Towards A Scalable DAG-based Distributed Ledger for Smart Communities

Caixiang Fan, Hamzeh Khazaei, Yuxiang Chen and Petr Musilek

***Abstract*—In recent years, Distributed Ledger Technology (DLT) has been playing a more and more important role in building trust and security for Internet of Things (IoT). However, the unacceptable performance of the current mainstream DLT systems such as Bitcoin can hardly meet the efficiency and scalability requirements of IoT. In this paper, we propose a scalable transactive smart homes infrastructure by leveraging a Directed Acyclic Graph (DAG) based DLT and following the separation of concerns (SOC) design principle. Based on the proposed solution, an experiment with 40 Home Nodes is conducted to prove the concepts. From the results, we find that our solution provides a high transaction speed and scalability, as well as good performance on security and micropayment which are important in IoT settings. Then, we conduct an analysis and discuss how the new system breaks out the well-known Trilemma, which claims that it is hard for a DLT platform to simultaneously reach decentralization, scalability and security. Finally, we conclude that the proposed DAG-based distributed ledger is an effective solution for building an IoT infrastructure for smart communities.**

***Index Terms*—Internet of Things, Smart Home, Smart Community, Blockchain, Distributed Leger, DAG, Energy Transaction.**

I. Introduction

INTERNET of Things is experiencing an exponential increase in terms of the connected devices. This is due to the ubiquitous connectivity, billions of IP addresses with IPv6 and rapid development of 5G. According to Gartner report, the number of connected devices is expected to be over 25 billion by 2020 [1]. However, this tremendous market growth raises new challenges such as security and privacy [2], scalability and data processing performance for IoT system architecture, which means that an effective solution needs to be devised.

A. Distributed Ledger Technology in IoT

Basically, there are two main types of DLTs according to different data structures for the ledger, which are Block based Blockchain (BC) and Blockless DAG based DLT (e.g. IOTA Tangle). BC is a distributed ledger for storing and sharing data across all nodes in a network. Based on different usage contexts, various types of data including transaction record data (e.g. Bitcoin), contract and even personal healthcare information can be stored in a BC system. This emerging technology has drawn increased academic and industrial attention due to its attractive features including immutability, scalability and decentralization. According to a recent survey [3], there are about 42 industries (e.g. law enforcement, ride hailing and stock trading) that could be transformed by BC in the future. And this number keeps increasing, especially at the early stage of BC application innovation. Clearly, BC technology is potentially an effective solution to overcome the challenges in IoT [2].

Although BC has the potential to tackle the IoT problems such as security and privacy [4], its application to build an IoT architecture remains difficult. Firstly, the application of BC in non-monetary IoT systems is not as straightforward as in electronic currency system such as Bitcoin [5]. In addition, there are many different types of DTLs, but no standards that would help identify the best one for IoT so far. For example, as for the participation permission, there are public, permissioned public/private and consortium networks; for transaction model, there are tokenized UTXO and non-tokenized account-based transactions [6]. Here, from the perspective of consensus, we list 5 types of main consensus mechanisms [7]:

- PoW (Proof of Work),
- PoS (Proof of Stake),
- DPoS (Delegated Proof of Stake),
- PBFT (Practical Byzantine Fault Tolerance), and
- Transaction References in DAG (Directed Acyclic Graph).

For BC based DLTs, the consensus mechanisms have many inherent disadvantages for IoT applications such as smart homes and communities. On one hand, the PoX consensuses are computationally expensive. According to the latest Bitcoin Energy Consumption Index, Bitcoin miners from all over the world consume over 70TWh of electricity every year to do the proof of work [8]. This is obviously not suitable for IoT scenarios with limited and light-weighted computation. On the other hand, the processed transactions per second (TPS) of the mainstream BC platforms like Bitcoin and Ethereum are very limited, because the single chain of blocks is linear and blocks cannot be created simultaneously. For example, one Bitcoin block takes 10 minutes to be created and added to the main chain, which is very inefficient and fails to meet the requirement of instant transaction in IoT.

With DAG, transactions can be directly attached to a chain without waiting to be wrapped into a block in advance. More-

C. Fan, H. Khazaei and P. Musilek are with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta, e-mail: {caixiang, hamzeh.khazaei, petr.musilek}@ualberta.ca.

Y. Chen is with the Department of Civil and Environmental Engineering, University of Alberta, Edmonton, Alberta, e-mail: yuxiang.chen@ualberta.ca.

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

over, all new added transactions can be simultaneously run on different chains, which interwoven to form a network called Tangle. Theoretically, the Tangle should be more efficient than traditional BC under the well-designed consensus mechanisms.

B. Benefits and Contributions

In this paper, we argue that the DAG-based DL is an effective solution for designing a transactive smart homes architecture. The specific IOTA [1] Tangle technology will be used to design our solution and conduct the experiments. In contrast to other IoT infrastructure proposals, our approach brings the following advantages to IoT architecture design:

- **Scalability:** In a local community, the permissioned private network has a high scalability due to the decentralized DAG-based design and no transaction rate limit.
- **Transaction speed:** The high transaction speed benefits from the DAG data structure and the efficient consensus mechanism. Transactions can be added to different chains in a Tangle simultaneously, which can speed up the transaction rate. For the largest TPS, an IOTA stress test held in April 2017 showed that the network had transaction processing capabilities of 112 Confirmed Transactions per Second (CTPS) and 895 TPS within a small test network consisting of 250 nodes [9].
- **Security and privacy:** Our solution adopts IOTA Tangle which originally uses the hash function called Curl-p [10], then switches to the Keccak (SHA-3) for cryptographic signing. As for the 34% attack, we leverage the Membership Service Providers (MSP) from Hyperleger [11] as the authority management to set up a trustable environment, combined with the coordinators implementation to protect the ledger from 34% attack. Here, 34% attack refers to an attack such as double-spending by a group of participants controlling more than 33% of the network's computing power. Additionally, the private Tangle ensures all data are encrypted and stored in the locally running Home Nodes.
- **No transaction fees:** Tangle gets rid of "mining" using the following mechanism: before issuing a transaction, the node must confirm two previous transactions and do a very light-weighted proof of work. This means that all participants need to contribute their computation power to maintain the network to eliminate the transaction fees.
- **Micro-transaction:** Unlike Bitcoin with a threshold on the minimum amount of a payment, people can send as little as 1 IOTA in our solution, which is worth $0.572701 (as of September 10, 2018) and will always be available for sending without fee. This makes the M2M P2P micro-transaction possible for smart homes, such as in the case of energy transaction among neighbors in a local community.
- **Decentralization:** IOTA Tangle eliminates the notion of miners. Every network participant only has access to limited computational resources. And anyone who wants to launch a transaction on the tangle needs to actively participate in the consensus. This makes our solution decentralized.

This paper contributes to the design of a new scalable IoT architecture for smart homes and communities using DAG-based DLT. Our approach differs from other solutions in the way that it applies a lightweight, scalable and high performance Tangle technology which is suitable for IoT. To the best of our knowledge, this is the first research work that leverages DAG-based DLT to build a transactive smart homes infrastructure.

II. Related Work

A systematic literature review on the BC for the IoT was conducted in [12]. The survey explored whether the BC can be employed to foster a decentralized and private IoT by investigating factors that affect integrity, anonymity and adaptability of this technology. Similar to this survey, another work [13] took a deep look into how IoT and BC (especially smart contract) can be used together. The authors concluded that the combination of BC and IoT is powerful and can lead to significant changes across several industries, creating opportunities for new business models and novel, decentralized applications [13]. Motivated by the positive conclusion, Novo proposed an IoT architecture for scalable access management in [14]. The decentralized access control system stored access control information using BC, which was developed to run as a single smart contract that defines the policy rules of the management system. However, unlike our solution, the previously mentioned systems had the limitations of transaction fees and processing speed from the inherited BC technologies [14].

In [2], the authors proposed a BC-based smart home architecture with a hierarchical structure consisting of three components: smart home, overlay network, and cloud storage. More specifically, [15] delved deeper and described the key components of smart home tier, in which an always online device played a role of miner to handle all transactions coming to or out of the smart home. This design provided an effective solution to overcome IoT security and privacy challenges by leveraging a new proposed BC called LSB (Lightweight Scalable Blockchain) [16], which adopted an IoT friendly consensus mechanism that eliminates the proof of work and incorporates a distributed trust method. In our solution, we share some features with the LSB such as no transaction fees, lightweight consensus mechanism and self-scaling. However, LSB employs the traditional BC which needs to wrap transactions into a block and wait for mining.

K. Yeow et al. [6] conducted a comprehensive review on decentralized consensus systems for IoT in terms of the data structure, consensus mechanism, and transaction models. From their proposed thematic taxonomy, a synthesized comparison between BC-based systems (e.g. Bitcoin and Ethereum) and DAG-based distributed ledgers (e.g. IOTA and Byteball) was conducted. By analyzing and summarizing the pros and cons, the authors found that the DAG outperformed on scalability,

[1] https://www.iota.org/

transaction confirmation speed and decentralization. They concluded that DAG might be an answer to overcome the challenges of the fast scaling IoT with the need for low latency micro-payments in the M2M P2P decentralized infrastructure [6]. As an example, a new DLT-based charging and billing IoT architecture for electric autonomous vehicles (EAVs) was proposed in [17]. The authors leveraged IOTA based payment system through M2M communication (MQTT) to carry out micro-transactions for charging and billing in EAVs. In another research project, the authors utilized IOTA Tangle to present a streaming data payment protocol (SDPP) which was an application-layer protocol for enabling micropayments among IoT transactions [18].

Motivated by these innovative applications, we propose a DAG-based IoT architecture for transactive smart homes leveraging IOTA Tangle.

III. DAG Based Network for Smart Homes

Like the CAP Theorem in distributed system design [19], there is a well-known Blockchin Trilemma in designing distributed ledger systems. According to Buterin [20], the founder of Ethereum, a BC platform can only fundamentally achieve 2 out of the following 3 traits at one time:

- **Decentralization** (a system running with each participant node only having access to limited computational resources including computation, bandwidth and storage);
- **Scalability** (the systems efficiency of processing transactions is higher than any single node);
- **Security** (Can handle all attacks from any entity with less computational resources than the system itself).

However, we argue that this trilemma can be addressed in our case by leveraging the architectural design principle of separation of concerns (SOC). Specifically, we achieve decentralization and scalability by using the IOTA consensus, and utilize a decentralized coordinators design with permission management to meet the security requirement. We describe the proposed solution in terms of architecture, consensus mechanism, coordinators and permission management.

A. Architecture

Figure 1 illustrates a fundamental high-level picture of the proposed architecture. There are three main parts including smart homes, the Tangle of inter-house transactions (TXs), and smart devices in the homes. In each smart home, there is an always online computation device called Home Node with pre-installed firmware and corresponding tangle reference implementation. Every Home Node is connected to its neighbor nodes with TCP/UDP protocols for communication and synchronizing the distributed ledger. In practice, this Home Node can be any kind of IoT device or specialized chip, that can provide the computational power, such as a server, VPS, PC or even microcomputers like RaspberryPi. All Home Nodes in a community provide the computational power to maintain and secure the distributed ledger network.

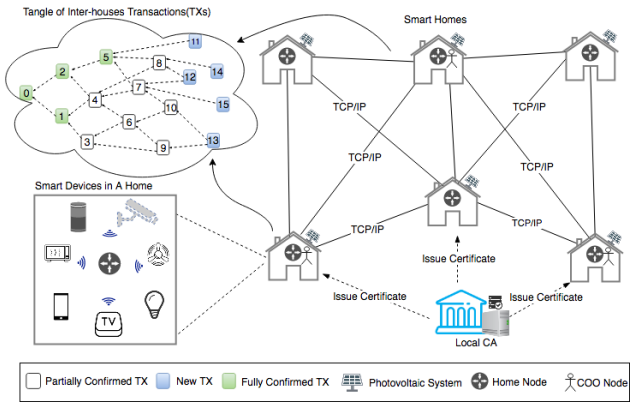

Fig. 1. DAG-based Smart Homes Architecture

When this system is used in the case of energy transaction, we assume that there is a microgrid as the infrastructure behind the Home Nodes network. The microgrid connects all photovoltaic systems and other distributed energy resources (DERs) installed at smart homes. Our proposed solution provides the microgid with a payment system to carry out DERs inter-house transactions in a decentralized, efficient and secure way without any transaction fees in a local smart community. In fact, the Tangle with DAG data structure can act as a data management system to transfer, store and even query both inter-house and intra-house data. For example, it can be used to send, receive and store the command message to remotely control smart devices in a smart home. However, in this paper, we just focus on the scenario of inter-house transaction data including sending, receiving and confirmation transactions.

B. Consensus Mechanism

In a payment system, there is always a mechanism called consensus which identifies when a transaction can be securely considered confirmed and added to the ledger. For the consensus mechanism of our solution, we follow the IOTA reference implementation and employ IOTA tangle to handle all transactions. IOTA is an open-source distributed ledger system across an asynchronous network. In this system, a new transaction must select two previous unapproved transactions (called tips) to approve according to a tip selection algorithm before adding to the Tangle. Basically, there are two solutions to reach consensus on confirmation in the tangle: the distributed Markov Chain Monte Carlo (MCMC) [10] approach and currently implemented coordinator (COO) [21].

The MCMC approach provides a probabilistic solution, similar to Bitcoin and other distributed ledgers. In this consensus algorithm, a particular transaction gets a confirmation confidence indicating its acceptance level at any given time by the following rules:

1) Use the MCMC method to select 100 new transactions (tips).
2) Calculate how many tips will directly or indirectly reach the transaction.
   -if it is less than 50%, the transaction is not yet

validated (not confirmed).
-if it is more than 50%, the transaction has a fair chance to be validated (partially confirmed).
-if it is 99% or 100%, the transaction is considered validated (fully confirmed).

In Figure 1, green boxes are fully confirmed transactions, which indicates that they are validated by all of current tips, while the white boxes are only partially confirmed. The blue boxes represent tips without any validation. In current public IOTA project, the coordinator is an entity controlled by the IOTA Foundation, which generates a zero-valued transaction, called a milestone, every minute. Under the coordinator consensus, only transaction referenced by a milestone can become confirmed, while the others cannot.

C. Coordinators

As the IOTA Foundation explains, the Tangle network has a small number of nodes at its infancy stage so that an attacker can easily create a lot of nodes and thus creating many malicious transactions. According to the MCMC algorithm, there is a relatively large chance that these malicious transactions are selected to be confirmed. To protect the infancy Tangle from 34% attack, a protection mechanism called the coordinator (COO) is employed. This does not mean it is centralized because the COO node follows all the consensus rules just like any other node. The only activity performed by COO node is continuous generation of trustable transactions which contain zero values, to help secure the infancy Tangle network.

In our solution, we modify the COO mechanism to be a cluster of randomly chosen COO nodes which are the normal Home Nodes equipped with the ability of issuing milestones, as shown in Figure 1. Therefore, if any COO node crashes, others can continue to take the responsibility and create milestones to confirm the transactions. This decentralized design not only removes the single point of failure from the system, but also reduce the risk of centralization.

D. Permission Management

To build the trust for all network participants, a hybrid security solution combining the permission management system and proof of work is employed before the number of nodes is large enough. Motivated by Membership Service Providers (MSP) solution in Hyperledger [11], we propose a similar local certificate authority (CA) using X.509 certificates as the permission management system. In a local community, each Home Node needs to get certification issued by the local CA to join the network, as shown in Figure 1.

To summarize, we propose a payment solution for smart homes peer-to-peer local energy transactions. Specifically, we leverage the DAG-based distributed ledger technology to build a permissioned, private and secure transaction network. In the next section, we evaluate and analyze some important metrics such as transaction speed and scalability of our proposed solution.

IV. Evaluation and Analysis

In this section, we will describe our experiments and results, and evaluate our proposed solution in terms of the transaction speed and scalability. Then, we conduct a general analysis and discussion based on the test results, providing some important insights about the DAG-based DL network application in IoT.

A. Experiments and Results

We employ IOTA Implementation Reference (IRI 1.5.3) and a coordinator simulation tool to deploy a private IOTA network on the SAVI OpenStack cloud platform [2]. In total, 40 nodes with the flavor of medium size virtual machines (4GB RAM, 2 VCPU and 40.0GB Disk) are used to build a network. We choose the medium size rather than high performance nodes because this is more likely to fit the IoT scenarios with a low Hashpower. In fact, more powerful nodes will improve the performance by reducing the time of proof of work and thus increasing the transaction speed. In practice, these nodes represent the Home Nodes installed in the smart homes.

In order to explore the metrics of transaction speed and scalability, we design a load testing method that consists of sending and receiving parts. For sending component, we set each sending node or sender to intensively send transactions in every short time interval such as 1 second or 2 seconds depending on the difficulty of proof of work called Minimum Weight Magnitude (MWM). All these transactions will be broadcast to all nodes through TCP/UDP. We control the transaction sending rate by controlling the number of senders during a test time window. For receiving component, we leverage zero message queue (ZMQ) to listen to the specified port on a Home Node and receive transaction data by subscribing *tx* and *sn*, which indicate all received transactions and new confirmed transactions, respectively.

We test the transaction speed of both TPS and CTPS under different network node scales (10, 20, 30, 40) with different MWM configurations, as shown in Figure 2, 3, 4 and 5, where TPS refers to the number of received transactions per second and CTPS refers to the number of confirmed transactions per second in the tangle. Three coordinators are randomly selected and set to generate milestones every minute.

In order to explore if different node scales influence the transaction speed, we use the same 10 senders with 3 COOs to test the TPS/CTPS under 10, 20, 30 and 40 nodes networks, respectively. The result is shown in Figure 6.

In current implementation, COOs play a critical role for confirming transactions. Therefore, we conduct an experiment to test the effect of different numbers of COOs on transaction speed by changing the number of senders under 40 nodes network and keeping MWM=9. The result is shown in Figure 7.

[2]https://www.savinetwork.ca/

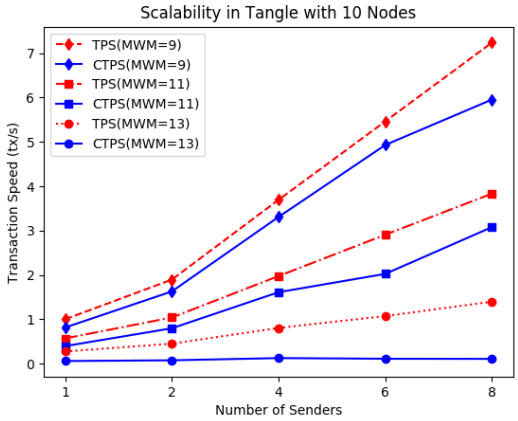

Fig. 2. Scalability in 10 Nodes Network

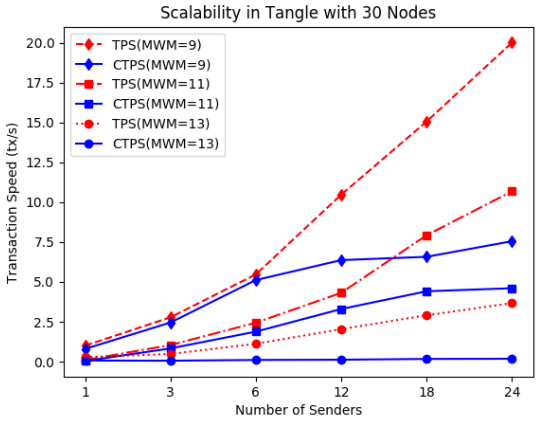

Fig. 4. Scalability in 30 Nodes Network

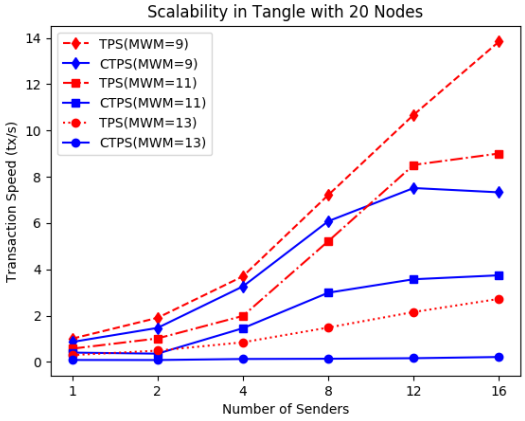

Fig. 3. Scalability in 20 Nodes Network

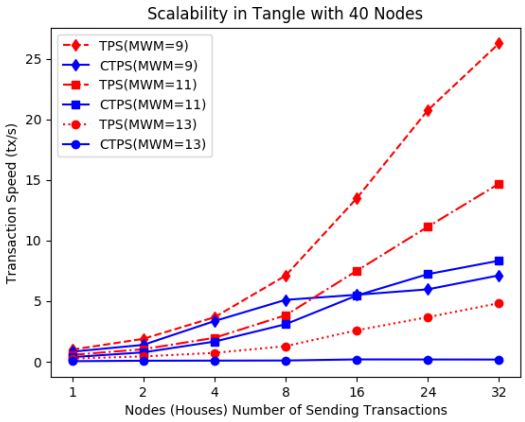

Fig. 5. Scalability in 40 Nodes Network

B. Analysis and Discussion

In this part, we analyze and discuss our proposed solution from the system throughput, scalability, decentralization and security perspectives by combining with the testing data.

Throughput: from the load test results, our solution provides a relatively good efficiency of processing transactions, as shown in Table I. Even in the situation of only one sender, the average TPS and CTPS can reach 1 tx/s and 0.83 tx/s, respectively, as shown in Figure 5. We argue that this is acceptable for the inter-house energy transaction in a local community.

From Figure 6, many flat lines tell that the nodes scale of network has almost no influence on the transaction speed. From Figure 7, we find that the CTPS has a peak value at a proper level of COOs number, e.g. CTPS reaches around 7.5 tx/s under 24 senders and 6 COOs. According to the consensus of currently implemented IOTA version, a transaction must refer to two tips and it can be considered confirmed when any milestone directly or indirectly reaches it. If not enough milestones are created, some transactions may not get any references to be confirmed. If too many are created, it may lead to a lower transaction generation rate in a closed network because of the Hashpower competition. Therefore, there should be a balance between the number of COOs and the number of unconfirmed transactions in the Tangle at one time.

TABLE I
BASIC PERFORMANCE STATISTICS IN 40 NODES NETWORK

Performance Values Under Various MWMs			
Items	MWM=9	MWM=11	MWM=13
Send Interval(s)	1	2	4
Max TPS(tx/s)	26.26	14.69	4.84
Max CTPS(tx/s)	7.13	8.34	0.19
Min TPS(tx/s)	1.00	0.57	0.30
Min CTPS(tx/s)	0.83	0.38	0.05

Scalability: from the TPS/CTPS results under different networks (Figure 2, 3, 4 and 5), it is obvious that as the number of senders increases, the transaction speed of both TPS and CTPS almost increases linearly. This indicates that transaction speed has a good linear scalability against the number of senders.

Decentralization: in our proposed solution, each Home Node only has access to limited computational resources. The decentralized coordinators are randomly selected from the

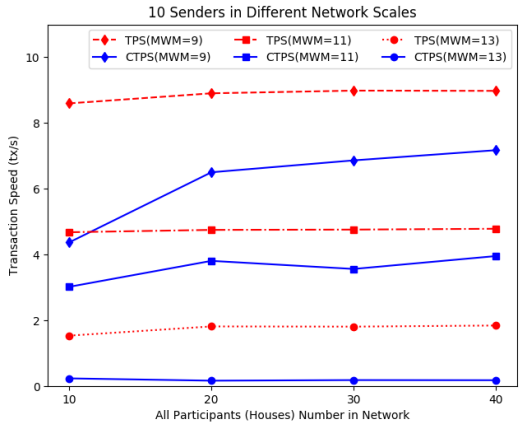

Fig. 6. Scalability in Different Configurations

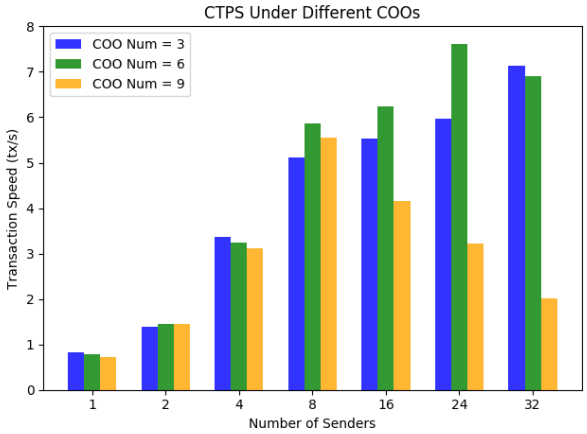

Fig. 7. Transaction Speed Under Different COOs

network participants and independently confirm transactions. There are no central nodes and middle man roles in transaction processing.

Security: IOTA consensus provides the protection for double spending attacks. From system design perspective, on one hand, the permission management system sets a trustable and private environment for transactions like the first wall. On the other hand, all the Home Nodes with changeable PoW difficulties will build a Hashpower wall (the second wall), which combines with the decentralized COOs to protect the system from 34% attack.

V. Conclusion and Future Work

In this work, we have proposed a DAG-based distributed ledger solution for IoT. Specifically, we introduce our solution in the context of smart homes for handling inter-house DERs transactions. With the initial experimental results, our solution provides high TPS/CTPS and good scalability which is suitable for IoT applications. We conclude that our proposed DAG-based distributed ledger is an effective solution for building a smart home IoT infrastructure. Further studies will be conducted on the decentralization optimization, security verification and containerization.

For the further study, we expect to optimize the system by removing COOs and only employing MCMC for consensus to achieve better decentralization. Next, we would like to explore the average transaction confirmation time which denotes the transaction time latency. More work on the comparisons with other IoT-oriented DL consensuses should also be conducted. Moreover, it is also interesting for us to conduct the research on performance evaluation such as analytical modeling and simulation for DAG-based DL systems.

Acknowledgment

This research was supported by the Natural Sciences and Engineering Council of Canada (NSERC), and its Strategic Network for Smart Applications on Virtual Infrastructure (SAVI). Also we would like to thank Cybera, Albertas not-for-profit technology accelerator, who supports this research through its Rapid Access Cloud services.

References

[1] P. B. Pureswaran and V., "Device democracy: Saving the future of the Internet of Things," tech. rep., IBM Institute for Business Value, New York, NY, USA, 2014.
[2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," in *Proc. Second Int. Conf. Internet-of-Things Des. Implement. - IoTDI '17*, pp. 173–178, 2017.
[3] CBinsights, "Banking Is Only The Beginning: 42 Big Industries Blockchain Could Transform," tech. rep., CBinsights, 2018.
[4] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes - Past, present, and future," *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 42, no. 6, pp. 1190–1203, 2012.
[5] S. Kornmesser, "Bitcoin: A Peer-to-Peer Electronic Cash System," *J. Gen. Philos. Sci.*, vol. 39, no. 1, pp. 53–67, 2008.
[6] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2017.
[7] C. G., "5 Types of Blockchain Consensus Mechanisms," 2018.
[8] Digiconomist, "Bitcoin Energy Consumption Index," 2018.
[9] Y. Yuan and H. Zhiwei, "DAG Technology Analysis and Measurement," 2018.
[10] S. Popov, "The Tangle," *New Yorker*, 2018.
[11] Hyperledger, "Membership Service Providers (MSP)," 2017.
[12] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, pp. 1–6, 2017.
[13] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[14] O. Novo, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," *IEEE Internet Things J.*, vol. 14, no. 8, pp. 1–12, 2018.
[15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work.*, pp. 618–623, 2017.
[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy," dec 2017.
[17] D. Strugar, R. Hussain, M. Mazzara, V. Rivera, J. Lee, and R. Mustafin, "On M2M Micropayments : A Case Study of Electric Autonomous Vehicles," 2018.
[18] R. Radhakrishnan and B. Krishnamachari, "Streaming Data Payment Protocol (SDPP) for the Internet of Things," 2018.
[19] H. Khazaei, M. Fokaefs, S. Zareian, Nasim Beigi-Mohammadi, Brian Ramprasad, M. Shtern, P. Gaikwad, and M. Litoiu, "How do I choose the right NoSQL solution? A comprehensive theoretical and experimental survey," *Big Data Inf. Anal.*, vol. 2, no. 1, 2016.
[20] G. Hummer, "On sharding blockchains," 2017.
[21] IOTA Foundation, "Consensus on the Tangle," 2018.