When Internet of Things Meets Blockchain: Challenges in Distributed Consensus

Bin Cao, Yixin Li, Lei Zhang, Long Zhang, Shahid Mumtaz, Zhenyu Zhou and Mugen Peng

***Abstract*—Blockchain has been regarded as a promising technology for Internet of Things (IoT), since it provides significant solutions for decentralized network which can address trust and security concerns, high maintenance cost problem, etc. The decentralization provided by blockchain can be largely attributed to the use of consensus mechanism, which enables peer-to-peer trading in a distributed manner without the involvement of any third party. This article starts from introducing the basic concept of blockchain and illustrating why consensus mechanism plays an indispensable role in a blockchain enabled IoT system. Then, we discuss the main ideas of two famous consensus mechanisms including Proof of Work (PoW) and Proof of Stake (PoS), and list their limitations in IoT. Next, two mainstream Direct Acyclic Graph (DAG) based consensus mechanisms, i.e., the Tangle and Hashgraph, are reviewed to show why DAG consensus is more suitable for IoT system than PoW and PoS. Potential issues and challenges of DAG based consensus mechanism to be addressed in the future are discussed in the last.**

***Index Terms*—Consensus Mechanism, Blockchain, Internet of Things, Direct Acyclic Graph, Tangle.**

I. Introduction

Internet of Things (IoT) has been identified as one of the most disruptive technologies of this century. It has attracted much attention of society, industry and academia as a promising technology that can enhance day to day activities, the creation of new business models, products and services, and as a broad source of research topics and ideas. Although the first idea of IoT emerged no more than two decades ago and many IoT ecosystems have been generated since then, some unsolved and important issues are still remained as follows:

- Trust: IoT cloud servers are closed systems. For one thing, the service providers have the ability to illegally control IoT devices. For another, it is hard to build the cooperation and trust relationship among different IoT business agencies;
- Security: the IoT data center is vulnerable since it is easy to be attacked by hackers using Distributed Denial of Service attack (DDoS), and when it happens, all IoT service may be affected due to the centralized topology;
- Overhead: current centralized model has a high maintenance cost, i.e., it is costly to timely update the softwares of millions of IoT devices;
- Scalability: the poor scalability of the centralized topology cannot meet the needs of massive IoT devices connection, i.e., a large delay might be caused by a surge of service requests.

As a brand of new distributed ledger technology (DLT), blockchain is originally designed for digital currency Bitcoin in 2009 [1]. With decades of operation in a decentralized network, Bitcoin did not encounter serious security incidents. This can be largely attributed to the advantage of consensus mechanism, which uses the computing power of whole network to ensure the immutability of the data. As such a security decentralization solution, blockchain is expected to transform IoT ecosystems by making them smart and more efficient. According to IDC (International Data Corporation) report, by 2019, 20% of IoT deployments will have basic levels of blockchain enabled services [2].

A. What is Blockchain

Blockchain is a peer-to-peer (P2P) distributed ledger technology for establishing trust and consensus in decentralized networks. On the one hand, to address the challenges in trustless distributed environment[1], consensus mechanism is adopted in blockchain in a decentralized way to reach the agreement for transactions among individual users. On the other hand, using digital signature and hash algorithm based encryption, security can be assured in the decentralization blockchain system [3].

Blockchain ledger has three basic concepts: transaction, block and chain. The "transaction" in blockchain is not restricted for trading, in fact, all the valuable information can act as a transaction to be broadcast in blockchain network. The blocks are storage units to record transactions, which are created and broadcast by those users authorized by consensus mechanism. Each block is identified uniquely by its hash value, which is referenced by the block came after it. This establishes a link between the blocks, thus creating a chain of blocks namely ledger. With the blocks accumulate sequentially in consensus process, the cost of attack and malicious modification would be increased exponentially [1].

[1]Refer to the Byzantine Generals Problem [4].

Bin Cao (email: caobin@cqupt.edu.cn), Yixin Li and Long Zhang are with Chongqing University of Posts and Telecommunications of China, College of Communications and Information Engineering and Chongqing Key Lab of Mobile Communications Technology, Bin Cao is also with the Beijing University of Posts and Telecommunications of China, Institute of Network Technology. Lei Zhang is with the School of Engineering, University of Glasgow, Glasgow, G12 8QQ, U.K. Shahid Mumtaz is with the Institute of Telecommunications, Portugal. Zhenyu Zhou is with the University of North China Electric Power, College of Electrical Engineering. Mugen Peng is with the Beijing University of Posts and Telecommunications of China, College of Communications and Information Engineering.

This work was supported in part by the National Natural Science Foundation of China (61701059, 61831002), the State Major Science and Technology Special Projects (2017ZX03001025-06), and the Beijing Natural Science Foundation under Grant No. JQ18016.

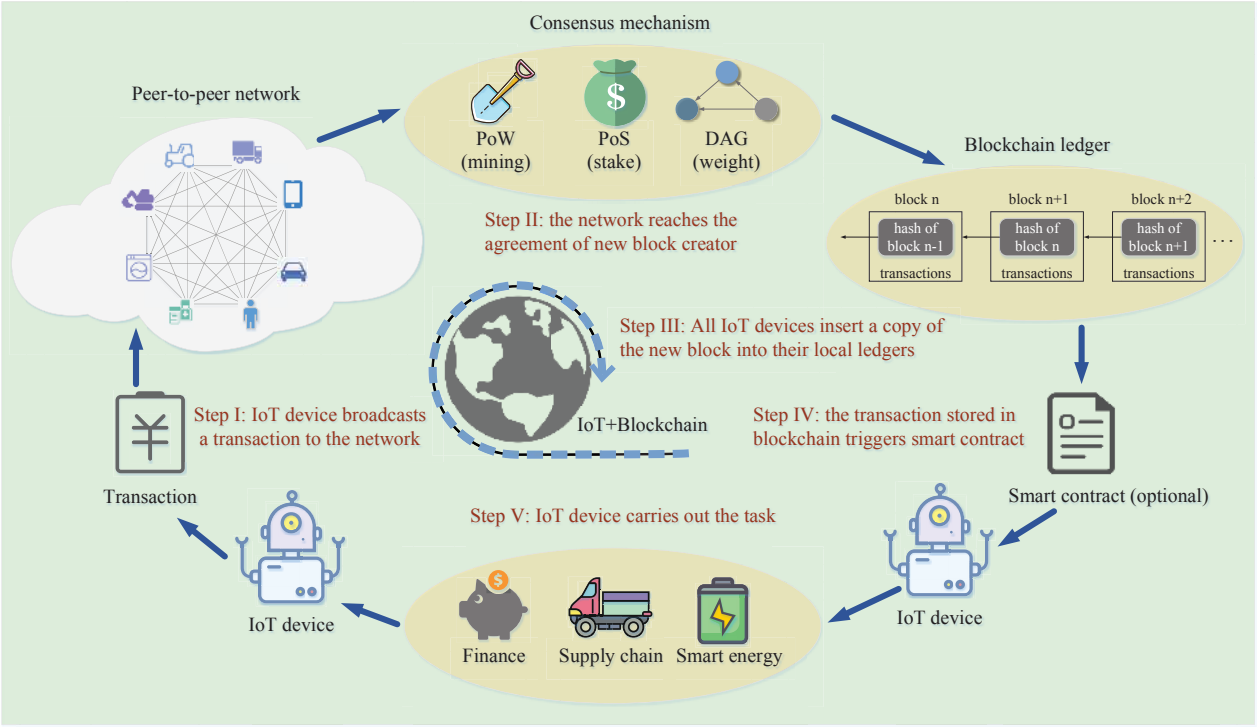

Fig. 1: An example of implementing blockchain in IoT system

B. Advantages of Blockchain for IoT

Firstly, using blockchain based decentralization, the burden of hot spot and the probability of Single Point of Failure (SPF) can be reduced significantly. Secondly, consensus mechanism and encryption algorithm in blockchain can be leveraged to strengthen IoT security. In addition, by using smart contact [5], IoT devices can carry out trading and execute actions autonomously. Besides, as a public distributed ledger where stored information can be audited by all the users, blockchain provides a trust platform for IoT business cooperation.

C. IoT and Blockchain Integration

Currently, the implementation of IoT and blockchain is on the agenda in industry and there are already promising solutions and initiatives in several areas. In supply chain industry, [5] provides a blockchain enabled supply chain model. In this model, the infomation stored in the blockchain can serve as a log of delivery for container shipments. All the movement of container from source to destination can be tracked by any supply chain entities, so that the shipment delay can be minimized and the missing asset can be tracked accurately. In healthcare domain, [6] provides a user-centric model for processing personal health data using blockchain network, ensuring the data ownership of individuals, as well as data integrity. By enforcing access control policies, the system makes sure that users can handle their personal data without worrying about the privacy issues. Besides, blockchain is also available in the other IoT applications, such as remote software updates and insurance for vehicle [7].

Particularly, blockchain plays an important role in energy trading for IoT applications in energy Internet. Nowadays, there exist some blockchain technologies which have investigated how to promote energy sharing among IoT devices to increase efficiency of energy utilization. Taking the Internet of Vehicles (IoVs) as an example, the electric vehicles have the ability to absorb excessive energy during the non-peak area and provide energy as distributed generators during the peak period. To enable secure energy trading, [8] proposes a localized P2P electricity trading framework, in which consortium blockchain is exploited to improve the security of transaction without relying on a third party. To improve the trading efficiency, [9] proposes a credit-based payment scheme, which supports the fast and frequent trading among energy nodes by establishing virtual credit banks. Besides, some digital currency has been presented for renewable trading based on blockchain, such as “Specoin” [10].

As shown in Fig. 1, to operate a blockchain enabled IoT system, the main steps are illustrated as follows: (i) All IoT devices operate on the same blockchain network; (ii) A IoT device generates a transaction for payment (or recording significant information), and broadcasts it to the network; (iii) The IoT devices receive the information and transactions in the network and validate them; (iv) All IoT devices perform hash algorithm to elect a winner whose candidate block will be broadcast and validated as a new block. (v) All IoT devices insert the identical copy of the new block into their local ledgers. (vi) The transaction stored in blockchain ledger triggers the smart contract[2] in IoT device. (vii) IoT device carries out a specific task, i.e., the movement of container

[2]Smart contract is only an option in this circle, which is an application on top of blockcahin, the IoT devices may use blockchain for many other applications without relying on smart contract.

in supply chain scenario, power supplying in smart energy scenario.

According to Fig. 1, we can see that consensus mechanism is the cornerstone in blochchain enabled IoT system, which builds a bridge between the raw data from infrastructure and the confirmed information for performing various applications. Therefore, the goal of this work is to clarify the challenges of consensus mechanism for blockchain enabled IoT systems. We illustrate the main idea of different types of consensus mechanisms and list their advantages and disadvantages in IoT ecosystem, then discuss some possible research directions of Direct Acyclic Graph (DAG) based consensus mechanisms.

The rest of this article is organized as follows. In Section II, we introduce the main idea of consensus mechanism, including Proof of Work (PoW), Proof of Stake (PoS) and DAG, and consider their practicability for IoT. In Section III, we review two existing DAG based consensus (Tangle and Hashgraph) and demonstrate their advantages in IoT through performance comparisons. In Section IV, we discuss some research directions of DAG based consensus. Conclusions are drawn in Section V.

II. Consensus Mechanism in Blockchain

In this section, we discuss different types of consensus mechanisms in blockchain, and consider whether the design criteria of corresponding consensus mechanism can meet the needs of IoT.

Consensus mechanism plays an indispensable role in blockchain to resolve the trust concern by answering the question "who will be the one has the right to insert the next block into blockchain". With consensus mechanism, the information can be announced orderly to all users without involvement of the third party. Nowadays, various consensus mechanisms have been proposed, PoW and PoS are the most widely used ones. However, the two consensus mechanisms based traditional blockchains face significant challenges when apply to IoT system. We introduce DAG based consensus mechanism as an effective solution.

A. *Blockchain* 1.0 : *Proof of Work*

PoW is proposed in the original blockchain application (e.g., Bitcoin). The core idea of PoW is the competition of computing power [1], the node performing the consensus mechanism (called miner) uses its computing resource for hashing operation to compete for the right to generate the new block with bonuses. The winner is the first one who obtains a hash value lower than the announced target. On the one hand, the computing difficulty in PoW must be high enough for preventing forking [3]. But on the other hand, the high computing difficulty would cause the deteriorated and meaningless energy consumption. Noted that the available resource of IoT devices is very limited. Therefore, PoW is not a good option for IoT system.

B. *Blockchain* 2.0 : *Proof of Stake*

Unlike PoW that relies on computing capability, coin age is used in PoS blockchain to avoid the high computational complexity of hash operation (e.g., Nxt[11]). The coin age of an unspent transaction output[3] is equal to its value multiplied by the time period after it was created. In PoS, a higher coin age will lead to a higher probability for the node to win the right of creating a new block, and in turn the coin age would be consumed (reset as zero) when the owner wins. Since winning probability is directly determined by coin age, PoS is beneficial for the wealthy miner, and might cause oligopolies or near-monopolies, then result in the generation of powerful third party. From this sense, the PoS consensus mechanism may not fit well to establish a smart distributed IoT systems.

C. *Limitations of PoW and PoS for IoT*

PoW and PoS are two typical traditional consensus mechanisms that work on a "single chain" (forking is illegal) architecture. To avoid forking and maintain a single version of blockchain ledger among all users, the consensus mechanism must slow down the access rate of new blocks. This might cause some significant bottlenecks in applying to IoT system. (i) *Resource consumption*: to slow down the access rate of new blocks and prevent blockchain network from attack, the traditional consensus process will consume much resource (i.e., computing power in PoW, coinage in PoS), which is too costly for the resource-limited IoT devices. (ii) *Transaction fee*: transaction fee is needed in traditional consensus mechanism to feed the miners, which might cause a heavy burden in the IoT system where most of tradings are micropayments. (iii) *Throughput limitation*: since the capacity of a new block is limited, Transaction Per Second (TPS) is limited to dozens usually (e.g., 7 TPS in Bitcoin and 20 to 30 TPS in Ethereum, which is unable to respond to the exponential growth of IoT devices. (iv) *Confirmation delay*: due to the low access rate of new blocks, the confirmation delay is too long for IoT applications (e.g., 60 minutes in Bitcoin and 3 minutes in Ethereum).

D. *BlockChain* 3.0 : *Direct Acyclic Graph*

DAG architecture and its consensus mechanism is proposed to overcome the shortcomings of traditional consensus for IoT. Some typical DAG consensus processes are shown in Fig. 2 and Fig. 3. DAG based consensus mechanism allows users to insert their blocks into the blockchain at any time, as long as they process the earlier transactions. In this way, many branches would be generated simultaneously, which is called as forking. This phenomenon is usually regarded as an issue in many traditional consensus process since it would cause "double-spending" [1]. However, DAG based consensus mechanism design innovative protocol and algorithm (detailed in next section) to address the double-spending problem, and allow any new arrival transactions access the blockchain network in a forking topology. As a result, the confirmation rate and TPS will not be limited anymore. Moreover, since the data stored in DAG is protected by massive forking blocks, the resource consumption can be very low for a user to

[3]The output of a transaction includes destination address and the amount of coin.

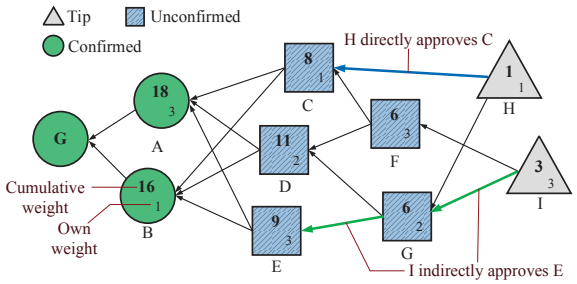

Fig. 2: An example of Tangle

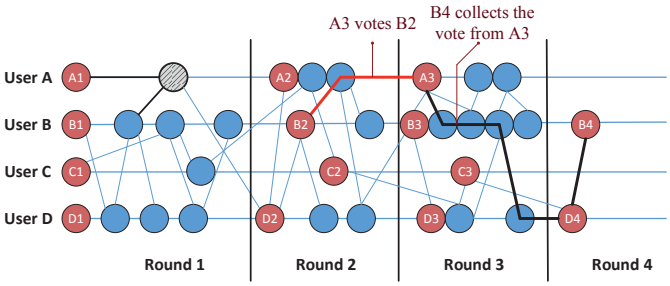

Fig. 3: An example of Hashgraph

create a new block. Accordingly, professional miner disappears and low or no transaction fee is possible, which is critically important to IoT ecosystem.

III. Typical DAG based Consensus

In this section, we introduce the consensus mechanism in Tangle and Hashgraph, respectively, which are the two typical DAG based consensus.

A. The Tangle

Tangle is the mathematical foundation of IOTA [12], a cryptocurrency for the IoT industry. As shown in Fig. 2, Tangle is a DAG based distributed ledger for recording transactions. It allows different branches to eventually merge into the chain, resulting in a much faster overall throughput. In Tangle, to access the ledger as a new vertex for storing a transaction, it has to approve a number of tips (typically two [12]). Thanks to this, the higher arrival rate of new transactions, the faster earlier transactions can be confirmed. On the other hand, since tips are the childless vertexes in Tangle, the new vertex selects tips and covers them could limit the branch to a reasonable scale. Moreover, since the workload to create a new vertex is light, all users can issue their transactions at any time without transaction fee, which is critical to the IoT application scenarios.

The consensus in the Tangle relates to cumulative weight. As shown in Fig. 2, the cumulative weight of a specific transaction is the sum of a vertex's own weight (proportional to the PoW that the issuing node invested into it [12]) and the overall weights of the vertices directly and indirectly approve it. Since the transactions stored in Tangle are secured by computing power, the cumulative weight of a transaction means its validity in the network and act as a decisive criteria to address double-spending problem.

In order to issue a new transaction and let the other users in the whole system accept it (i.e., win enough cumulative weight to reach an agreement for the consensus), the main procedures are listed as follows. (i) A user creates a unit as a vertex in the DAG graph to store its transaction. (ii) The user selects two tips with no-conflict according to a Markov Chain Monte Carlo (MCMC) algorithm [12], and adds the hash of the selected tips into its storage unit. (iii) The user finds a nonce to solve a cryptographic puzzle to meet the difficulty target. It is similar to PoW but with a very low difficulty-of-work, which can avoid spamming. (iv) The user uses its private key to sign the storage unit for security, and broadcasts it to others. (v) When the other users receive it, they should check whether it is legal or not based on the digital signature and PoW based nonce. Successfully checked new storage unit would be added as a new tip in the Tangle, and waits for confirmation through direct approval and indirect approval till its cumulative weight reaches the predefined threshold.

In a public ledger, building forking (or branch) and redoing the work is the only way to tamper with data and conduct double-spending. To address this problem, the single chain based consensus mechanism (e.g., PoW) use the longest chain as the criterion. To this end, to guarantee and maximize the own profit, a rational user should choose the longest chain to work when forking occurs. The reason is that the longest chain has the lowest probability to be orphaned. Similarly, the Tangle uses the MCMC tip selection algorithm to select the branch with the largest overall cumulative weight. Moreover, with the assistance of distributed and parallel approval in Tangle, the overall computing capability of honest users in large scale IoT system could be powerful to prevent double-spending, where the branch generated by an attacker is hard to outweigh the honest one. Meanwhile, any single user does not need to consume much power on computing for security.

B. Hashgraph

Hashgraph [13] is proposed for replicated state machines with guarantee of Byzantine fault tolerance, it is asynchrony, decentralization, no PoW, eventual consensus with probability one, and high speed in the consensus process. Gossip protocol and virtual voting are two key elements in Hashgraph. Using gossip protocol, every transaction will be known by all users. After that, the agreement of the order of transactions will be reached through virtual voting algorithm. In order to get a better understanding of Hashgraph, we will briefly introduce how gossip protocol and virtual voting run.

According to gossip protocol, in a fixed interval, each user in Hashgraph should randomly choose another one to announce all the transactions it knows. For example, the shadow unit in Fig. 3 represents user B sends some information to user A that A does not know, so A creates the event which links A and B to store the unknown information. In this way, every event will be known by all participants eventually. Note that gossip protocol is a low-cost method, the overhead to exchange a storage unit is very small, which includes

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)

positional information (3 to 6 bytes), signature (64 bytes) and transactions within the unit (about 100 bytes).

To achieve the consensus, the system needs to select the "famous witnesses" through virtual voting (all users perform the voting algorithm based on the graph connectivity). The famous witnesses are elected from witnesses which are the first events in each round (the red units in Fig. 3). An electing process includes voting and checking. As shown in Fig. 3, the witnesses in round 3 vote for the witnesses in round 2. Then, the witnesses in round 4 will collect the votes in round 3. If the voting in round 3 and checking in round 4 succeed, the witnesses in round 2 would become famous. The events in round 1 voted by the famous witnesses in round 2 will be confirmed. The creation time of the confirmed events will be accepted by all users, which acts as a proof to prevent double-spending.

C. Comparisons

To demonstrate the advantages and limitations of DAG based consensus for IoT, we compare its performance with two mainstream consensus mechanism in Table I.

These comparisons reflect that DAG based consensus mechanisms are more suitable for large-scale IoT than PoW and PoS. Specifically, DAG based consensus has the lower transaction fee, resource consumption, and it can achieve a much higher transaction throughput. However, some limitations are still remained in DAG based consensus mechanisms, e.g., centralization concern in Tangle. Moreover, the confirmation delay of DAG consensus would be affected by traffic load significantly, especially when the traffic load in practical IoT scenario changes over time. Hence, to apply DAG based consensus, the mentioned issues but not limited on these should be addressed.

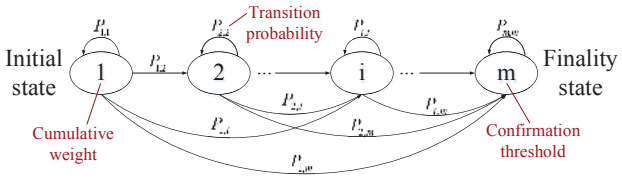

Fig. 4: Markov chain model for the consensus process of a new transaction

IV. Challenges of DAG based Consensus

Although DAG based consensus mechanism has many advantages, as an emerging technology, it is still far from perfect to be widely used in IoT systems. Some main issues of DAG based consensus are open to be explored.

A. Analysis Model

Design a generalized theoretical mathematical model is important to analyze the performance of DAG based consensus machanism. In [12], the authors analyze the speed of the cumulative weight typically grow in the stationary high load regime, it provides some qualitative and quantitative insights into the consensus process of the Tangle. In [14], the authors prove the existence of ("almost symmetric") Nash equilibria in a DAG-valued stochastic process where a part of players try to optimize their strategies.

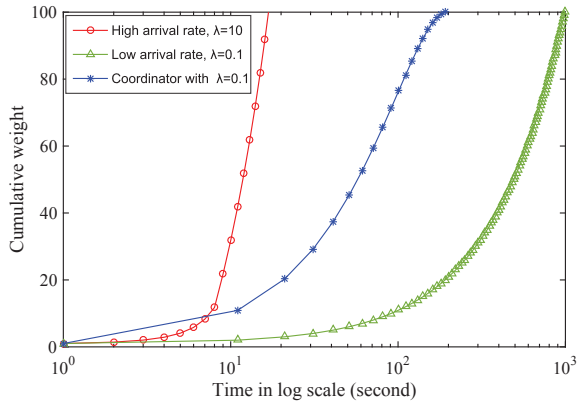

Fig. 5: Cumulative weight growth curve in different regimes

Considering the features of consensus process, we believe that an analytical model using Markov chain is a promising approach. The formulation of an Markov chain model for the consensus process of a new transaction is shown in Fig. 4. The model uses the cumulative weight introduced in Tangle as the confirmation criterion. Accordingly, we can analyze the N-step transition probability from the current state to the finality state. As a result, the increasing rate of cumulative weight, TPS and confirmation delay can be analyzed in a theoretical approach.

One of the most significant and remaining problem of the Markov Chain based model is how to capture the transition probabilities matrix, especially in the large network scale with the huge number of system states. Moreover, the transition probability is also strongly affected by the design criteria of consensus mechanism, e.g., they are totally different between Tangle and Hashgraph. Therefore, the Markov Chain based model needs to be optimized in the future work.

B. The Low Bound Limitation

As we mentioned before, there is no technical up bound of throughput in DAG based consensus process. However, in practical IoT scenario, it is impossible that the new transaction arrives quickly and steadily all the time. Taking bicycle-sharing application as an example, there are very few transactions at night. In this case, the confirmation delay could be quite large.

In order to show the impact of arrival rate (defined as λ) on the consensus process, we conduct a simple simulation based on the Markov chain model in section A. In Fig. 5, we can see clearly that when the arrival rate of new transaction is low, the cumulative weight would increase slowly. Since the confirmation of a transaction is determined by its cumulative weight [12], as a result, the confirmation delay would be very large when the arrival rate is low.

To this end, coordinator is involved in DAG based consensus process to improve confirmation rate in low trading traffic load regime. The coordinator is an entity controlled by a third party, which issues zero-value transactions to process unconfirmed transactions. In Fig. 5, we can see that with the assistance of coordinator, the cumulative weight increases more quickly in the low arrival rate situation. On the one hand, this solution could resolve the large confirmation delay issues in the low arrival rate situation. On the other hand, centralization problem might be incurred, since the coordinator is a third party, which disobeys the basic rule of blockchain. Due to this, coordinator can only be used in private or closed situations, i.e., consortium blockchain.

C. Mobile Blockchain

It is nature to assume that typical IoT devices are wireless connected. In many researches on consensus process (i.e., Tangle and Hashgraph), communications are assumed wired or perfect. However, due to the wireless channel fluctuation, the communication might be a bottleneck for the blockchain enabled IoT systems. We discuss the challenges related to communication in blockchain enabled IoT systems from different layers.

1) Lower layer: In physical layer, some fundamental metrics such as signal-to-interference-plus-noise ratio (SINR) and communication throughput should be analyzed to show how the wireless communication quality affect/constrain the blockchain-enabled IoT system deployment (e.g., node distribution), protocols (e.g., size of block, frequency of transactions) and confirmation delay, etc. On the other hand, given a transaction throughout bound in blockchain (e.g., one block in every 10 minutes as defined in Bitcoin [1]), it is valuable to know how to deploy the IoT devices that can optimally meet this bound. Another challenge comes from the fact that IoT devices might be massively connection, which has been identified as one of the main features for fifth-generation (5G) wireless communication. The trade-off between the system overhead and security performance will be an interesting topic to be explored. In addition, physical links and access control protocol will influence the communication performance in terms of throughput and latency, which might be two factors that may pose extra bottleneck to the consensus process. Finally, joint wireless and consensus mechanism design to maximize the overall security level is of interest from the system level.

2) Upper layer: In route layer, considering the memory space and processing capacity of IoT devices are normally constrained, the deteriorated delay in bottleneck would affect the consensus process (i.e., the congested IoT device might be regarded as the a "lazy" node erroneously [12]). Therefore, an efficient routing protocol in blockchain enabled IoT system should prefer the resourceful IoT devices to propagate transactions. Meanwhile, in Transmission Control Protocol (TCP) layer, a protocol should be designed to meet the specific QoS needs of blockchain network. Especially, when a transaction failure occurs, the protocol should identify the exact reason. If the transaction failure is caused by transmission error or timeout rather than consensus mechanism, the retransmission should be performed by the protocol for correction and recovery.

D. Blockchain Strategy Optimization

In DAG based consensus mechanism, every participant is also an approver to store and update the ledger in a

distributed manner. Since most IoT devices are limited for power and memory, the energy saving and caching strategy should be well designed to lighten and balance the workload of each user. For instance, a resource optimization strategy, which allows resource-limited IoT devices to issue transactions only, resourceful IoT devices to process the transactions and generate blockchain, can be developed. Meanwhile, due to the selfishness and rationality, some incentive mechanisms should be performed to motivate the suitable IoT devices to participate into consensus process. In order to let IoT devices make the optimal strategy in a distributed manner, game theory is a nature selection. For example, in [15], the authors propose an auction based approach for PoW offloading in mobile blockchain.

V. Conclusions

In this article, we have introduced the concept of blockchain and the benefits of using it into the IoT systems. We start from illustrate the main ideas of consensus mechanism including PoW, PoS and DAG, and discuss their advantages and limitations for IoT. Two DAG based consensus mechanisms, i.e., Tangle and Hashgraph are introduced. We also compare the main characteristics of PoW, PoS, and DAG. Furthermore, we present a visible simulation results to show the impact of transaction arrival rate on consensus process in DAG based blockchain, and reveal its low bound limitation. Challenges for the DAG based consensus mechanism to use in the IoT system are summarized from analysis model, major drawback, mobile blockchain and optimization strategy.

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.i-scoop.eu/blockchain-distributed-ledger-technology/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/academic-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 blockchain," 2017. [Online]. Available: https://arxiv.org/pdf/1710.01567.pdf.