes.

Another byzantine consensus algorithm is called Tendermint[21], in this method a new block is determined in different rounds. Each a node will broadcast an unconfirmed block in this round. All nodes need to be known about the selection made . This process is divided in to three steps. In the first step the validators choose whether to broadcast the proposed block and this step is referred as Prevote step. If the node receives over 2-3 prevotes on then it will move on the next stage , this step is called pre commit step. In the last step, commit the node will validate the block and later it will be accepted.

6. Future scope

As block chain had shown immense advancement and it's potential in the whole industry . Here we can discuss it's possible future developments in five different areas like block chain testing, trends towards centralization, big data analytics , smart contract and in areas of artificial intelligence

6.1 Block chain testing

Different kinds of block chains was introduced in a very small amount of time , around 700 cryptocurrencies are listed in coindesk in 2017. A very strong block chain testing mechanisms are required to test different blockchains. Block chain testing is carried out in two different phases . First phase is called standardization , here all criteria have to made and agreed and later it enters to the testing phase where the testing needs to be performed with different criteria.

6.2 Trends towards centralization

As years as moving ahead there is a trend where the miners are centralized in the mining pool. Total 51% of the hash power in bitcoin network is owned by 5 mining pools. Apart from that selfish mining strategy showed that pools with over 25% of the total computing power. As block chain served a few organizations , some methods should be introduced to solve this issue.

6.3 Big data analytics

Block chain can be easily combined with big data. This combination can be divided in to data management and data analytics. In data management block chain can be used to store important data as the process is distributed and secure.

6.4 Smart Contracts

It is a computerized transaction[22] protocol that which executes the terms of a contract. As it was proposed before a long time and this concept can be implemented with block chain .By this concept block chain can be applied in to different areas like IoT and banking services. Smart contract researches can be divided in to two types. First is development where it can be used to smart contract development.

6.5 Artificial Intelligence

As the block chain technology is getting updated every year , new opportunities for artificial intelligence is also created. AI technologies can be used to solve many block chain challenges. Block chain and smart contract can be used together to restrict the misbehaviours carried out by AI products.

7. Conclusion

Block chain is an immensely growing technology and it is being applied to various fields other than bitcoin. In this paper we have discussed about different block chain technologies and it's challenges and the future improvements that can be done. A lot of research works and advancements are required in block chain in order to apply it in all fields and it can be studied and resolved in the future.

References

1. Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf
namecoin (2014) *Namecoin*, https://www.namecoin.org/

2. Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016) 'Hawk: the blockchain model of cryptography and privacy-preserving smart contracts', *Proceedings of IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, pp.839–858.

3. Zhang, Y. and Wen, J. (2015) 'An IoT electric business model based on the protocol of bitcoin', *Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN)*, Paris, France, pp.184–191.

4. Sharples, M. and Domingue, J. (2015) 'The blockchain and kudos:Adistributed system for educational record, reputation and reward', *Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015)*, Lyon, France, pp.490–496.

5. Noyes, C. (2016a) *Bitav: Fast Anti-Malware by Distributed Blockchain Consensus and*

Feedforward Scanning, arXiv preprint arXiv:1601.01405.

6. Eyal, I. and Sirer, E.G. (2014) 'Majority is not enough: Bitcoin mining is vulnerable', *Proceedings of International Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg, pp.436–454.

[7] Biryukov, A., Khovratovich, D. and Pustogarov, I. (2014) 'Deanonymisation of clients in bitcoin p2p network', *Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security*, New York, NY, USA, pp.15–29.

[8] Lee Kuo Chuen, D. (Ed.) (2015) *Handbook of Digital Currency*, 1st ed., Elsevier.

[9] Buterin, V. (2014) *A Next-Generation Smart Contract and Decentralized Application Platform*, WhitePaper.

[10] NRI (2015) *Survey on Blockchain Technologies and Related Services*, Technical Report.

[11] Johnson, D., Menezes, A. and Vanstone, S. (2001) 'The elliptic curve digital signature algorithm (ECDSA)', International Journal of Information Security, Vol. 1, No. 1, pp.36–63.

[12] Buterin, V. (2015) *On Public and Private Blockchains*, https://blog.ethereum.org/2015/08/07/onpublic-and-private-blockchains/.

[13] Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf namecoin (2014) *Namecoin*, https://www.namecoin.org/

[14] King, S. (2013) *Primecoin: Cryptocurrency with Prime Number Proof-of-Work*, 7 July.

[15] Vasin, P. (2014) *Blackcoin's Proof-of-Stake Protocol v2*, https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf

[16] King, S. and Nadal, S. (2012) *Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, Self-Published Paper, August.

[17] Wood, G. (2014) *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, Ethereum Project Yellow Paper

[18] Zamfir, V. (2015) *Introducing Casper the Friendly Ghost*.

[19] Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M. (2014) 'Proof of activity: extending Bitcoin's proof of work via proof of stake [extended abstract]', *ACM SIGMETRICS Performance Evaluation Review*, Vol. 42, No. 3, pp.34–37.

[20] Schwartz, D., Youngs, N. and Britto, A. (2014) *The Ripple Protocol Consensus Algorithm*, Ripple Labs Inc White Paper.

[21] Kwon, J. (2014) *Tendermint: Consensus without Mining*.

[22] Szabo, N. (1997) *The Idea of Smart Contracts*.