TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 4425 - 4434

When IoT Meets Blockchain: Challenges in Distributed Consensus

Dr. Sunitha. C[1], CHRISTINA J[2], VIGNESWAR J[3]

[1] Head of Department, Sri Krishna Arts and Science College

[2,3]Student, Sri Krishna Arts and Science College

Article Info
Volume 82
Page Number: 4425 - 4434
Publication Issue:
January-February 2020

Article History
Article Received: 18 May 2019
Revised: 14 July 2019
Accepted: 22 December 2019
Publication: 22 January 2020

Abstract

The blockchain is seen as a beneficial development for IoT (Internet of Things), as it offers vital answers for a package which can fix security and trust checks, major help expenses, etc. Blockchain's decentralization will be mainly due to the consensus mechanism which awards specific trade during a distributed path without the ties between others. It begins with the basic message of blockchain and explains why the accepted component recognizes a particular career during a blockchainIoT process. Two basic ideas of commended mechanisms such as Proof of Stake (PoS) and Proof of Work (PoW) are addressed and reports are demanded in IoT. The Direct Acyclic Graphs(DAG) is used to show why it is reactive than IoTPoS and PoW structure. Hashgraph and Tangle are mainly based on consensus mechanisms.

Key words:*Consensus Mechanisms, Blockchain, IoT, DAG, Tangle..*

INTRODUCTION

As a powerful platform to improve day-to-day operations, build recent business models, goods and services, as well as a broad range of analytical issues and concepts, IoT receives great attention from culture, industry and the world. Even though the first IoT project came into existence over the past 20 years and since then there have been multiple IoT systems, some unresolved and critical problems remain the following:

Trust: Closed systems are IoT database servers. One of the things that services are able to control IoT devices illegally is the flexibility. for one, the collaboration and trust relationship between entirely different IoT entities is arduous;

Safety: The IoT knowledge centre is sensitive because the Distributed Denial of Service(DDoS) attack can be easily done by hackers and once the situation arises, any IoT system can also be affected by hierarchical topology;

Operating cost: At the present hierarchical model, it costs a lot to manage, i.e. upgrade code for several IoT devices in a timely manner.

Scalability: The low measuring efficiency of central topology does not comply with the requirements of the broad combination of IoT devices.

Blockchain, as a whole, was originally conceived in 2009 for the Digital Currency Bitcoin[1] as a Distributed Ledger Technology(DLT). Despite decades of service in an increasingly decentralized network, Bitcoin has yet to face serious security incidents. Partly because the consensus method, using the computation power of the whole network, is improved to ensure information exchangeability. As such, blockchain is supposed to change IoT environments by providing responsive and additionally effective solutions to security decentralization. As indicated in the IDC International Data Corporation 2019 report, 200th IoT organizations will be able to have fundamental grades of blockchain-enabled administrations [2].

A. What is blockchain

In order to build trust and consensus in restricted frameworks, Blockchain could be a shared record (P2P) of acceptable technology. For one thing, to address the problems of an untrustworthy and distributed environment1, the blockchain mechanism is implemented in a restricted way to agree on transactions between individual clients. In the decentralized blockchain system, security is assured[3] with the aid of computerized labeling and hash equation based on general encryption.

Blockchain has 3 fundamental forms: transaction, block and chain. In reality, all the precious information is a payment that is to be carried on the blockchain network. The "transaction" is not limited to trade. The blocks are capable for recording transactions made by those customers approved by the consensus process and transmitting them. The hash value which is registered by the block after it is identified in clear terms to each block. It provides a relation between all the blocks and therefore specifically records a group of blocks. Blocks accumulating consecutively in consensus methods will dramatically multiply the cost of threats and harmful modifications [1].

B. Benefits of Blockchain forIoT

First, the pressures of the hotspot and the risk of single failure can be substantially reduced by blockchain-based decentralization. Secondly, consensus and authentication mechanisms can be used in blockchain to improve IoT safety. Yes, IoT devices can autonomously conduct trading and actions using intelligent contact[5]. In addition, blockchain offers a trust mechanism for IoT business communication as a publicly distributed ledger in which stored data can be investigated by all users.

C. Integration of IoT and Blockchain

Right today, the use of Internet of things and blockchain is encouraged and supporting structures and projects have already been introduced in many fields[5].It establishes blockchain value chain template for the supply chain industry. In this design, a log of the distribution of container deliveries will run within the blockchain. Each supply chain entity will be monitoring all movement from start point to end point to lower shipment delay and to accurately monitor the missing value In the clinical field[6] the patient model is used to plan individual health information using a blockchain system that ensures that people are data-owners and integrity. The system is adamant that consumers are using their direct knowledge despite worrying regarding safety issues with its access control guidelines. However, within the choice IoT technologies, blockchain is also open, similar to improvements for centralized programming and vehicle protection[7].

Blockchain assumes a major job on the internet in particular. There are a few blockchain technologies in these days which have researched how IoT devices can encourage power sharing in order to increase their energy usage rate. For instance by using Internet of Vehicles (IoV), electric vehicles can absorb energy across non-top areas and supply energy throughout the peak season as distributed generators. A localization model for P2P Electricity mercantilism, in which blockchain institutes are utilized to improve the safety in Group action without the use of a foreign entity, is proposed to modify secure power mercantilism[8]. The payment-based transaction scheme[9] proposes improving merchandising power by developing digital credit banks that facilitate quick and popular mercantilism among the energy knots. In addition, a certain digital currency was conferred for blockchain-based renewable mercantilism, such as "Specoin"[10].

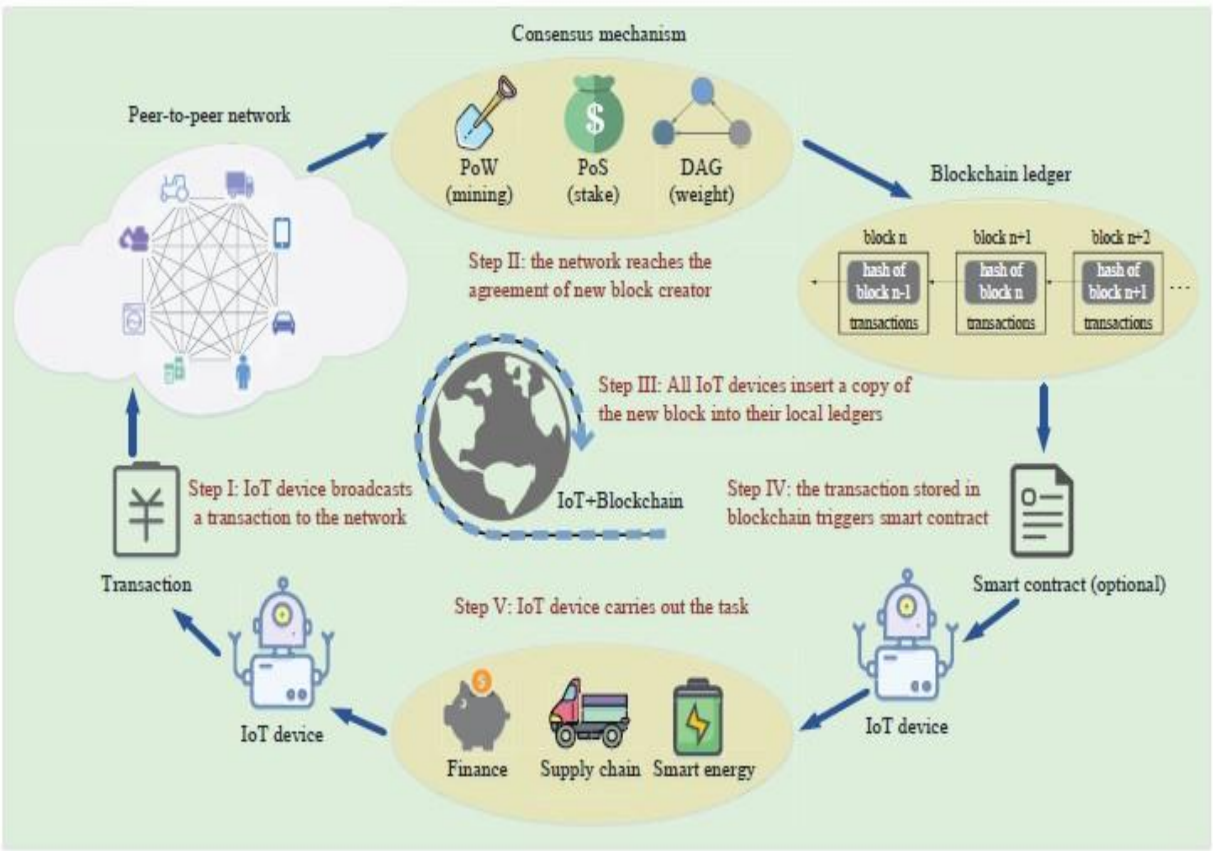
Consensus mechanism
Peer-to-peer network
PoW (mining)
PoS (stake)
DAG (weight)
Blockchain ledger
block n
block n+1
block n+2
hash of block n-1
hash of block n
hash of block n+1
transactions
transactions
transactions
Step II: the network reaches the agreement of new block creator
Step III: All IoT devices insert a copy of the new block into their local ledgers
IoT+Blockchain
Step I: IoT device broadcasts a transaction to the network
Step IV: the transaction stored in blockchain triggers smart contract
Transaction
Smart contract (optional)
Step V: IoT device carries out the task
IoT device
IoT device
Finance
Supply chain
Smart energy

Fig. 1: An example of implementing blockchain in IoT system

The function to empower a blockchain is seen in the fig. 1. In the fig 1, the consensus process is the foundation for a blockchain-enabled IoT platform, which generates an extension among network data and the data agreed to carry

out different uses. The purpose of the work is therefore to clarify the complexities of a consensus process for blockchainIoT Frameworks that are empowered. The basic structure of various types of consensus structures and their benefits and drawbacks in the biological IoT process was addressed at that stage in certain practicable Direct Acyclic Graph (DAG) exam headings based on consensus process.

We tend to discuss mechanisms and processes in Section II, which take into account their practicability for IoT's, to incorporate the key consensus method, which includes Proof of Work Proof of Stake and DAG. We examine section II existing DAGs (Hasgraph and Tangle) in Section III, mainly exhibit through a consensus mechanism and show their benefits in Internet of things through quality exams. We tend to discuss DAG in Section IV. In Section V conclusions are shown.

II.CONSENSUS PROCESS IN BLOCKCHAIN

In the present section, it explains various types of consensus frameworks within blockchain and analyze if the preparation requirements of the correct consensus framework deal with IoT problems or not. A consensus process takes on an important task in blockchain in order to determine the question regarding legitimacy by reacting to "which one has the privilege of putting this block in blockchain." With the framework of consensus, the results is correctly reported for all clients without the outside agency. DAG's mainly based consensus process was implemented as an effective resolution. Several consensus structures are now being developed, with Proof of Work and Proof of Stake being the most commonly used ones. Nonetheless, all conventional blockchains and consensus structures also face key problems for the IoT process.

A. Proof of work (PoW)

In the blockchain system, PoW is predicted (e.g., Bitcoincryptocurrency). The central structure for PoW is that the Power Register [1] challenges the consensus (miner) center to use its working capital to hack business and bid for a new block of bonuses. The champion is that the first person who gets less than the stated objective is a hash price. At one standpoint, PoW's storage issue should be high enough to prevent forking [3]. Anyhow, the higher processing issue will cause the energy consumption to be reduced and useless. The accessible IoT app capacity is severely limited. PoW is therefore not a good IoT device option.

B. Proof of Stake (PoS)

In PoSblockchain, coinage is used as a strategic distance from high-calculative multifaceted nature of hash activity (e.g., Nxt[11]), which differs from PoW's processing capability. The coinage of an unused trade production suffices to increase its value by the time it was made. A greater age of coinage in PoS will provide a greater chance that the nodes will win the authority to make an alternative block and then use the coin-age (refresh as zero) as the holder has won. Give the chance to win is genuinely regulated by the age of coin. PoSis beneficial to the rich digger and could possibly lead to duopolies or near controlling business models. In this case, it may not be feasible for the POS consensus framework to carry out a clever distributed IoT model.

C. Drawbacks of PoW and PoS

PoS and PoW are two conventional structures of consensus which operate on a single chain structure. The understanding process will impede the entry rate in the most recent blocks to avoid the bending and hold a variety of blockchain records among all customers. This could trigger some significant bottlenecks for IoT.(i) Consumption of capital: The conventional consensus method can use abundant resources (i.e., energy storage at PoW, POS coinage), which is essentially irreproachably exorbitant for asset-constrained IoT phones, to impede the entry of number of new block and prevents blockchain from attacking.(ii) Transaction charge: The conventional consensus method requires transaction fees to fund the miners that could cause a considerable burden in the Internet of things Structure, where the majority of trading is micropayment. (iii) Output restriction: Even though the ability of replacement blocks is restricted, Transaction Per Second (TPS) is usually restricted to dozens (For instance, 7 TPS in the Digital currency and also 20 TPS to 30 TPS on the Ethereum, that cannot respond to the extremely rapid development of IoT equipment). (iv) Acknowledgement lag: The confirmation lag is probably long for IoT apps due to the minimal authentication of number of new blocks (e.g., hr n Bitcoin and 3 mins in Ethereum).

D. Direct Acyclic Graph (DAG)

It is expected that the development of DAG and its consensus process will solve the limitations of conventional IoT consensus. In DAG-based consensus process, it lets users to add the blocks into another blockchain at a certain age as soon as they complete a transaction earlier. Several branches would be formed simultaneously during this method, which is called forking. In several conventional consensus approaches, this design is sometimes considered a problem as it would trigger "double-spending"[1]. Nonetheless, the mostly consensus-based DAG framework styles revolutionary algorithmic rules and protocol (explained in the next section) to resolve the double spending drawback and permit any fresh transfers to enter the network in a topology that is extremely forking. The confirmation speed and TPS will therefore no longer be restricted. In addition, the information stored in the DAG which is covered by large forking blocks, consumption of resources is going to be terribly small for a client to create a replacement block. As a result, skilled miners are disappearing and minimal or no service charges are feasible, which is crucial to the IoT environment.

III. DAG BASED ON CONSENSUS PROCESS

A. Tangle

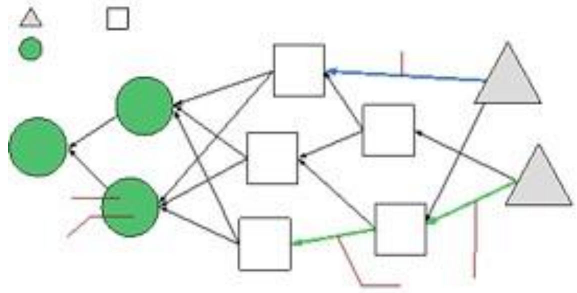

Fig.2:AnexampleofTangle

Tangle is IOTA's mathematics [12], an IoT company cryptocurrency. In the figure 2, Tangle is shown to be a DAG-based transaction log. It permits entirely new branches to integrate into the chain, leading in a quicker overall results. In Tangle, a no of tips must be accepted in order to unlock ledger as replacement point for holding a contract (typically 2[12]). As a result, the high arrival speed of the latest exchanges will be confirmed by the faster earlier payments. On either hand, as tips are also the childless vertex in Tangle, the current vertex chooses as well as includes tips that could limit the unit to a cheap scale. In addition, as the remaining task at hand to make a substitution point is light, all clients will give their exchanges whenever without exchange charge that is pivotal to IoT gadgets situations.

The Tangle consensus has to do with accumulative size. As illustrated in Figure.2, The accumulative intensity of a particular payment is that the total of the own weight of the vertex (approximately equal to the PoW endowed by the problem node[12]) is legitimately and roundaboutly supported by the general weight of vertices. Even though the exchanges put away in Tangle is checked by processing power, an exchange's cumulative weight means its validity within the scheme and goes as unambiguous requirements to address the issue of the double expenditure.

The key procedures are described as follows in addition to issue a replacement dealing and enable the other users throughout the process to approve it (i.e., obtain enough accumulative weight to succeed in a consensus agreement). (i) To store the payment, a user generates a unit as more of a vertex within the DAG map. (ii) Users pick 2 non-conflict tips in compliance with the algorithmic principle of the Markov Chain Monte Carlo (MCMC) [12] and apply the hash of the chosen tips to their storage. (iii) The viewer finds time to resolve a crypto puzzle in order to meet the objective of the problem. It's close to PoW, but it has a very low working complexity that can prevent spamming. (iv) The client uses his non-public key to register and relay the storage unit to others for security purposes. (v) At the time that opposing customers get this, they should verify whether the advanced mark is legitory or not and PoW based on the majority of the new storage devices that were effectively inspected for the non-components would be added to the Tangle as a replacement tip.

The building forking (or the branch) and re-trying research in an open ledge is primarily about adjusting information and doubling expenditure. The single block-based consensus system (e.g., PoW) uses the longer chain as its basis for handling this downside The typical customer should select longest chain to run when burning takes place, ensuring and optimizing their statement interest. The reason seems that longest chain has a low risk of orphaning.

The Tangle also uses the algorithmic MCMC tip selection principle to pick the branch with highest total weight accumulation. In addition, the general registration ability of reasonable customers in a large IoT network can be strong, thanks to appropriate and simultaneous support from Tangle, to stop duplication of expenses when an attacker's branch is difficult to overcome the honest ones. In the meantime, no individual user will use much energy for security computing.

B. Hashgraph

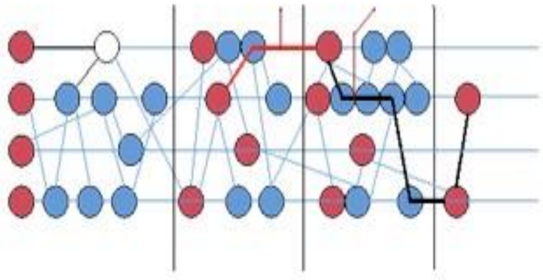

Figure 3: An example of Hash graph

For distributed state devices, Hashgraph[13] is designed to ensure byzantine error detection; it is asynchronous, decentralized, not a dust, ultimate probable consensus and rapid in the technique of consensus. Hashgraph keys are the gossip protocol and the virtual vote. That offer is exposed to all users using a gossip protocol. Then a digital voting algorithm principle is used to reach an agreement for the sequence of payments. We will concisely explain how the gossip protocol and online voting work in order to facilitate a knowledge of Hashgraph.

Each Hashgraph customer will randomly pick a different customer to report each exchange he knows as per Gossip protocol. For instance, shadow unit is shown in figure 3. represents B sending any data to A, which A will not understand, so A generates an event that connects A and B to hold hidden information. Thus all individuals will gradually be known for each event. The overhead for sharing of a storage unit, including location data (3 to 6 byte), a signature (64 bytes), transactions inside the device (around 100 bytes), may be a cheap technical gossip protocol. The process must choose the "famous witnesses" in the form of digital votes to achieve consensus (the graph connectivity is maintained in all customers ' choices). In order to achieve consensus. The prominent witnesses were selected from the key occasions in each round (In figure 3, red units). A process of choice involves polling and confirmation. As Fig 3 shows, in round 3 spectators vote for round 2 witnesses. Then in round four, the witnesses will take votes in round three. If the selection is successful in round three and the test in round four, the witnesses are noticed in round 2. The incidents voted by the well-known witnesses in round 1. Both users recognize the time of formation of the verified events as a signal to avoid double expenditure.

C: Comparison

We equate its success with two other consensus mechanisms in Table I to illustrate the benefits and drawbacks of the DAG-based consensus for IoT.

All such similarities indicate that the DAG mainly based on mechanism of consensus as well as PoW and PoS for the huge-scale IoT. In particular, DAG-based consensus process has a reduced transaction fee and resource usage, and can achieve significantly greater transaction efficiency. For DAG-based consensus structures, such as Tangle centralization, a few impediments remain however. In addition, the delay of confirmation of the DAG mechanism of consensus would be influenced significantly by traffic loads, particularly when traffic load evolves over time in the realistic IoT scenario. Therefore, however, the above-mentioned inquiries should not be addressed in order to implement a DAG-based on mechanism of consensus.

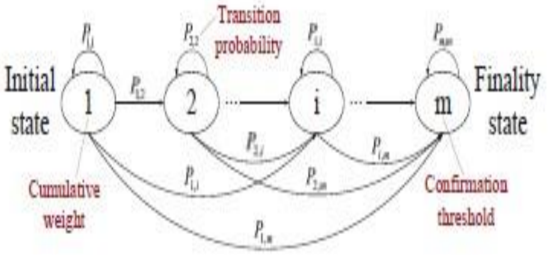

Figure 4: Markov chain model

IV.CHALLENGES IN DAG

While the DAG based mechanism offers many advantages, and that is far from well-used in IoT technologies as an expanding technology. There are major issues to be explored with DAG-based consensus processes.

A. Analyzing Model

The plan to produce a summarized hypothetical numerical system must be based mostly on a consensus method to dissect the DAG presentation.

In[12] the researchers examine the cumulative weight growth rate in static heavy load administration in general. In the Tangle consensus method they have provided theoretical and practical insights. The developers demonstrate the existence in[14] of (nearly symmetric) Nash equilibrium in a probabilistic process that is considered by the DAG when a piece of competitors attempt to streamline certain ways. Taking into account the possibilities of the consensus process, we find a promising solution to the theoretical method using the Markov chain. Figure 4, provides the description of a markov chain template for the Substitution Management Agreement Procedure.

In light of the fact that the assert measures, the model is using the total weight of Tangle. We will thus review the N-step chance of advancement from the current condition to last one. Thus, a hypothetical methodology could disrupt the expanded rate of total mass, TPS as well as postponement.

TABLE I: Comparisons of PoW, PoS and DAG based Consensus

	Bitcoin [1]	Nxt [11]	Tangle [12]	Hashgraph [13]
Byzantine fault tolerance	<51% of all computing resource	< 1/3 of total assets	<51% of all computing resource using MCMC tips selection	Dishonest participants < 1/3
Transaction fee	0.0001 BTC	1 Nxt	Zero	Zero
Resource requirements	Enormous computing power	Coin age	Low computing power	Low computing power and bandwidth
Throughput	7 TPS	4 TPS	No technical up bound	2.5×10^5 TPS
Confirmation delay	60 mins	10 mins	Depend on transaction arrival rate	Subject to communication frequency
Finality	Six cumulative blocks at least	Ten cumulative blocks at least	Cumulative weight reaches confirmation threshold	Seen by all the famous witnesses in a latter round
Unique features	• Competition for mining • PoW	• The miner of the next block are predictable • PoS	• Offline transactions • Quantum Immune • DAG	• Proof of Asynchronous Byzantine fault tolerance • Gossip to gossip and Virtual voting • DAG
Major drawback	High resource consumption (hash complexity)	Centralization concern (coin age)	• The large confirmation delay in low trading traffic load • Centralization concern (when coordinator involves)	The large confirmation delay caused by low communication frequency (gossip protocol)

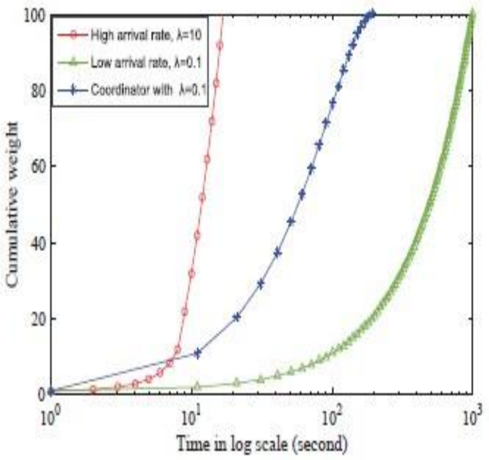

Figure 5: Cumulative weight growth curve

The best way to achieve the structure of change probabilities is one of the biggest and continuing drawback of Markov Chain model, particularly in the gigantic system scale with a wide array of process systems. In addition, the likelihood of transformation is strongly influenced by preparation requirements from the consensus system, for example, Hashgraph and Tangle are completely extraordinary. Therefore, within future work, the model based on the Markov Chain must be strengthened.

B. Limitation of the Low bound

Since we have already mentioned, in the consensus mechanism which is based on DAG, there is neither scientific connection. It would not be realistic, however, that new business will arrive quickly, continuously in functional IoT circumstances. For instance, there are only little transaction at nighttime for taking the bike sharing request. In this scenario, the lag in verification may be very tremendous.

We tend to perform a simple simulation using Section A's Markov chain model, to indicate the effect of the arriving frequency (described as) on consensus system. In the illustration 5, we may obviously get that the additive weight is slowly increasing when the arrival frequency of the new deal is small. Since it is dependent on its additive weight if the approval of deals is confirmed [12], the time limit for confirmation would be extremely long until the arrival rate has dropped. Towards this purpose, the coordinator participates in a DAG consultation process to improve the confirmation frequency in low traffic loads. An external individual, that offers a zero valuation exchange to manage informal trades, is limited by the facilitator. In the illustration 5, we would have seen that the additive weight is increasing faster in the lower arrival situation with the aid of the organizer. This answer, on either hand, could solve major confirmatory lag problems in lower incoming rates. Once, centralisation drawback can be triggered, because the facilitator could be an outsider who opposes the main blockchain norm. It means that the arranger can be used only in non-public or shut down cases, i.e. the blockchain consortium.

C. Mobile Blockchain

IoT devices are obviously linked remotely. Communications are believed to be configured or flawless for a few tests of the consensus system (i.e. Hashgraph and Tangle). But the interaction problems in blockchain powered IoT frameworks from entirely different levels were addressed.

1) Lower layer:

In physical framework, it must be examined how much the remote correspondence value effect / force the blockchain-empowering IoT structure (e.g. blocksizes, rate of transfers) and verifying delays submit, etc, some simple metrics like the signal-to-interference-plus-noise relation (SINR) and communications efficiency. On either hand, provided an all-round exchange within blockchain (i.e. 1 block every 10 mins as outlined in bitcoin [1]), the best method for sending IoT devices that ideally meet this requirement is relevant. This problem is because IoT products can be significantly connected, which is described for wireless transmission in fifth generation (5G). The balance between both the framework and the application of protection is an interesting challenge to analyze.

However, physical linking and the authentication protocol can affect communication efficiency and latency quality, that could pose a further obstacle to the consensus method by means of dual factors Finally, it is important from system level to design the joint network and mechanism to optimize safety.

2)Upper layer:

In the routing layer, the low bottleneck deferment will affect the methods of consensus (that is , "lazy" Node mistakenly considered[12]) provided the memory storage and procedure limit of the IoT gadgets. An inexpensive steering arrangement within the IoT platform driven by blockchain should therefore lead towards the inventive IoT tools to build exchanges. In the meantime, the protocol should be required to meet the particular QoS specifications of the blockchain framework in the Transmission Control Protocol (TCP) layer. In particular, the protocol will specify precise reason for a failure in a transaction. When a transaction error is triggered not by a consensus but by a transmission or scheduling error, the transfer should be carried out using the repair and restoration protocol.

D. Blockchain Utilization Strategy

Each member has the authorization to store and review the leader on a circulated basis in the DAG consensus process. Even though most IoT systems are power and memory-restricted, the power saving techniques must be intended to make the customer work easier and more efficient. For example, a resource utilization strategy may be developed to allow energy-limited IoT technologies to only address payments, IoT machines capable of transaction processing and creating blockchain. In the meantime, certain incentive structures to encourage the right IoT products in the consensus system should be applied in terms of greed and fairness. To make IoT systems possible, concept of games is a natural fit to construct the ideal situation in a decentralized manner. In [15] eg, the researchers suggest a bid-based approach to PoW mobile blockchain offloading.

V. CONCLUSION

Here we are discussed blockchain solutions and the advantages of using them in IoT frameworks. We begin by defining the most conceptual arrangements like PoS, DAG and PoW and speak about the privileges and obstacles of PoW and PoW. The Hashgraph and Tangle are provided with two DAG-based elements. Researchers are thinking together about basic qualities for hostages, DAG and PoS. We have reasonable results on re-enactments to demonstrate how the exchange presence rate impacts on a DAG-based blockchain consensus system and to reveal its small other impediment to it. The difficulties for the IoT system based consensus framework on DAG are minimized by the research template, major obstacle, multiple blockchain as well as methodology for enhancement.

REFERENCES

[1] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” White paper, 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] I-SCOOP, “Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge,” 2018. [Online]. Available: https://www.iscoop.eu/blockchain-distributed-ledgertechnology/blockchain-iot/.

[3] G. BitFury, “Proof of stake versus proof of work,” White paper, Sep. 2015.

[4] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Trans. on Progr. Lang. and Sys. (TOPLAS), vol. 4, no. 3, pp. 382-401, Jul. 1982.

[5] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet-of-Things,” IEEE Access, vol. 4, pp. 2292-2303, May 2016.

[6] X. Liang, J. Zhao, and et al., “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” In Proc. IEEE 28th Annual International Symposium on PIMRC, Oct. 2017.

[7] A. Dorri, M. Steger, and et al., "Blockchain: a distributed solution to automotive security and privacy," IEEE Communication Magazine, vol. 55, no. 12, pp. 119-125, Dec. 2017.

[8] J. Kang, R. Yu, and et al., "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," IEEE Trans. Ind. Inf., vol. 13, no. 6, pp. 3154-3164, Dec. 2017.

[9] Z. Li, J. Kang, and et al., "Consortium blockchain for secure energy trading in industrial internet of things," IEEE Trans. Ind. Inf., vol. 14, no. 8, pp. 3690-3700, Aug. 2018.

[10] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access," IEEE Veh. Technol. Mag., vol. 13, no. 1, pp. 32-39, Mar. 2018

[11] Nxt. community, "Nxt: a peer-to-peer digital socioeconomic system," White paper, July. 2014.

[12] S. Popov, "The tangle," White paper, 2018. [Online].Available:https://www.iota.org/research /aca demic-papers.

[13] L. Baird, "The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance," White paper, 2016. [Online]. Available:http://www.swirlds.com/ developer resources/whitepapers/.

[14] S. Popov, O. Saa, and P. Finardi, "Equilibria in the Tangle," 2017.[Online].Available: https://arxiv.org/pdf/1712.05385.pdf.

[15] Z. Xiong, S. Feng, and et al., "Edge computing resource management and pricing for mobile

[16] blockchain," 2017. [Online]. Available: https:// arxiv.org/pdf/1710.01567.pdf.