Journal of Engineering and Applied Sciences 14 (Special Issue 2): 5579-5584, 2019
ISSN: 1816-949X

Improved Blockchain Network Performance using Hypergraph Structure

Faiza Mahmood Shuker
College of Medicine of Hamorabi, University of Babylon, Hillah, Iraq
Faiza.mahmood1@yahoo.com, 07801639277

Abstract: Essentially, a blockchain is a distributed database of records or public ledger of all digital events and transactions have been carried out and shared among participants. In the public ledger, every transaction is confirmed by consensus of the majority participants in the framework. Once the information is entered, it cannot be erased. A blockchain network is economical and efficient because it eliminates duplication of effort among stakeholders and reduces the need for intermediaries. In this study, a model of blockchain depending on hypergraphs is proposed. The main goal of the proposed model is to minimize the consumption of storage and to fix the extra security problems. Here, the hyperedge is utilized as the storage nodes organization, also, the whole networked data storage is converted into part network storage.

Key words: Blockchain, network performance, hypergraph, storage nodes, network storage, public ledger

INTRODUCTION

Until now, the concept of trust between multiple parties has been utilized in businesses and in some situations in industries. And this type of trust based business is about to be stopped and changed with the technology of blockchain. The technology of blockchain refers to the technology of distributed ledger which can register the transactions between participants in a permanent and secure manner. Essentially, through the process of databases sharing between multi-participants, blockchain removes the requirement for the trusted third parties to record, verify and coordinate the transactions. To facilitate the transformation from a central to a non-central and distributed system as shown in Fig. 1 (Heutger and Kuckelhaus, 2018). The technology of blockchain has been exceedingly used in different fields like finance (Treleaven *et al*., 2017), insurance (Gatteschi *et al*., 2018), industrialization (Miller, 2018) and health-care (Esposito *et al*., 2018). This technology has a distributed ledger which includes transactions connected blocks to all members of the network.

Bitcoin is one of the extreme effective cryptocurrency, it provides a big achievement with its capital market reach 10 billion $ at "2016" (Esposito *et al*., 2018). Through a particularly designed structure of data storage, Bitcoin transactions, the network could occur without a third party and the main technology for building Bitcoin is blockchain, that proposed at 2008 and executed at 2009 (Nakamoto, 2008). Blockchain can be considered as a public ledger and all promising transactions are stored in blocks list. This chain increases as new blocks are attached to it constantly. Generally, the technology of blockchain has key attributes of non-centralization

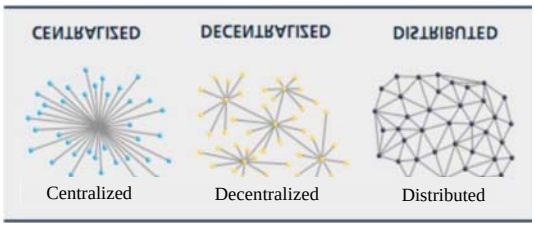

Fig. 1: The transformation from a central to a non-central and distributed system utilizing blockchain (Heutger and Kuckelhaus, 2018)

persistency and anonymity. Based on these attributes, the blockchain is capable of highly saving the cost and improving the efficiency (Hileman, 2016). The technology of blockchain can be utilized in different services of financial like online payment, digital assets and remittance (Zheng *et al*., 2017; Peters *et al*., 2015) because it permits the payment process to be done without any intermediary or any bank. Also, it is applicable into other domains like intelligent contracts (Foroglou and Tsilidou, 2015), public services (Kosba *et al*., 2016), internet of things (Akins *et al*., 2013), reputation techniques (Zhang and Wen, 2015) and services of security. These domains support blockchain in multi-ways. Firstly, blockchain is unalterable. Once the transaction is packed into the blockchain, it can't tamper. Businesses which need big honesty and reliability can utilize blockchain for attracting customers. Beside, blockchain is distributed and can prevent the single point of fail case. For smart contracts, it could be automatically implemented via. miners once the contract has been deployed on the blockchain (Zheng *et al*., 2017).

Literature review: The technology of blockchain appeared to in the beginning of 2009 via. the cryptocurrency bitcoin. The users of Bitcoin utilize a Public Key variable (PK) for generating transaction information and broadcasting it on the network to funds transfer. Little researches have been presented in this domain and the attempt to raise the performance of blockchain such as Kan *et al.* (2018) worked on a simulation of the blockchain with parallel mining and graph structure to maximize the performance of blockchain. The core framework is the alteration of the chain data structure to GraphChain and uses the modern mechanism of mining for enabling parallel mining. Schuh and Larimer (2015) proposed a delegated proof of stake method which tries to minimize the decision-makers number for increasing the efficiency of the system. Nakamoto presented an improvement of the performance of original Bitcoin (Hileman, 2016) by introducing the microblock that works as a lighter block among other original blocks on the chain. Qu *et al.* (2018) proposed an improvement of the original blockchain network based hyper graph structure based on network parameter graph rank c and verification threshold in (0,1).

MATERIALS AND METHODS

Blockchain model based on hypergraph: The blockchain technology implementation needs that all network nodes maintain the records of the synchronized data that will obviously place more pressure on the storage of data. Thus, minimizing the nodes number which synchronize data in the network can warranty the normal blockchain process. The theory of hypergraph is used to divide the whole network into considerable hyperedges and in order to minimize the pressure of storage, every hyperedge stores a portion of transaction data (Qu *et al.*, 2018). The improve blockchain model is shown in Fig. 2.

The architecture of blockchain: The blockchain is a series of blocks that contains a full list of records of the transaction such as a traditional public ledger. An instance of a blockchain is shown in Fig. 3. At a former block hash included in the header of the block, a block has just one parent block. Genesis block is the name given to the first in a blockchain that has no parent block (Miller, 2018).

Once more than a specified number of people validates the transaction the transaction details are stored in the form of a block and that block is added to the existing 'blockchain'. Hence, the name, blockchain. Moreover, the blocks once validated and added are immutable. Figure 4 shows these blocks have a specific hash associated with every block. These hashes are like fingerprints, unique to every block. The persons validating the transaction process are called as miners. More the number of miners, better the efficiency of transaction (Heutger and Kuckelhaus, 2018).

A block in all contains of data, a hash and a hash of previous block. Since, it contains a hash of a previous block, hence, in a blockchain all the blocks contain data for the previous blocks, so, it becomes almost impossible for a blockchain to be corrupt (Heutger and Kuckelhaus, 2018).

In order to be a portion in the system of blockchain, the participated entities should install and run some programs which connect their computer/server to other

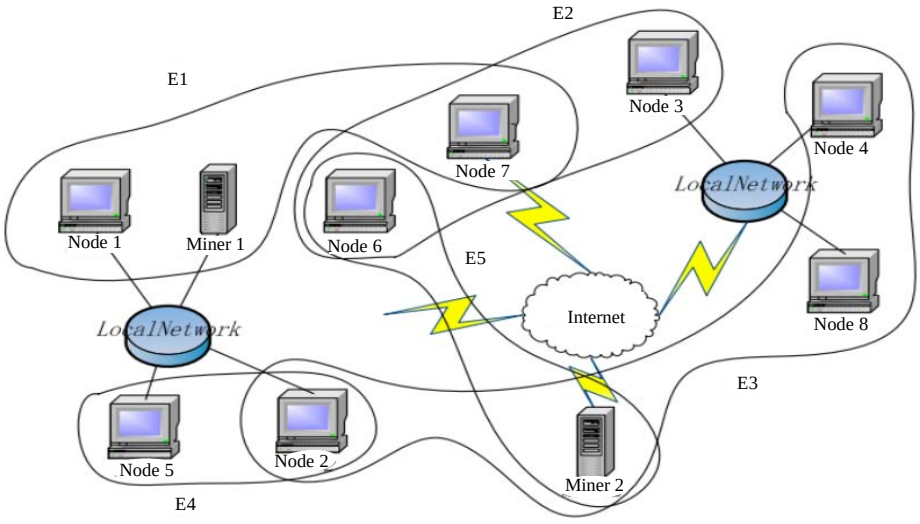

Fig. 2: Hypergraph based blockchain architecture (Qu *et al.*, 2018)

Table 1: The differences among the original blockchain models

Models	Storage	Blockchain structure	Verification	Miner's function
Original blockchain	One node one copy	One chain	By node itself	POW
Hypergraph-based blockchain	Part nodes have a copy	Several subchains	By other nodes	POW and linear independence matrix

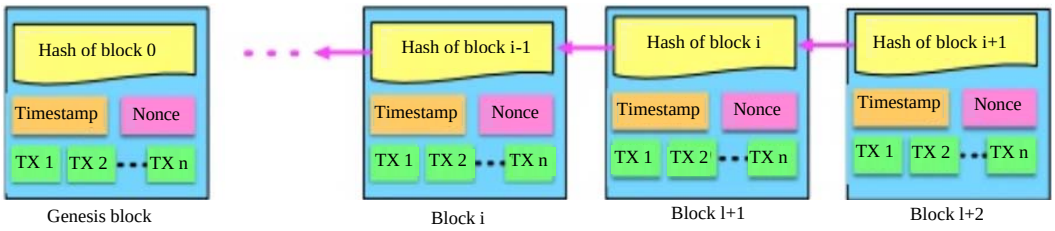

Fig. 3: An example of of a continuous sequence of blocks in blockchain (Miller, 2018)

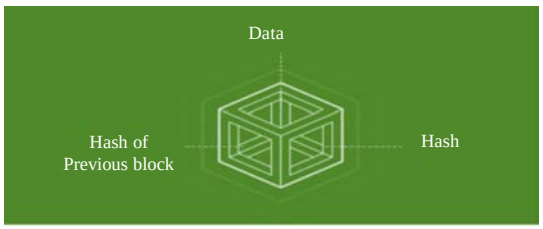

Fig. 4: Components of a block in a blockchain (Lewis and Larsen, 2015)

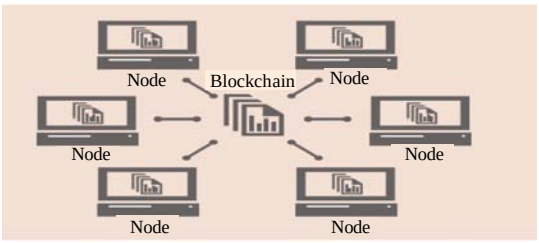

Fig. 5: The network nodes of blockchain (Lewis and Larsen, 2015)

network entities. When running this program, the entities work as individual validators, named the nodes of network. As a first time, if a node connects to the network, it will download a full copy of the database of blockchain on to its computer/server (Lewis and Larsen, 2015). The nodes network manages the database, also called the blockchain. The nodes are points for adding new data as well as validating and propagating the new data which have been presented for the blockchain as shown in Fig. 5 (Lewis and Larsen, 2015).

Hypergraph structure: The system of a hypergraph and finite sets represents the most general notation in discrete mathematics. In the past few years, the theory of hypergraph has been demonstrated to help in real-world problems solving. As a mathematical notation,

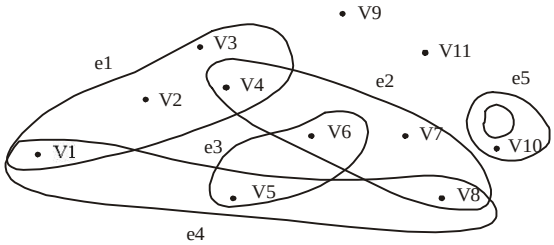

Fig. 6: An instance of a hypergraph (Qu *et al*., 2018)

hypergraphs can be used to simulate computer networks, biological networks, data structures, process scheduling and various other systems (Qu *et al*., 2018). An instance of a hypergraph is illustrated in Fig. 6.

If the existing block in a specific sub-blockchain of a specific node is full (certainly, the existing block of the sub-blockchain refers to a vector of other nodes in the same hyperedge in the head of sub-blockchain is full as well), regarding to the working concept of blockchain, the existing full block data, the value of the former block hash and other information will be presented to the network. The whole miners will take these data and competitively compute the value of encryption hash, if a miner resolves the puzzle, then, it will present it on the network and the nodes that gain this POW will easily verify the results. When the results are reasonable, the block will be encrypted and stored, else the results will be ignored and the computations continues. The differences among the source blockchain models are demonstrated in Table 1 (Qu *et al*., 2018).

Security discussion: If the transaction is occuring, then, the blockchain network nodes will compare the vector of the recorded attributes with the vectors in its own head of sub-blockchain. When the transaction and the matching process is verified to be valid, the record is inserted into the existing block of the corresponding sub-blockchain. These records are separately stocked and nearly there is

no one has a copy for these recodes which is diverse with distributed storage as by Raman and Varshney (2017) that utilizes a coding approach for reducing the capacity of storage and ensuring all the record's integrity. Dependent on the operating mechanism, the rate of the success of the attack is based on two operators, the threshold of verification and co-rank (cr). The threshold of verification identified the number of the forged nodes when the attacker needs to be trusted. And the co-rank identified the number of nodes is in a hyperedge. Thus, higher numbers of the threshold of verification and co-rank are recommended for protection against this security problem.

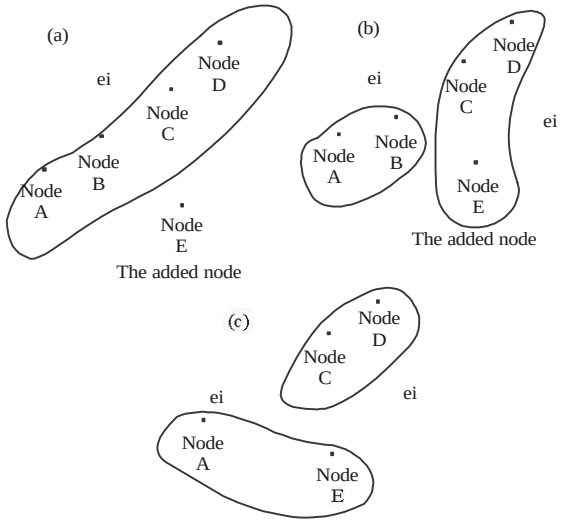

Fig. 7: a-c) Insertion and deletion of a node (Qu *et al*., 2018)

Particularly, when the co-rank is N that is the number of the nodes. Qu *et al*. by Bretto (2013) use tϵ(0, 1), therefore, to improve the security issues of blockchain network, we use in this study co-rank equals to N-1 to prevent sub blockchain equals the original blockchain and verification threshold which is a random number obeying the standard normal distribution that is tϵ(0, 1). The biggest values of c and t, the more nodes required. If a node newly enters the network, it will be inserted randomly to different hyperedges. A schematic diagram of dividing and aggregation is shown in Fig. 7. In order to keep the connection of hyperedges, if a node is inserted to the network, it is simultaneously inserted to different hyperedges.

RESULTS AND DISCUSSION

Experiments and evolution: In this study, the process of analyzing security shows the necessity of the threshold of verification and co-rank. The experiments have been designed to verify the network characteristic and the obtained results in Fig. 8 illustrates that the effect of using verification threshold as random number obeying the standard normal distribution when the attacker needs the transaction to be trusted, he/she should control at least c/(1- t) nodes and the difference between using t obeying normal distribution and from using uniform distribution in (0, 1). The high values of c and t, the most nodes required. In Eq. 1, T (n) represents the difficulty to forge a hyperedge. It is concerning with network scale N, the rank C and the verification threshold t obeying normal distribution.

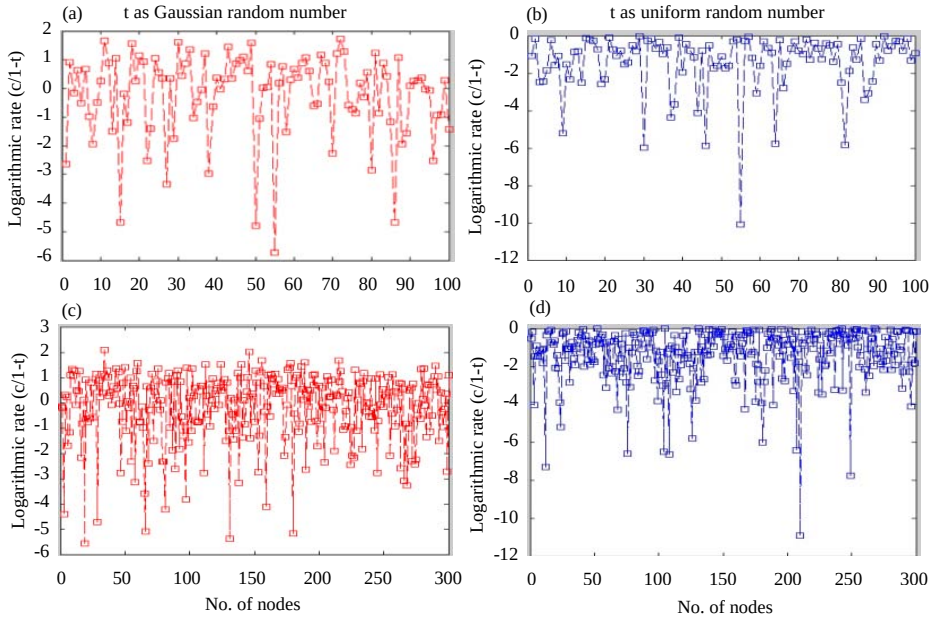

Fig. 8: Continue

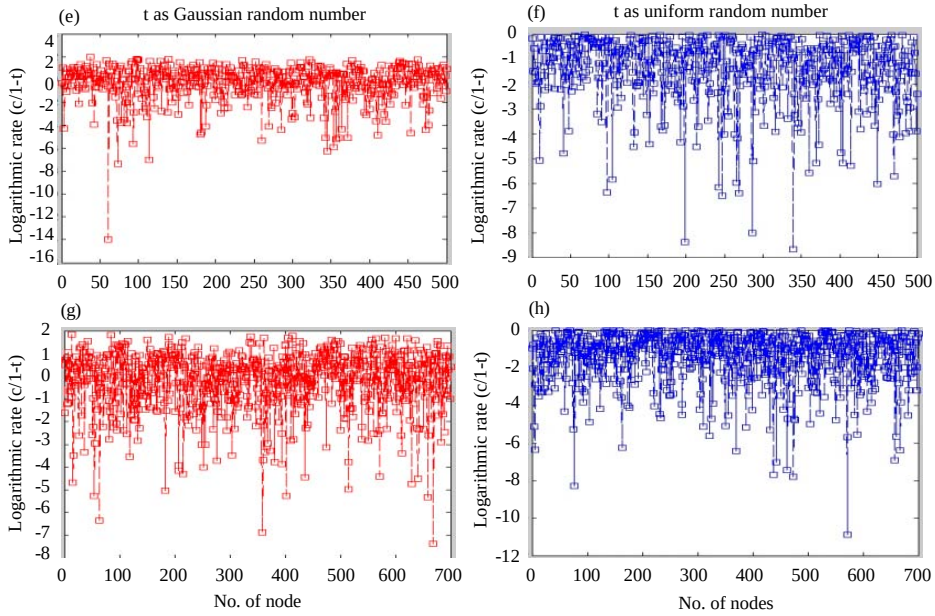

Fig. 8: The network evolution with different N and threshold: a) N = 100; b) N = 100; c) N = 300; d) N = 300; e) N = 500; f) N = 500; g) N = 700 and h) N = 700

$$T(n)=\left(\frac{C}{2}\right)^{\log_2\frac{N+1}{2}}\times\left(\left(\frac{C}{2}^{\log 2\frac{1}{1-t}}\right)-1\right)$$

CONCLUSION

In this research, a new method is proposed for increasing the performance of blockchain via. abstracting the network of blockchain in a hypergraph. The theory of hypergraph has been used for partition the whole network into several hyperedges and every hyperedge stores a portion of transaction data to minimize the pressure of storage. An extra security problem has been discussed for this model and put forward the strategies of response and the security risk to an reasonable stage via. the network setting factors has been reduced. Experimental results of using verification threshold t as Gaussian random number can improve the security of blockchain network relation to the hypergraph rank C.

ACKNOWLEDGEMENTS

I will be so glad to be thankful for all my colleagues to support my works in place of Hamorabi College Medical, University of Babylon.

REFERENCES

Akins, B.W., J. Chapman and J. Gordon, 2013. A whole new world: Income tax considerations of the Bitcoin economy. Pittsburgh Tax Rev., 1: 1-39.

Bretto, A., 2013. Hypergraph Theory: An Introduction. Springer, Cham, Switzerlands, ISBN:978-3-319-00080-0, Pages: 119.

Esposito, C., A. De Santis, G. Tortora, H. Chang and K.K.R. Choo, 2018. Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE. Cloud Comput., 5: 31-37.

Gatteschi, V., F. Lamberti, C. Demartini, C. Pranteda and V. Santamaria, 2018. To blockchain or not to blockchain: That is the question. IT. Prof., 20: 62-74.

Heutger, M. and M. Kuckelhaus, 2018. Blockchain in logistics: Perspectives on the upcoming impact of block chain technology and use cases for the logistics industry. Accenture, Dublin, Ireland. https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf

Hileman, G., 2016. State of blockchain q1 2016. CoinDesk, New York, USA. https://www.coindesk.com/state-of-blockchain-q1-2016

Kan, J., S. Chen and X. Huang, 2018. Improve blockchain performance using graph data structure and parallel mining. Cryptography Secur., 1: 1-6.

Kosba, A., A. Miller, E. Shi, Z. Wen and C. Papamanthou, 2016. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. Proceedings of the 2016 IEEE International Symposium on Security and Privacy (SP), May 22-26, 2016, IEEE, San Jose, California, USA., ISBN:978-1-5090-0825-4, pp: 839-858.

Lewis, A. and M. Larsen, 2015. Understanding blockchain technology and what it means for your business. Master Thesis, Accenture, Dublin, Ireland.

Miller, D., 2018. Blockchain and the internet of things in the industrial sector. IT. Prof., 20: 15-18.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. J. Netw. Comput., 1: 1-30.

Peters, G.W., E. Panayi and A. Chapelle, 2015. Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective. J. Financial Perspect., 3: 1-46.

Qu, C., M. Tao and R. Yuan, 2018. A hypergraph-based blockchain model and application in internet of things-enabled smart homes. Sens., 18: 1-18.

Raman, R.K. and L.R. Varshney, 2017. Dynamic distributed storage for scaling blockchains. Inf. Theor., 1: 1-19.

Schuh, F. and D. Larimer, 2015. BitShares 2.0: Financial smart contract platform. Master Thesis, Cryptonomex Inc., Blacksburg, Virginia.

Treleaven, P., R.G. Brown and D. Yang, 2017. Blockchain technology in finance. Comput., 50: 14-17.

Zhang, Y. and J. Wen, 2015. An IoT electric business model based on the protocol of bitcoin. Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, February 17-19, 2015, IEEE, Paris, France, ISBN:978-1-4799-1866-9, pp: 184-191.

Zheng, Z., S. Xie, H. Dai, X. Chen and H. Wang, 2017. An overview of blockchain technology: Architecture, consensus and future trends. Proceedings of the 2017 IEEE International Congress on Big Data (Bigdata Congress), June 25-30, 2017, IEEE, Honolulu, Hawaii, USA., ISBN:978-1-5386-1997-1, pp: 557-564..