Postprint of Research on Local Directed Acyclic Graph Blockchain in Wireless Internet of Things

Authors: Yang Changlin, Wang Jiguang, Wangqing

Date: 2022-05-10T11:22:57+00:00

Abstract

To reduce data storage requirements and transmission overhead in wireless Internet of Things (IoT), a local directed acyclic graph blockchain scheme (LDB) based on directed acyclic graph (DAG) is proposed. This scheme addresses node storage constraints and transmission overhead by enabling wireless IoT nodes to store only their own data blocks and the block hash values of neighboring nodes, reduces the data verification process while ensuring data security, and enhances overall network utilization. Additionally, a malicious node detection mechanism is proposed to effectively identify malicious nodes within the network. In simulation experiments, by comparing with IOTA across different network models, the storage requirements, transmission overhead, and link load of LDB and IOTA are evaluated. Experimental results demonstrate that at a network scale of 500 nodes, LDB reduces node storage space by 99.8%, decreases average transmission overhead by 66.2%, and reduces maximum load by approximately 28-fold compared to IOTA.

Full Text

Preamble

Local Directed Acyclic Graph Blockchain in Wireless Internet of Things

Yang Changlin[1],[2]†, Wang Jiguang[1], Wang Qing[3]
(1. School of Computer Science, Zhongyuan University of Technology, Zhengzhou 451191, China;
2. School of Software Engineering, Sun Yat-Sen University, Zhuhai, Guangdong 519082, China;
3. School of Electrical & Information Engineering, Tianjin University, Tianjin 300072, China)

Abstract: To reduce data storage requirements and transmission overhead in wireless Internet of Things (WIoT), this paper proposes a local directed acyclic graph blockchain scheme (LDB) based on DAG. The scheme addresses node storage limitations and transmission consumption by enabling WIoT nodes to store only their own data blocks and hash values of neighboring nodes' blocks, thereby reducing data verification processes while ensuring data security and improving overall network utilization. Additionally, a malicious node detection mechanism is proposed to effectively identify malicious nodes in the network. Through simulation experiments comparing LDB with IOTA across different network models, we evaluate storage requirements, transmission consumption, and link load. Experimental results demonstrate that with a network of 500 nodes, LDB reduces node storage space by 99.8%, average transmission consumption by 66.2%, and maximum link load by approximately 28 times compared to IOTA.

Keywords: local directed acyclic graph blockchain; wireless Internet of Things; data integrity

0 Introduction

The Internet of Things (IoT) encompasses all things connected to the Internet [1]. With continuous upgrades of IoT devices and advancements in wireless communication technologies, wireless IoT (WIoT) has found widespread applications in healthcare, energy, automotive, environmental protection, and transportation [2]. According to Juniper Research, globally connected WIoT devices will grow from 38.5 billion in 2020 to 50 billion in 2023 [3]. While the proliferation of WIoT devices brings great convenience, it also introduces various security challenges. WIoT devices generate, process, and exchange large volumes of privacy-sensitive data [4] that are closely related to people' s daily lives. Moreover, WIoT devices connect via wireless links with inherently low security, and their limited power, storage, and computational capabilities make them vulnerable to attackers who may steal, misappropriate, or forge identities to tamper with devices, posing significant threats.

Blockchain, as a distributed computing and storage system integrating multiple technologies, has been widely applied in WIoT security due to its decentralization, immutability, and traceability [5]. Blockchain also provides robust privacy protection for transactions through cryptographic hash algorithms. However, blockchain security relies on its highly redundant nature, requiring each node to store complete transaction histories to ensure data security [6]. WIoT devices are typically simple in design with limited memory, making it difficult to store entire blockchains. For example, the Bitcoin blockchain [7] required nearly 380GB per node by early 2022 [8], presenting a massive challenge for WIoT node storage.

To address blockchain storage requirements, current widely adopted solutions include light nodes, compressed blockchains, sharded blockchains, and coded

blockchains [9]. Light nodes [7] store no block data and must rely on full nodes when verifying specific transactions, reducing system distribution and creating security vulnerabilities [10]. Compressed blockchains reduce storage by deleting partial blockchain information, with nodes storing only transaction information needed for new block verification [7], user balances [11], or block summaries [12], but this permanently loses some block data, compromising blockchain integrity. Sharded blockchains [13] partition the blockchain into multiple sub-chains, reducing storage proportionally with shard count, but cross-chain transactions and shard merging require high node functional complexity. Additionally, fewer nodes in sub-chains reduce security [14]. Coded blockchains [15] use error correction coding to distribute blockchain data across nodes, but require powerful encoding/decoding capabilities, increasing operational costs.

Compared with traditional blockchains, directed acyclic graph (DAG) blockchain' s high concurrency is considered the most promising research direction for solving blockchain scalability issues, gaining increasing attention from academia and industry [16]. DAG also brings new solutions to WIoT storage problems, exemplified by IOTA (Internet of Things Application cryptocurrency) [17], Byteball [18], and Hashgraph [19]. Specifically, literature [6] proposes a lightweight DAG blockchain for resource-constrained vehicular social networks, where each node stores only data of interest within topic groups, and further proposes intra-group historical data pruning to reduce duplicate storage. Literature [20] presents a DAG-based IIoT architecture combining differential privacy to ensure data privacy and integrity, along with a load balancing algorithm to balance node energy consumption and network lifetime. Literature [21] proposes a Lightweight and Scalable Distributed Ledger for IoT (LSDI), dividing large P2P networks into smaller ones to reduce computational overhead and deleting old transactions to reduce storage overhead, demonstrating high transaction throughput while managing WIoT storage and computational costs. Literature [22] analyzes and compares DAG-based blockchains, concluding IOTA is most suitable for WIoT as it achieves zero transaction fees, ensures data integrity, and avoids double-spending attacks. However, IOTA is transaction-oriented, requiring transaction verification and complex weight calculation during block generation. Moreover, IOTA exhibits extremely rapid storage expansion and requires network-wide broadcasting for new blocks, making it unsuitable for direct deployment on resource-constrained WIoT nodes.

In current WIoT applications, nodes do not need to verify or judge data collected by other nodes [23], such as temperature or humidity measurements. When such data is sent to users, they make final decisions based on the data, such as initiating fire alarms [24] or artificial rainfall [25]. Therefore, integrating WIoT with blockchain requires ensuring data immutability while preventing network administrators from making incorrect decisions based on attacker-modified data.

To reduce storage requirements and transmission consumption in WIoT while ensuring data security, this paper proposes a Local DAG Blockchain (LDB)

scheme that provides secure data storage for resource-constrained WIoT with low storage and transmission demands. In essence, LDB uses DAG blockchain as the underlying data structure for WIoT, operating at the data level rather than block level for greater efficiency and scalability compared to traditional blockchains. Unlike IOTA, LDB nodes only send data summaries to physically close neighbors without network-wide broadcasting, reducing transmission overhead. Simultaneously, nodes store only their own generated data blocks and summaries of a few neighboring blocks, dramatically reducing network storage requirements.

---

1 System Model

This paper' s proposed LDB integrates optimizations in block structure, operation mode, complexity, and security to meet WIoT nodes' low-energy, low-storage requirements while ensuring data security, making the system secure and resource-efficient.

In traditional blockchains, nodes must independently store all blocks, establishing a unidirectional link from genesis to latest blocks. For resource-constrained WIoT, this is impractical. To address this, LDB is divided into physical and logical layers: WIoT and DAG blockchain. At the physical layer, WIoT consists of sensor nodes and users, with sensor nodes storing only locally generated data blocks and minimal neighbor summary information to reduce storage. At the logical layer, the DAG blockchain links sensor node-collected data to achieve immutability. Table 1 summarizes the notation used.

Table 1. System Symbols

Symbol	Description
P	Data or transaction information
$F(\cdot)$	Function to compute data digest and block hash
d	Parent block hash byte length
S_i	Sensor node i
t_i^Z	Timestamp when node i generates block Z
b_i^Z	Address of block Z from node i
σ_i^Z	Signature of block Z from node i
R	Sensor node transmission radius
d_{ij}	Euclidean distance between sensor nodes i and j
θ	Block size and field length
N_i	Neighbor set of sensor node i
n_i	Number of blocks generated by sensor node i
C_{avg}	Average network transmission consumption

Symbol	Description
S_i^Z	Storage space occupied by block Z on WIoT node i
h_{ij}	Current state block hash value of sensor node j, neighbor of node i

At the physical layer, WIoT is represented as $G = (V, E)$, where V is the set of sensor nodes and E is the set of links between them. Assuming each node has identical transmission range R, two nodes are neighbors if their Euclidean distance is less than R, defined as $N_i = \{j \mid d_{ij} < R, \forall j \in V\}$. The node set V and link set E constitute the WIoT.

At the logical layer, $D = (B, L)$ represents the DAG distributed ledger structure, where B is the set of data blocks and L is the set of links between blocks. Each element in L is an ordered pair of elements in B (i.e., (b_α, b_β)), denoted as l_k, representing a link between data blocks. For any block $b_\alpha \in B$, no path exists from b_α back to itself, establishing a directed acyclic graph among data blocks.

Let $b_i^Z = \langle i, Z, t_i^Z \rangle$ denote the block generated by sensor node i at time t_i^Z, where Z is the latest block sequence number generated by that node. Set $h_{ii}^Z = F(b_i^Z)$ as the block hash value. Each node i's current state block is b_i^Z, and $h_{ij}^Z = F(b_j^Z)$ represents the hash of neighbor node j' s current state block. Thus, $h_{ij}^Z = F(b_j^Z)$. Assuming node i generates data at rate r_i, when it generates θ bytes of data, it packages them into a block with data portion size θ, where timestamp t_i^Z is calculated by:

$$t_i^Z = \frac{\theta}{r_i}$$

Figure 1 illustrates an LDB blockchain example. The upper portion shows a DAG blockchain with 9 blocks generated by three nodes (1, 2, 3), each producing 3 blocks. This can be converted to a traditional DAG blockchain, such as IOTA' s consensus mechanism Tangle [17], shown in the lower portion.

2 Local Directed Acyclic Graph Blockchain (LDB)

This section first analyzes IOTA' s block structure, then discusses storage and transmission consumption in IOTA-based WIoT systems, proposes LDB' s block structure and operation mode, analyzes sensor node storage and transmission consumption, and finally examines LDB' s security.

2.1 IOTA Block Structure

In IOTA, transactions are the basic data units, with each block containing one transaction. The complete block set contains all transaction-related information. Figure 2 shows IOTA' s DAG blockchain block structure, which primarily

consists of block address, Tag, two parent block hashes, timestamp, nonce, Bundle, signature, and information list. The information list varies by application: transaction information in cryptocurrency, or data to be stored in WIoT devices. Unlike single-chain blockchains, each IOTA block contains two parent block hashes.

The size of an IOTA block b_i^{IOTA} is:

$$|b_i^{IOTA}| = |F(A)|+|F(d)|+|F(Tag)|+|F(t_i^Z)|+|F(x)|+|F(\text{Bundle})|+|F(\text{nonce})|+|F(M)|+|F(P)|$$

In IOTA-based sensor networks, the storage space occupied by blocks on sensor nodes is calculated as:

$$S_i^{IOTA} = \sum_{b_i^Z \in B} \sum_{i=1}^{n} |b_i^Z|$$

Each sensor node broadcasts new blocks to all nodes during generation, so IOTA' s average transmission consumption is:

$$C_{avg}^{IOTA} = \sum_{b_i^Z \in B} \sum_{i=1}^{n} |b_i^Z| \times \theta$$

2.2 LDB Block Structure

Considering that WIoT nodes do not need to verify other nodes' historical data in practical applications [23], LDB redefines its block structure for better WIoT suitability. Unlike IOTA, LDB stores and transmits data information, so it removes IOTA's Tag and Bundle fields while changing transaction information to data information. Since nodes must store neighbor node summary information, LDB extends IOTA' s two parent block hashes to P_i parent block hashes, where P_i depends on the number of neighbor sensor nodes of block i' s originating sensor node.

Thus, LDB block structure includes block address, P_i parent block hash values, timestamp, nonce, signature, and data information, as shown in Figure 3. This structure ensures data security and resists Sybil, replay, and DDoS attacks.

The size of an LDB block b_i^{LDB} is:

$$|b_i^{LDB}| = |F(A)| + P_i \times |F(d)| + |F(t_i^Z)| + |F(f)| + |F(\text{nonce})| + |F(M)| + |F(P)|$$

2.3 LDB Operation Mode

In LDB, when sensor nodes collect sufficient data, they broadcast only to neighbor nodes rather than network-wide, and each node stores only its own blocks and neighbor-broadcasted block hashes. The operation mode proceeds as follows:

1. Sensor node i collects data f_i within a time period;

2. Obtains block signature using the data address' s private key;
3. Uses stored neighbor nodes' latest state block hashes as parent hashes h_{ij}, then performs proof-of-work to find an appropriate nonce value;
4. Sensor node i composes new block $b_i^Z = \langle i, Z, t_i^Z \rangle$ with f_i, block address, h_{ij}, nonce, signature, and timestamp, computes $h_i^Z = F(b_i^Z)$, broadcasts to neighbor nodes $j \in N_i$, and stores link information locally;
5. Neighbor nodes j store received h_i^Z in local storage and update neighbor state blocks.

Figure 4 illustrates the LDB workflow. For simplified notation, blocks are represented as b_i^Z and hashes as h_i^Z. When sensor node E collects data f_E, it signs the block using its private key, uses neighbor node D' s current state block hash h_D^Z as parent hash, performs proof-of-work to find nonce, packages f_E, block address, h_D^Z, nonce, and signature into block b_E^Z, computes h_E^Z, and broadcasts to node D. Similarly, when node A collects data f_A, it uses neighbor nodes B and C' s current state block hashes h_B^Z and h_C^Z as parent hashes, performs proof-of-work, packages f_A, block address, h_B^Z, h_C^Z, nonce, and signature into block b_A^Z, computes h_A^Z, and forwards to nodes B and C. Upon receiving h_A^Z, nodes B and C update their storage.

Thus, each sensor node only sends blocks to neighbors, forming a localized blockchain system, while all node block data collectively form a complete DAG blockchain, ensuring data security.

In LDB-based sensor networks, block storage space is calculated as:

$$S_i^{LDB} = \sum_{b_i^Z \in B} \sum_{i=1}^{n} |b_i^Z| + \sum_{j \in N_i} |h_{ij}^Z|$$

In LDB, each new block only sends its hash to neighbor nodes, so average transmission consumption is:

$$C_{avg}^{LDB} = \sum_{b_i^Z \in B} \sum_{i=1}^{n} |h_i^Z| \times \theta$$

2.4 Storage and Transmission Complexity Analysis

To evaluate LDB performance, we compare storage and transmission consumption between the two approaches. Assuming n sensor nodes in the network, each block comprises a header and body. In Bitcoin, for example, the block header contains metadata linking to the previous block, while the block body contains all transaction information. Since the block body is much larger than the header [17], let storage and transmission complexity for block bodies be $O(\theta)$ and for headers be $O(1)$.

IOTA's storage and transmission complexity is $O(n\theta)$. In LDB, each node stores all block headers and only its own generated data (a minimal portion of block

bodies). Additionally, LDB nodes only send block headers and bodies to neighbors, not network-wide. Therefore, LDB' s storage complexity is $O(n+\theta)$ and transmission complexity is $O(\theta)$. In the worst case where all nodes are mutual neighbors, LDB' s storage complexity remains far smaller than IOTA' s, with identical transmission complexity. However, in practical WIoT networks, the probability of all nodes being neighbors is extremely low, with $|N_i| \ll n$, making LDB' s actual transmission complexity lower than IOTA' s (see experiments 3.5 and 3.6).

2.5 Security Analysis

This section analyzes LDB' s security in WIoT and discusses three attack modes:

1) Sybil Attack Resistance: In P2P networks, a malicious node can assume multiple identities to refuse block reception or transmission, effectively preventing other users from accessing the network. If attackers control 51% of nodes, they can easily alter transaction order and prevent confirmation. In LDB, when at least one honest node exists, hash digest links in the honest node' s logical DAG reveal disconnections, enabling attack detection. If sensor node i is attacked, creating numerous malicious nodes sending false data hashes h_{ij}^{Z}, the network administrator obtaining node i' s data can verify neighbor node j' s blocks and detect logical DAG link errors. Furthermore, LDB' s quantitative proof-of-work during block creation ensures block validity, enabling Sybil attack resistance.

2) Replay Attack Resistance: Replay attacks involve sending previously received packets to deceive systems, primarily targeting authentication processes. Attackers steal authentication credentials via network sniffing and resend them to authentication servers. In LDB, each block b_i^Z contains a timestamp t_i^Z, enabling precise time synchronization with minimal transmission delay, even in large networks. In Figure 4, if sensor node A is attacked and resends previous block hashes h_{13}^{Z} to nodes B and C, the first transmission timestamp $t_{A,1}$ differs from the resent timestamp $t_{A,2}$. Since $t_{A,1} \neq t_{A,2}$, nodes B and C can reject duplicate transmissions, effectively resisting replay attacks.

3) DDoS Attack Resistance: DDoS attacks involve multiple attackers simultaneously targeting one or more victims, or a single attacker controlling multiple machines. In LDB, each block has its own timestamp t_i^Z. If attackers send numerous blocks from a single sensor node simultaneously, the attack is easily detected. Since sensor networks typically use inexpensive devices, compromised nodes can be replaced. Thus, DDoS attacks have minimal impact.

3 Experiments

3.1 Experimental Environment

Simulation experiments were coded in PyCharm using Python 3.7 and run on a Windows 10 system with an Intel Core i7-7500U CPU and 8GB RAM. To ensure accuracy, each data point represents the mean of 100 independent simulation runs.

3.2 Main Parameter Settings

To thoroughly evaluate LDB performance in WIoT, we implemented the proposed LDB scheme based on DAG blockchain and validated its feasibility against IOTA. For representative results, network models were randomly generated with sensor nodes placed randomly within a 50m radius circle. Key parameters include: sensor node transmission range $R = 20m$, average data generation rate $r_i = 50$ bit/s, block data portion size $\theta = 1024$ bit (based on IOTA' s small size [27]), block hash length $F(\cdot) = 256$ bit, fixed-size blocks $P = 500$ bit, and average block generation time $t_i^Z = 10$ s. In IOTA, sensor nodes broadcast blocks using gossip protocol, where nodes send updated ledger states to neighbors, compare requested versions, check for conflicts, update their ledger states, and forward updates. In LDB-based WIoT, nodes only send blocks to neighbors, simplifying broadcasting.

Since LDB block headers store P_i more hash values than IOTA's 2 parent hashes, experiment 3.3 demonstrates minimal block header impact on node storage. Experiment 3.4 compares block header impact on storage between LDB and IOTA, showing storage ratios. Experiment 3.5 evaluates storage and transmission consumption differences in random WIoT networks, clearly showing LDB' s significantly lower storage. Finally, experiment 3.6 compares link load between the two approaches.

3.3 Impact of Block Headers on Storage Space

For realistic data distribution, we assume Poisson-distributed data generation rates. The network initially contains $Z = 1000$ blocks. Figure 5 shows sensor node data distribution. Since LDB blocks contain more parent hashes than IOTA' s 2, we analyze block header storage impact. Based on equations (5) and (8), we record the ratio of sensor nodes using LDB versus IOTA and display frequency distributions in Figure 6. Results show that with $n = 500$ nodes, the block header ratio increases storage by only 0.1% compared to no headers, decreasing further as network scale grows. Thus, block headers have minimal impact on overall node storage.

3.4 Node Storage Comparison and Analysis

Figure 7 compares overall node storage trends between LDB and IOTA in WIoT. The experiment assumes $n = 500$ sensor nodes, each generating $Z = 40$ blocks.

Based on equations (4) and (7), node storage increases as nodes continuously collect data and receive blocks from others. Both methods show increasing trends, but at timestamp $t_i^Z = 50$s, LDB-based WIoT node storage is approximately $S_i^{LDB} = 4.39 \times 10^3$ bit, while IOTA-based WIoT node storage is $S_i^{IOTA} = 2.0 \times 10^7$ bit—approximately 500 times larger. As node count increases, LDB storage scales down proportionally with network size. This occurs because IOTA requires every node to store all blocks network-wide, while LDB only stores neighbor node hashes. Results demonstrate that LDB reduces WIoT node storage space by 99.8% compared to IOTA, with greater reductions as network size increases.

3.5 Transmission Consumption Comparison and Analysis

Figure 8 shows overall transmission consumption trends between LDB and IOTA in WIoT, analyzing block size impact. In equations (5) and (8), LDB links refer to neighbor connections, while IOTA links refer to network-wide connections. Both methods' consumption increases over time, but LDB' s is substantially lower. At $t_i^Z = 50$s, LDB average transmission consumption is $C_{avg}^{LDB} = 6.1 \times 10^5$ bit, while IOTA' s is $C_{avg}^{IOTA} = 1.96 \times 10^6$ bit—a 66.2% reduction. This is because IOTA nodes forward blocks to neighbors' neighbors iteratively until all nodes receive them, whereas LDB only sends block hashes to immediate neighbors. Results show LDB reduces average transmission consumption by 66.2% compared to IOTA.

3.6 Link Load Comparison and Analysis

Figure 9 depicts link traffic variation between the two methods, measured as block count per link. The experiment assumes a network of $n = 500$ sensor nodes generating $Z = 2000$ blocks across 1500 links. In IOTA-based WIoT, link 1 transmits approximately 2000 blocks with irregular, high-volume distribution. In LDB-based WIoT, link traffic is more balanced, preventing excessive network link load. Results demonstrate that LDB reduces maximum link load by approximately 28 times compared to IOTA, effectively alleviating link congestion and reducing network link load.

---

4 Conclusion

This paper investigated a WIoT data security transmission scheme based on DAG blockchain. We proposed a secure WIoT data transmission model (LDB) that leverages blockchain technology to achieve data immutability. LDB introduces DAG blockchain technology distributed to local nodes, eliminating network-wide data verification. This reduces node storage requirements and inter-node transmission consumption while improving overall network throughput. Compared with IOTA, LDB demonstrates superior link traffic distribution.

Future work will continue exploring blockchain data security in IoT, particularly WIoT. To address DAG blockchain storage bottlenecks, we will investigate enhanced storage techniques. While this paper provides security and performance analysis of IOTA and LDB, subsequent research will examine LDB' s concrete implementation in WIoT. Considering WIoT characteristics, future work may incorporate a credit scoring mechanism for each node to detect potential attacks.

References

[1] Shi Huiyang, Liu Ling, Zhang Yuqing. A review of BoT: Blockchain for the Internet of Things [J]. *Journal of Cyber Security*, 2019, 4(5): 76-91.

[2] Chen Min, Hao Yixue. Task offloading for mobile edge computing in software defined ultra-dense network [J]. *IEEE Journal on Selected Areas in Communications*, 2018, 36(3): 587-597.

[3] Fakhri D, Mutijarsa K. Secure IoT communication using blockchain technology [C]// *International Symposium on Electronics and Smart Devices (ISESD)*. IEEE, 2018: 1-6.

[4] Qu Chao, Tao Ming, Zhang Jie, et al. Blockchain based credibility verification method for IoT entities [J]. *Security and Communication Networks*, 2018: 1-11.

[5] Restuccia F, Kanhere S D, Melodia T, et al. Blockchain for the internet of things: Present and future [J]. arXiv preprint arXiv:1903.07448, 2019.

[6] Yang Wenhui, Dai Xiaohai, Xiao Jiang, et al. LDV: A lightweight DAG-based blockchain for vehicular social networks [J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(6): 5749-5759.

[7] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [DB/OL]. (2008-10-31) [2019-10-02]. http://bitcoin.org, 2008.

[8] Blockchain. BlockchainCharts [EB/OL]. (2022) [2022-04-04]. https://www.blockchain.com/charts.

[9] Sun Zhixin, Zhang Xin, Xiang Feng, et al. Survey of storage scalability on blockchain [J]. *Journal of Software*, 2021, 32(1): 1-20.

[10] Karame G O, Androulaki E. *Bitcoin and Blockchain Security* [M]. Artech House, 2016.

[11] Nadiya U, Mutijarsa K, Rizqi C Y. Block summarization and compression in bitcoin blockchain [C]// *International Symposium on Electronics and Smart Devices (ISESD)*. IEEE, 2018: 1-4.

[12] Kim T, Noh J, Cho S. SCC: Storage compression consensus for blockchain in lightweight IoT network [C]// *IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2019: 1-4.

[13] Zamani M, Movahedi M, Raykova M. Rapidchain: Scaling blockchain via full sharding [C]// *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018: 931-948.

[14] Das S, Kolluri A, Saxena P, et al. On the security of blockchain consensus protocols [C]// *International Conference on Information Systems Security*. Springer, Cham, 2018: 465-480.

[15] Dai Mingjun, Zhang Shengli, Wang Hui, et al. A low storage room requirement framework for distributed ledger in blockchain [J]. *IEEE Access*, 2018, 6: 22970-22975.

[16] Gao Zhengfeng, Zheng Jilai, Tang Shuyang, et al. State-of-the-art survey of consensus mechanisms on DAG-based distributed ledger [J]. *Journal of Software*, 2020, 31(4): 1124-1142.

[17] Popov S. The tangle [J]. *White paper*, 2018, 1(3). https://www.iota.org/main/media/docs/IOTA_{Whitepa

[18] Churyumov A. Byteball: A decentralized system for storage and transfer of value [J]. https://byteball.org/Byteball.pdf, 2016.

[19] Baird L. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance [J]. *Swirlds, Inc. Technical Report SWIRLDS-TR-2016*, 1.

[20] Zeng Pengjie, Wang Xiaoliang, Dong Liangzuo, et al. A blockchain scheme based on DAG structure security solution for IIoT [C]// *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2021: 935-943.

[21] Cherupally S R, Boga S, Podili P, et al. Lightweight and scalable DAG-based distributed ledger for verifying IoT data integrity [C]// *International Conference on Information Networking (ICOIN)*. IEEE, 2021: 267-272.

[22] Bhandary M, Parmar M, Ambawade D. A blockchain solution based on directed acyclic graph for IoT data security using IOTA Tangle [C]// *5th International Conference on Communication and Electronics Systems (ICCES)*. 2020: 1124.

[23] Guo Cai, Li Xuran, Chen Yanhua, et al. Blockchain technology for Internet of things: an overview [J]. *Chinese Journal on Internet of Things*, 2021, 5(1): 72-89.

[24] Mahgoub A, Tarrad N, Elsherif R, et al. IoT-based fire alarm system [C]// *Third World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*. IEEE, 2019: 162-166.

[25] Malhotra A, Som S, Khatri S K. IoT based predictive model for cloud seeding [C]// *Amity International Conference on Artificial Intelligence (AICAI)*. IEEE, 2019: 669-773.

[26] Sarfraz U, Alam M, Zeadally S, et al. Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions [J]. *Computer Networks*, 2019, 148: 361-372.

[27] *Additional technical specifications for IOTA implementation details.*

Note: Figure translations are in progress. See original paper for figures.