Research Journal of Computer and Information Technology Sciences ISSN 2320 – 6527
Vol. **10(1),** 27-30, June **(2022)** *Res. J. Computer and IT Sci.*

Review Paper

Blockchain: Challenges and possible alternative (Hashgraph)

G.S Rohit and K. Subhashini Spurjeon
Department of Information Technology, Bhilai Institute of Technology, Durg, CG, India
rohitgeddam2018@gmail.com

Available online at: www.isca.in
Received 24th November 2020, revised 29th December 2021, accepted 8th February 2022

Abstract

Blockchain technology is one among the foremost popular technologies in recent years, it's already changed people's lifestyles in some areas thanks to its great influence on many businesses or industries, and what it can do will still cause an impact in many places. Blockchain technologies bring us more reliable and convenient services, however, the safety issues and challenges behind this technology are additionally a crucial topic that we'd like to concern about. One of the main drawbacks of blockchain with current implementations is speed of the network and efficiency. We compare blockchain with hashgraph and survey the benefits of hashgraph over blockchain.

Keywords: Blockchain, Security, Smart contract, Bitcoin, Hashgraph, virtual voting

Introduction

There are several applications of blockchain, however bitcoin is one of the first applications of blockchain, it's kind of a digital currency based on blockchain technologies. Bitcoin is used to trade things on the internet. Because of the explosive success of bitcoin, people have now started using blockchain technologies in several other fields such as finance, IOT, supply chain, voting, health care[1], storage. The Blockchain is responsible for storing the entire network's transaction history with a relatively secure time-stamp[2]. With the increasing popularity of blockchain and use of it in our daily life, Cybercriminals would get an opportunity to exploit this technology to their advantage [3,4]. Ferrag *et al.*[5] discussed different application domains of blockchain–IoT, such as IoV, IoE, IoC, edge computing, and others. In this paper, we will discuss various shortcomings or challenges of blockchain technology in section 2, then in section 3 we will compare blockchain with hashgraph and try to survey how hashgraph is better than blockchain, then the paper is concluded.

Issues and Challenges with Blockchain

Blockchain is already considered as a powerful technology[6], blockchain definitely has some major advantages however it's not without its share of challenges and issues.

The 51% attack: The probability of mining a block increases with increased ability of miners to do more work. A miner can do more work by increasing the computational power of the CPU or GPU, due to this mechanism people join together to mine more blocks and constitute mining pools. Once the pool holds 51% computing power, it can take control over the blockchain network, this is a serious concern[7] which is prone to cause security issues[8,9]. Empirical evidence shows that Bitcoin miners form pools[9], If someone/pool has more than 51% computation power it becomes easier and faster to find the Nonce value quicker than others[9]. This allows them to prevent new transactions from gaining confirmations and they could halt the transactions altogether. Also while they are in control it would be possible to reverse transactions that were completed while they were in control or they could modify the transaction data which may cause double-spending attacks[10,11].

The Fork Problem: This problem captivates a large number of blockchain networks. This problem is related to the decentralized architecture of the blockchain. Whenever a newer version of blockchain software is published, consensus rules are also updated to the nodes. This divides the whole set of nodes in a blockchain into: i. Nodes which have been upgraded (New nodes), ii. Nodes which haven't been upgraded (Old nodes).

This division gives rise to a few possible cases in getting consensus, according to which fork problems are divided into two types: i. Hard Fork, ii. Soft Fork.

The old nodes are distinguished from new nodes based on the computational power.

Hard Fork: Hard Fork happens because the old node verification requirement is much stricter than the new node
When the network comes to a new agreement and it isn't compatible with the previous version of agreement, the old nodes simply deny the mining of new nodes, Therefore one chain breaks up into two chains. Old nodes continue to maintain the chain which it thought was right. To solve this problem all the nodes in that network need to be requested to upgrade their agreement and the nodes which haven't been upgraded will continue not to work.

Soft Fork: Soft Fork happens because the new node verification requirement is much stricter than the old node, when the network comes to a new agreement and it isn't compatible with the previous version. The new nodes couldn't agree with the mining of old nodes. As the newer nodes have more computing power than that of older nodes, the mining of older nodes will not be approved by the newer nodes; however the newer and the older nodes will continue to work on the same chain. In case of soft fork all the nodes in the network don't require to upgrade to the newest agreement simultaneously they can be upgraded gradually unlike hark fork. When Soft fork happens the old nodes are unaware that the consensus rules have changed which contradicts that in the blockchain network each node can verify the correctness correctly to an extent.

Scaling of the blockchain network: As a blockchain network grows bigger the computation will also get harder, also a large blockchain network takes time to sync data which can cause reliability issues for the client[12]. This is one of the major concerns of the blockchain network.

Speed of Transaction: Taking Bitcoin into consideration, as of 2019 it was only capable of processing seven transactions per second and etherium which is another blockchain network could theoretically process eight transactions per second which when compared to other technologies currently in use which could process hundreds of requests per second is a major downside of blockchain. Meanwhile, new ledger technologies are in development that would offer significant increase in transaction speed, however the deployment of these technologies is still very limited.

Integrated Cost Problem: It would take a lot of time, energy and money to change the existing legacy systems with a new technology. Blockchain still needs to prove its economic benefits of Blockchain's lack of standard poses a problem. Standards are important for networks to deal with information systems, however obtaining a global industry standard is not easy and it would take a lot of time before organizations have a common blockchain standard.

Blockchain Solutions may consume too much energy: Taking bitcoin as an example which uses a proof-of-word consensus algorithm relied on miners to do the work. Miners solve complex mathematical problems and get incentives. Since theses mathematical problems are not easy and very complex they require the computer to do the heavy lifting for long hours which intern leads to higher energy usage. However not all blockchain technologies run in the same way, there are other consensus algorithms that solve the problem. In short, central networks are efficient in terms of energy usage whereas public networks consume a lot of energy to be operational.

Data Immutability: The major disadvantage of blockchain technology has always been the data immutability. Although many systems such as the supply chain management and the financial systems benefit greatly from that. Privacy is the right of every person on this planet, however if the person uses a blockchain technology, it leaves a digital footprint which cannot be removed from the system if the person doesn't want it there. So simply there is no way to remove traces, challenging privacy rights.

Inefficiency: There are a variety of blockchain based technologies, if we talk about bitcoin in particular one can notice a lot of inefficiencies in the system. When you try to set up a blockchain miner program on your system, the ledger could very easily cross 100's of GB, therefore it's not efficient in terms of storage. The blockchain network as it grows tends to slow down, which is against the ideals of a commercial entity which requires a network to be as fast as possible and as secure as possible, however these inefficiencies have been improving.

Legacy Systems: Not all businesses want to embrace a new technology. There are still many organizations that heavily rely on their legacy system to operate their business. If the business wants to adopt blockchain technology they would need to completely replace their current technology which might not be a feasible option for every business.

Blockchain alternative: Hashgraph

Hashgraph is a consensus method offering a different approach to distributed ledger technology[13]. It was developed by CTO of Swirlds Leemon Baird. It is an aBFT consensus algorithm that is capable of securing the platform against attacks. It uses directed acyclic graphs and does not require miners to validate transactions. Hashgraph offers secure, reliable and a fast network. It is implemented using the Lisp programming language. The most attractive advantage of a hashgraph is its speed.

Approach: Hashgraph differs from blockchain in its approach, in blockchain data gets stored in blocks which is a linear way, when ever new data is to be appended it gets appended as a block in the existing chain. On the other hand hashgraph uses a directed acyclic graph approach to store and access information. In both the Distributed ledger technologies each and every node has a copy of the ledger making both a truly decentralized system.

Security: Hashgraph and blockchain both are strong options when it comes to security, however blockchain utilizes a cryptographic method for ensuring security of the data that is stored and transmitted on the network.Peer-to-peer (P2P) network is a fundamental part of how Blockchain technology works and is one for the reasons for its solid security[14]. The blocks in a blockchain network are tamper-proof and there is no way to change the integrity of the data, as when someone tries to modify a block, all the previous blocks become invalid thus indicating of a malicious activity[15].

Hashgraph uses aBFT for securing the network .Each and every event is recorded correctly and the approach makes sure that none of the data can be tampered with. However just as in blockchain, in hashgraph once a transaction is completed, there is no way to change it.

Consensus Algorithm: When it comes to consensus there is no single approach in blockchain. Consensus algorithms varies from platform to platform, however there are many popular consensus algorithms which are used in blockchain technology, some of them are proof-of-work, proof-of-stake, proof-of-elapsed-time, etc. Hashgraph uses virtual voting as a form of consensus.Hashgraph in itself is a consensus algorithm with lots of features which make hashgraph an alternative to blockchain.

Speed: Speed of blockchain varies with implementation; however it is comparatively slower than hashgraph. In theory hashgraph can reach a speed of 5,00,000 transactions/second. On the other hand blockchain implementations such as bitcoin, ethereum etc. are much slower in speed (about 100 to 10,000 transactions/second) when compared to hashgraph.

The main reason behind the fast speed of hashgraph is the method used by it known as Gossip method. In the Gossip method less information is needed to be propagated across the network which ultimately increases the speed of the network.

Fairness: Hashgraph is fairer when it comes to miners or users. In blockchain miners have a lot of power when it comes to selecting orders miner wants to process, order of processes and they could even stop transactions all together, this would not be fair to anyone who is connected to the network.

Hashgraph handles fairness in a different way. It allocates nodes in a random manner utilizing consensus time stamping, so that no one is affected because of the order of the transactions.

Efficiency: Efficiency of a hashgraph reaches 100% because of the approach used by it. Blockchain's block approach makes it harder for miners to work on a block. Consider the case when two blocks are mined at the same time, then the miner's community now needs to decide on one block discarding the other block, at the end the efforts of the miner of the discarded block gets wasted, which results in a less efficient network. Hashgraph does not suffer from this problem as hashgraph doesn't rely on block creating rather it rely on creating events.

Adoption and Development Stage: Blockchain beats hashgraph easily when it comes to the adoption and development stage. Blockchain is much older technology which has been in active development for a decade, Hashgraph on the other hand is not adapted as widely as blockchain yet and it is still in active development.

Conclusion

Blockchain is surely an innovative new technology with lots of applications and many more applications which are not thought of yet. Although there are few challenges with blockchain technology, many of them have already been improved with new techniques, others are under extensive research. For the blockchain to be truly integrated in our daily life the government needs to make corresponding laws for blockchain, and enterprises should be ready to embrace this new technology.

Hashgraph has become a strong contender against blockchain solely because of the major benefits demonstrated by the hashgraph. The first and the major advantage of hashgraph is speed, because of the high speed of hashgraph network instant sharing of information is now possible between network participants. Hashgraph also aims to reduce the cost of running which is currently high for blockchain. The research shows that with hashgraph it is possible to reach consensus within the same network consisting of 32 computers in just 3.0 seconds, and further reduction of 1.5 seconds is possible depending on the regions[16]. Hashgraph can execute 250000+ transactions per second which is much better than what blockchain can handle currently. The drawbacks of hashgraph which are related to security and decentralization require further improvement. While scalability is the main concern of the majority of the existing public blockchain networks, hashgraph faces very similar issues. We conclude by saying that the hashgraph is a relatively new technology trying to solve some of the drawbacks of the blockchain, and while it shows promising improvements over blockchain, we are yet to see hashgraph work in a public setting.

Acknowledgments

I would like to thank my mentors Dr. Ani Thomas, H.O.D I.T. department BIT, Durg and Mrs. K Subhashini Spurjeon assistant professor, I.T department BIT, Durg, for guiding me throughout the process of writing this paper and providing me with various useful resources.

References

1. M. Mettler (2016). Blockchain technology in healthcare: The revolution starts here. *Proc. IEEE 18th Int. Conf. E-Health Netw. Appl. Services (Healthcom)*, pp. 1-3, Sep. 2016.

2. Nakamoto, S., & Bitcoin, A. (2008). Peer-to-Peer Electronic Cash System. November 2008. https://bitcoin.org/bitcoin.pdf, Accessed on 2015-01-01. A peer-to-peer electronic cash system.

3. Opara E. U. and Soluade O. A. (2015). Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities. *International Journal of Electronics and Information Engineering*, 3(1), 10–18.

4. J. Singh (2014). Cyber-attacks in cloud computing: A case study. *International Journal of Electronics and Information Engineering*, 1(2), 78–87, 2014.

5. Ferrag M., Derdour M., Mukherjee M., Derhab A., Maglaras L. and Janicke H. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. *IEEE Internet Things J.*, 6(2), 2188-2204.

6. J. L. D. L. Rosa, V. Torres-Padrosa, A. el-Fakdi, D. Gibovic, O. Hornyák, L. Maicher, et al. (2017). A survey of Blockchain technologies for open innovation. *Proc. 4th Annu. World Open Innov. Conf.*, pp. 14-15, 2017

7. Hajdarbegovic N. (2014). Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack. New York, NY, USA: Coin Desk.

8. Courtois, N. T., & Bahack, L. (2014). On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718.

9. Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. *In International conference on financial cryptography and data security*, pp. 436-454. Springer, Berlin, Heidelberg.

10. Karame, G. O., Androulaki, E. & Capkun, S. (2012). Two bitcoins at the price of one?. Double-spending attacks on fast payments in Bitcoin. Cryptology EPrint Archive.

11. Rosenfeld, M. (2014). Analysis of hashrate-based double spending. *arXiv preprint arXiv*:1402.2009.

12. Karame, G. (2016). On the security and scalability of bitcoin's blockchain. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 1861-1862.

13. Schueffel, P. (2017). Alternative distributed ledger technologies Blockchain vs. Tangle vs. Hashgraph-A high-level overview and comparison. Tangle vs. Hashgraph-A High-Level Overview and Comparison, December 15, 2017. Available: https://ssrn.com/abstract=3144241.

14. Sharma, T. K. (2018). How does Blockchain use public key cryptography. Preuzeto, 24, 2020.

15. Lin I.C. and Liao T.C. (2017). A survey of blockchain security issues and challenges. *IJ Netw. Secur.*, 19(5), 653-659.

16. Hedera Smart Contracts (2020). Leemon Baird, Mance Harmon, and Paul Madsen. https://hedera.com/hh-whitepaper-v1.5-190219.pdf.