SPACECHAIN: A THREE-DIMENSIONAL BLOCKCHAIN ARCHITECTURE FOR IOT SECURITY

Miao Du, Kun Wang, Yinqiu Liu, Kai Qian, Yanfei Sun, Wenyao Xu, and Song Guo

ABSTRACT

Deploying blockchain in IoT is an effective way to address traditional security issues. However, existing approaches have two major limitations: since the blockchain itself is subject to attacks, including selfish mining, double spending, and distributed denial of service attacks, IoT smart devices are also vulnerable once hackers successfully invade blockchain systems; due to the heterogeneity and resource limitations of IoT devices, the deployment of the existing blockchain systems in the IoT scenario cannot reflect strong adaptability and meet IoT service requirements. In this article, we introduce Spacechain, a secure and high-performance blockchain system with three-dimensional ledger architecture, to enable blockchain open in IoT. Specifically, we first design a three-dimensional architecture with novel data structures to deal with the heterogeneity and scalability of IoT networks. Then, we propose the Three-Dimensional Greedy Heaviest-Observed Sub-Tree (3D-GHOST) consensus mechanism for Spacechain to improve security and network performance. Additionally, we conduct detailed security analysis and extensive experimental verification to demonstrate the performance of Spacechain.

INTRODUCTION

It is universally known that the era of intelligent Internet has gradually arrived along with the emerging development of the Internet of Things (IoT). Undoubtedly, the development momentum of IoT is currently unstoppable. The cloud-to-object connection is creating new opportunities, for example, the revitalization of manufacturing, the rapid development of smart cities, and the establishment and sharing of digital archives, all of which take advantage of the IoT [1]. However, existing IoT technologies are clearly unable to meet the rapidly evolving IoT needs due to insufficient authentication, inefficient semi-automated transactions, and traceability of records [2].

Fortunately, deploying blockchain in IoT recently is an effective solution to the above issues [3]. The blockchain is hierarchically structured through a peer-to-peer (P2P) network so that the entire network can perform complete information transfer and verify its accuracy [4]. In addition, the blockchain utilizes automatic filtering mode to establish credit resources. This kind of reliable resource can effectively improve the security of IoT transactions. More importantly, blockchain nodes can independently participate in or leave without any interference to the entire blockchain. Thus, blockchain solutions can rationally integrate IoT data resources, and promote the security of IoT users [5].

The decentralization, self-management, and collective maintenance of blockchain subvert the way IoT develops. Obviously, the blockchain can ensure the data integrity, traceability, and non-tampering, which in turn causes a waste of some network resources (e.g., communication bandwidth and computation resources) [6]. In addition, the distributed structure of blockchain and the limited computation power of IoT nodes have become the major obstacles to deploying blockchains in IoT scenarios.

To address scalability and security issues, some approaches attempt to provide a reliable and scalable solution to the blockchain for proper IoT management [7–9]. For example, Huh *et al*. [7] proposed a seven-layer blockchain platform-based IoT management system to deal with the synchronization and heterogeneity issues in IoT. On the other hand, some methods have also been proposed to enhance blockchain security, that is, blockchain-based key management [10], anonymous multi-signature [11], and homomorphic encryption [12]. However, they failed to achieve network performance and security optimization due to the lack of innovation throughout the blockchain architecture.

Therefore, deploying blockchain in IoT scenarios still face multiple challenges:

- Security threats, including selfish mining, double spending, and distributed denial of service (DDoS) attacks
- Deficient resource utilization due to the heterogeneity of IoT
- Insufficient scalability of blockchain due to the dynamics of IoT devices

In order to design a secure and high-performance IoT-oriented blockchain architecture, we summarize architectural design principles and performance requirements as follows.

Security: Although blockchain technology can resist traditional attacks in IoT (e.g., man-in-the-middle [MITM] attack, advanced persistent threats [APTs], and eavesdropping [6]), some special attacks (e.g., selfish mining and double spending) against the characteristics of blockchain still need to be taken seriously. Once the distributed

Miao Du, Yinqiu Liu, Kai Qian, and Yanfei Sun are with Nanjing University of Posts and Telecommunications; Kun Wang (corresponding author) is with the University of California; Wenyao Xu is with the State University of New York, Buffalo; Song Guo is with The Hong Kong Polytechnic University.

Digital Object Identifier: 10.1109/MWC.001.1900466

1536-1284/20/$25.00 © 2020 IEEE

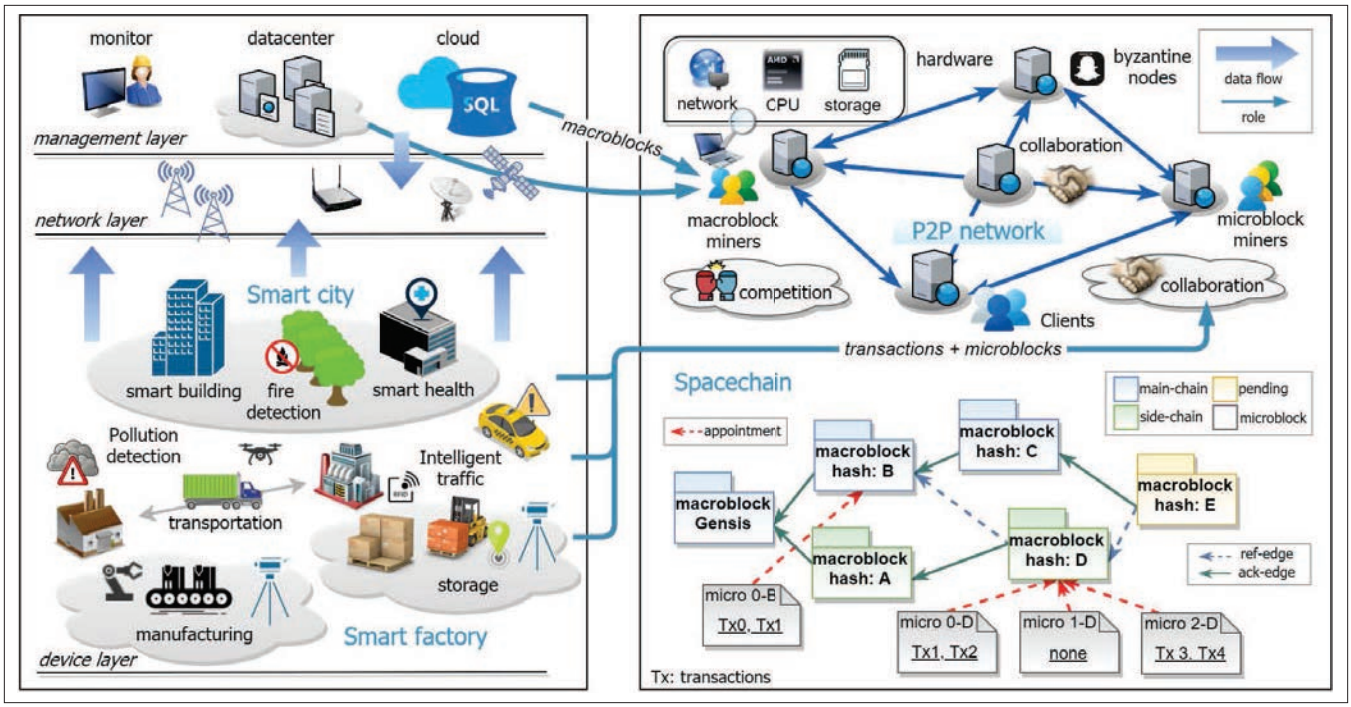

FIGURE 1. A three-dimensional blockchain architecture of Spacechain in IoT.

blockchain architecture is introduced into IoT, the overall security requirements will increase accordingly, especially for some of the transactions on the chain.

Adaptability: The IoT environment is constantly changing, which brings adaptive demands to blockchain architecture. Undoubtedly, adaptability is critical to ensuring successful blockchain deployment. The blockchain architecture can cater to IoT users by expanding the range of applications.

Scalability: Scalability is an important metric in the design of distributed blockchain architecture for IoT. Specific design concepts include resource efficiency, flexibility, and network performance stability.

To this end, we put forward Spacechain, a three-dimensional blockchain architecture. We introduce Spacechain into IoT to improve the security and network performance. The main contributions of our article are listed as follows:

- We propose Spacechain, an innovative IoT-oriented three-dimensional blockchain architecture to address the heterogeneity and scalability of IoT networks.
- We present a novel Three-Dimensional Greedy Heaviest-Observed Sub-Tree (3D-GHOST) consensus mechanism for Spacechain to improve the security and network performance.
- We conduct detailed security analysis, and then evaluate the performance of Spacechain by comparing the various metrics with the previous works.
- We summarize several challenging open issues, indicating potential research directions for the future.

Spacechain: A Three-Dimensional Blockchain Architecture in IoT

In this section, we propose Spacechain, which is a three-dimensional blockchain architecture for IoT. Specifically, we introduce the design principles in terms of the ledger architecture, data structures, and parallel workflows, respectively.

Three-Dimensional Ledger Architecture

Viewed from ledger architecture, the previous blockchain (e.g., Bitcoin and Ethereum) adopts two-dimensional structures, wherein the ledger only consists of one kind of block. The newly created blocks point to one (in Bitcoin) or several (in Ethereum) parent blocks, thus forming the linear or graphic ledger. To enhance the scalability, we present the concept of a three-dimensional ledger composed of two kinds of blocks, namely macroblock and microblock. In detail, we first construct a directed acyclic graph (DAG) foundation using macroblocks. Then numerous microblocks connect to the DAG foundation and form the third dimension. Such a three-dimensional ledger architecture effectively accommodates the parallel workflows, which improves the network scalability and overcomes the serious heterogeneity in IoT. As shown in Fig. 1, the DAG foundation has the following core elements:

- **Vertex:** Macroblocks are called vertices, where the root of these vertices is called Genesis. In addition, the tip refers to the vertex whose in-degree is 0 (e.g., E).
- **Edge:** Edge indicates the connection between two vertices. When miners create a pending macroblock, they will fulfill the Ref_hash to connect to previous vertices, where Ref_hash refers to a list for storing the hash values of paternal macroblocks.
- **Ack-edge:** The acknowledgment edge (ack-edge) is the embodiment of the voting relationship. If one vertex connects to another via ack-edge, this vertex acknowledges its validity. In Ref_hash, the ack-edge is the first element.
- **Ref-edge:** The reference edge (ref-edge) represents a timing relationship. After determining the ack-edge, the newly created macroblock

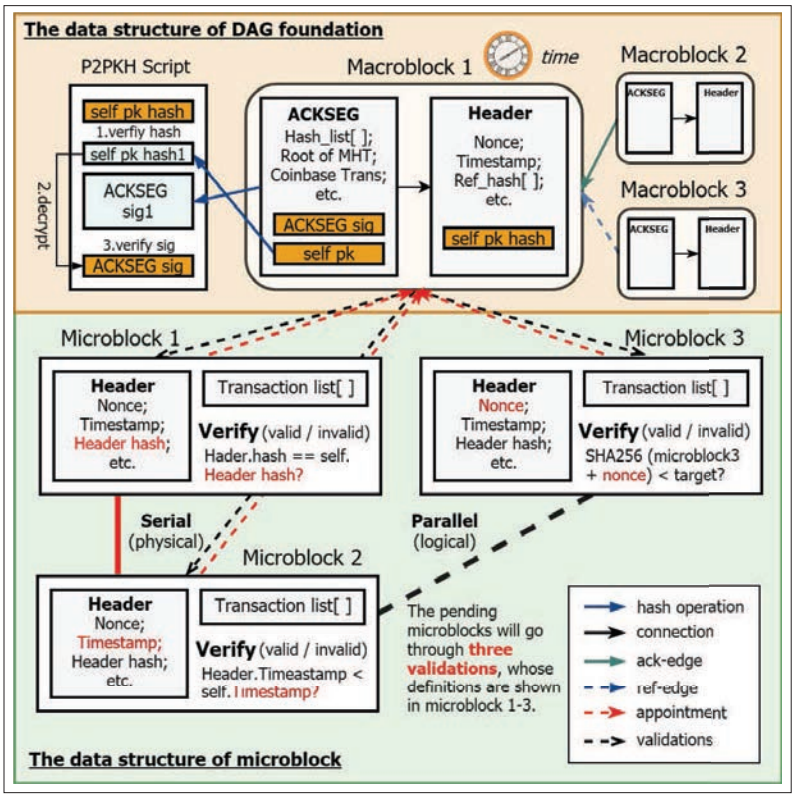

FIGURE 2. Data structure of macroblock and microblock.

will connect with the remaining *tips* via ref-edge and further fill the Ref_hash.

For each vertex of DAG, all the microblocks connecting to it are mutually independent, for example, 0-D, 1-D, and 2-D belonging to D. Moreover, the number of connected microblocks reflects the weight of one vertex in the three-dimensional ledger, which is vital for the proposed 3D-GHOST.

Data Structure Design

As shown in Fig. 2, Spacechain divides the ledger entries into macroblocks and microblocks. In our proposal, one macroblock header and the corresponding acknowledgment segment (ACKSEG) constitute a macroblock. During each round of ledger extension (i.e., *epoch*), all significant control information is saved in the macroblock header, including the aforementioned Ref_hash, the pending solution of proof of work (PoW), and the Unix timestamp. Furthermore, ACKSEG encapsulates the confirmation message of one epoch, which also contains a series of important information, for example, the hash list of microblocks, the coinbase transaction rewarding the miner, and the root of the Merkel tree. Note that the validity of ACKSEG is protected by Pay-to-Public-Hash (P2PKH) style scripts. Only if the received ACKSEG passes such scripts can peers acknowledge the confirmation massage within it.

As for microblocks, they carry the necessary metadata (e.g., timestamp and PoW solution) and numerous transactions from IoT devices and users. The validation of microblocks contains three steps:

- PoW validation for verifying the pending PoW solution
- Header_hash validation for verifying whether the microblock is assigned to the targeted macroblock
- Timestamp validation for verifying whether the microblock belongs to the right epoch.

No matter which kind of blocks are being created, PoW is needed since it can effectively ensure the network security and defend the ambiguous data tampering. Under PoW, peers are required to solve one tough hash puzzle before creating blocks. More precisely, they use the binary type of the previous block with a changing nonce as inputs, then execute hash operations until the output is smaller than the predefined target. This process is both computation-intensive and time-consuming, thus limiting the involvement of power-constrained IoT devices. In Spacechain, we update traditional PoW and integrate it into the parallel workflows, which is mentioned in the following part.

Parallel Workflows

As illustrated in Fig. 1, we divide peers into macroblock miners and microblock miners to create the corresponding type of blocks. Among them, the macroblock miners are suggested to be executed by power-sufficient nodes (e.g., the monitors and data centers in the management layer). Meanwhile, numerous power-constrained devices, such as robotics, vehicles, and smart phones, are still open to Spacechain by serving as microblock miners. Apart from accommodating heterogeneous devices, the network decentralization also gets enhanced since more nodes are included in the consensus.

To exploit the capacity of both kinds of miners, we design dedicate workflows for them. First, we modify the conventional PoW by assigning different *targets* for creating macroblocks and microblocks. Since macroblocks carry almost all control information of the ledger extension, their creations require a smaller target; otherwise, attackers can easily propose fake messages. In addition, the relationship between macroblocks ought to be competitive, further enhancing the security of macroblocks. Contributing to our three-dimensional ledger, microblocks only contain transactions with higher concurrency and strict validation mechanisms. Hence, the target can be greatly relaxed, thereby enabling Spacechain for power-constrained IoT devices. The parallel workflows of macroblock and microblock miners in a multi-miner P2P network are shown as follows.

Macroblock Miner: After addressing the PoW, the macroblock miner is allowed to make a pending macroblock header, and then interact with other nodes in the P2P network. The whole complex process involves five critical steps:

Step 1: Append the hash of the latest main-chain vertex to the pending macroblock header's Ref_hash. Search *tips* in the local ledger, then fulfill Ref_hash using their hashes.

Step 2: Broadcast the proposed macroblock header over the P2P network.

Step 3: Once the pending macroblock header gets confirmed, the creator will become the current leader, and its *epoch* will also be launched. Other macroblock miners become followers and restart mining. The leader is responsible for verifying microblocks sent from various microblock miners.

Step 4: When receiving the new macroblock header, the leader collects all microblocks verified within the current *epoch*, then fulfills the Hash_list of ACKSEG.

Step 5: The leader broadcasts the ACKSEG; then the local host performs a restart operation on the mining process. Its own role will change to follower accordingly.

Microblock Miner: Recall that multiple microblocks that connect to the same macroblock are independent; in our Spacechain, numerous micro block miners work in parallel. For microblock miners, updates of macroblock header and ACKSEG only affect the data synchronization without terminating their running processes. As long as the local host completes the PoW, it can create and broadcast the microblocks. The concurrent transactions over the entire P2P network are thus processed by collaborative microblock miners, where everyone only packages the nearby transactions. Note that microblock miners can offload duplicate transactions from local memory when receiving new microblocks to mitigate the transaction overlap.

ACKSEG: In Spacechain, macroblock and microblock miners cooperate in extending the three-dimensional ledger. Before broadcasting microblocks, the miners should claim their target leader via header_hash. When building ACKSEG, the leader will confirm all valid microblocks, them append their hashes to hash_list. The remaining nodes in the P2P network can add correct microblocks according to the instructions of ACKSEG, thereby ensuring ledger synchronization.

Apart from two types of miners, there are also clients and Byzantine nodes in Spacechain's P2P network. If the IoT devices cannot meet the minimal requirement for serving as a miner (i.e., a processor, some storage room, and a network interface), they can only act as clients and send transactions to miners for processing. Finally, Byzantine nodes refer to malicious attackers, which might conduct any type of attack, such as selfish mining and double-spending, to destroy Spacechain.

3D-GHOST Consensus Mechanism for Spacechain

In this section, we present a novel consensus mechanism named Three-Dimensional Greedy Heaviest-Observed Sub-Tree (3D-GHOST) for Spacechain. As illustrated in Fig. 3, this mechanism can be divided into two procedures, that is, dynamic weight distribution (DWD) and Greedy Traversal.

Main-Chain and Side-Chain

To enable the blockchain function, distributed peers need to reach consistency on the validity of all transactions. In most cases, peers will encounter two types of risky transactions, namely conflicting transactions and duplicate transactions. The former might be created by attackers, intending to spend the same input multiple times for launching double-spending attacks. The latter is mainly attributed to latency, which means the same transaction occurs in several blocks. When handling risky transactions, blockchain systems only accept its first occurrence by sorting the local ledger. Therefore, the core task is to confirm the order of all blocks. Attributed to the propagation latency, multiple blocks might point to the same parent (i.e., forks). The most confirmed fork is defined as the main-chain, while others remain side-chains. To sort a forked ledger in security matters, blockchain employs consensus mechanisms. However, existing designs, such as the Nakamoto Consensus (NKC) of Bitcoin and the GHOST of Ethereum, only process the transactions on the main-chain, but side-chains are discarded. Generally, side-chains also carry massive transactions, so simply discarding side-chains results in poor performance. In contrast, the DAG foundation of Spacechain exploits all forks for maximizing the performance. To sort the three-dimensional ledger, we propose 3D-GHOST.

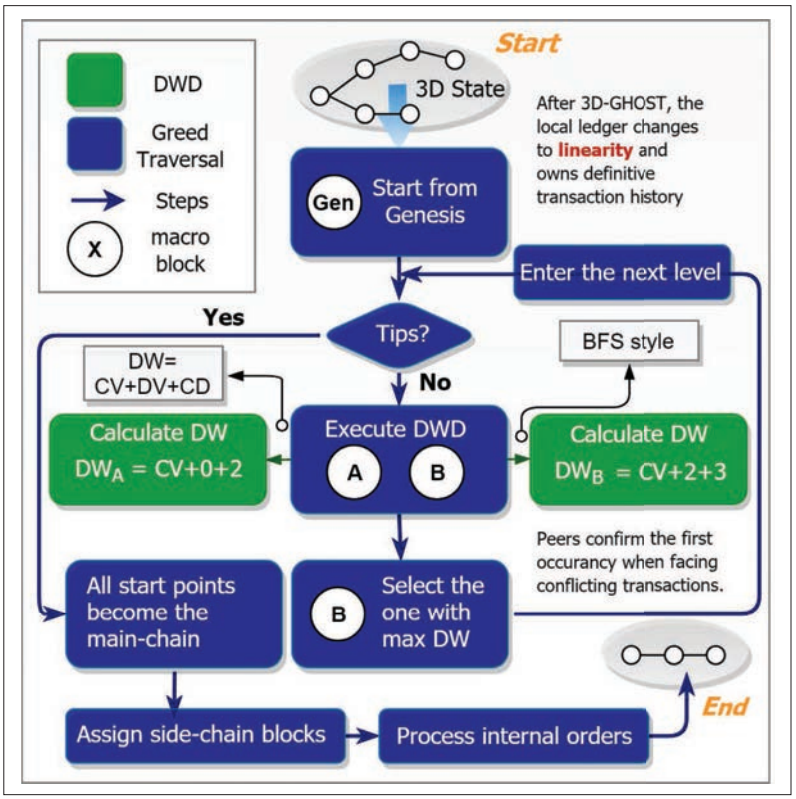

FIGURE 3. *3D-GHOST* Consensus Mechanism for *Spacechain*.

Dynamic Weight Distribution

We first design a novel DWD mechanism for dynamically assigning weight to macroblocks. In traditional GHOST, the weight of all blocks is fixed, while the dynamic weight (DW) adopted in 3D-GHOST can better reflect the real-time ledger state, including the throughput and the security level. Specifically, 3D-GHOST divides the DW of any given vertex into three aspects: *cardinal value*, *data validity*, and *contact degree*. We further explain the DWD mechanism from these metrics.

Cardinal Value (CV): CVs of macroblock and microblock are negatively correlated to their current creation rates. When the total computation power of miners increases significantly, lower CV can reduce the DW of macro/micro blocks. In contrast, higher DW will encourage miners to create more blocks in the idle periods.

Data Validity (DV): DV is defined as the total number of valid transactions packed by each macroblock. This means the conflicting or duplicated transactions will be excluded when calculating DW. To maximize throughput, considering DV, Spacechain encapsulates the most efficient transactions into the main-chain as much as possible.

Especially for IoT scenarios, selfish mining is serious since most IoT devices are power-constrained and are easily manipulated by malicious nodes. As a result, the established transaction history will be tampered with, which severely damages the blockchain security.

Contact Degree (CD): The design of CD stems from PHANTOM [13]. PHANTOM stresses that the side-chain produced by attackers is less interconnected than that of honest nodes. The CD of one vertex equals the sum of macroblocks that can reach it via **Ref-** or **ack-edge**. In this way, CD reflects the connectivity between the vertex and the entire ledger.

After measuring the above metrics, DW is defined as the sum of CV, DV, and CD. For each vertex in Spacechain, DWD distributes the corresponding DW, which is the premise of executing Greedy Traversal.

Greedy Traversal

Recall that when processing forks, the one that acquires the most confirmations will be the main-chain. In Spacechain, DW represents miners' confirmations. Hence, every vertex in the DAG foundation should be traversed for calculating its DW by executing DWD. Therefore, we further present a greedy traversal algorithm, named Greedy Traversal.

As shown in Fig. 3, applying the breadth-first-search strategy, Greedy Traversal starts from Gen and calculates the DWs of vertices level by level. For multiple vertices at the same level (i.e., the root of forks), it selects the one owning the greatest DW as the starting point for entering the next level. For instance, Fig. 3 illustrates the situation where the Greedy Traversal reaches the second level of the DAG in Fig. 1. At this level, Greedy Traversal has two choices: A and B. Since DW_A is lower than DW_B, the algorithm will choose B as the starting point. After reaching one *tip*, the set of all starting points construct the main-chain. For the remaining macroblocks, they are assigned to the nearest main-chain vertex; for example,, A belongs to Gen and D belongs to B in Fig. 1. Finally, the internal order of all macroblocks belonging to the same main-chain vertex is also determined by the DW.

Based on DWD and Greedy Traversal, we propose the novel 3D-GHOST consensus mechanism that effectively accommodates the three-dimensional ledger of Spacechain. With the assistance of *3D-GHOST*, distributed peers could reach consistency on transaction history. Given that the macroblocks that carry more valid transactions or have higher connectivity will be put forward, the system throughput and network security can also be maximized.

Security Analysis

In this section, we analyze the security issues on the proposed Spacechain from the perspective of selfish mining and double spending, respectively.

Selfish Mining

In distributed networks, the validity of a certain transaction is not fixed due to the potential of selfish mining attacks [14]. More seriously, attackers organized by mining pools might overturn the main-chain that has been confirmed by all honest nodes. Suppose that attackers and honest nodes start mining simultaneously based on the same vertex; the successful rate of selfish mining will decay over time.

Traditional blockchain systems have proven to be vulnerable against such attacks. When the attackers just own higher than 25 percent of total computation power, attackers will overturn the main-chain with a high probability. Especially for IoT scenarios, the selfish mining is serious since most IoT devices are power-constrained and are easily manipulated by malicious nodes. As a result, the established transaction history will be tampered with, which severely damages the blockchain security.

To address these issues, Spacechain first employs novel three-dimensional ledger architecture with 3D-GHOST to resist selfish mining attacks. Note that the side-chain created by attackers is undetectable until it is broadcast. Under the parallel workflows, numerous microblock miners will not appoint the attackers as their leader. Similarly, subsequent macroblocks cannot connect to a malicious side-chain through ack-edge or ref-edge. In such a case, the side-chain created by attackers generally has less DW than that of honest nodes. Consequently, the malicious side-chain cannot overturn the main-chain.

Since IoT-oriented blockchain usually introduces credits for rewarding devices, we modify the rewarding strategy for further defend against selfish mining attacks. Recall that selfish mining attacks are usually conducted by mining pools. For PoW-based blockchain, most power-constrained devices tend to join in mining pools since they cannot create blocks by themselves. Within mining pools, they can devote their computing power and then acquire the corresponding rewards. Just as Eyal *et al*. [14] summarized, peers will perform the operations that maximize their benefits. In Spacechain, the three-dimensional ledger facilitates the innovations of rewarding strategy. For macroblock miners, their credits come from creating macroblocks and validating microblocks. As to microblock miners, they are rewarded for creating microblocks and carrying transactions. Following this strategy, we guarantee that no matter whether for power-sufficient or power-constrained peers, individually performing the suggested role leads to the highest credit. Therefore, the risk from mining pool and selfish mining is further decreased.

Double Spending

Double spending is another security concern that hinders the blockchain. In practical cases, attackers will submit the normal transactions with payments, and then execute double-spending by employing helpers to broadcast conflicting transactions. Specifically, helpers are hosted by the same organization as the attacker's host and connected via a low-latency communication link. Once the attacker creates a conflicting transaction, helpers can achieve the transaction information and forward the transaction to their peers the first time so that the broadcast range and speed of the attacker's transaction will greatly exceed the original transaction. Since blockchain nodes will first acknowledge the first arriving transaction when encountering conflicting transactions, the attacker's transactions will be recognized by more nodes and have a greater probability of being packaged into the blockchain.

If the macroblock with the conflicting transactions is confirmed by the P2P network, the attack is implemented. Since the attackers are connected by low-latency confidential channels, the conflicting transactions will be forwarded faster and thus be received by more peers.

Thus, we apply the conflicting transaction forwarding (CTF) mechanism [15] to mitigate the influence of helpers. Specifically, CTF requires honest peers to normally perform the forwarding when peers receive conflicting transactions rather than only caching them. In previous blockchain systems, where only one block can be confirmed per round, the conflicting transactions that achieve relatively more peers are easier to be packed in blocks. Since the transaction processing of microblock miners is in parallel, both normal and conflicting transactions will be packed into microblocks, then assigned to leaders. In this way, helpers no longer affect the confirmations while the sequence of two transactions relies on the latency from the microblock miners, thereby defending against double-spending attacks.

In summary, Spacechain can effectively resist selfish mining and double spending attacks. We will further validate our analysis through experiments in the following section.

Performance Evaluation

In this section, we first establish the experimental platform, then compare the proposed Spacechain with the existing blockchain protocols, including standard NKC and GHOST [15], in terms of defense effect and network performance.

Implementation and Evaluation Settings

Implementation: We implement the prototype of Spacechain in Python 3. Three components make up the implementation of Spacechain: macroblock miners, microblock miners, and clients.

Simulator: To simulate different scales of workloads in the P2P network of Spacechain, we compile the automatic transaction generator. As an abstract wallet software, the transaction generator connects to the address list and initiates one simulated transaction at an adjustable rate.

Testbed: We construct a multi-miner P2P network test composed of 50 geographically distributed cloud virtual machines (CVMs) to feature the heterogeneity of the IoT network. Specifically, we divide all CVMs into 10 macroblock miners and 40 microblock miners. Each miner performs a client's workflows and is connected by one transaction generator. Moreover, CVMs are clustered into four sets with individual computing power, which is defined as the maximum number of hashes that can be executed per second. From clusters 1 to 4, peers' computing power gradually decreases.

Defense Effect

We test the defense effect on selfish mining and DDoS attacks for Spacechain. First, we test the defensive performance of selfish mining by comparing the value of the incentive efficiency (ICE). In addition, we perform DDoS attack testing, where the performance metric is confirmation latency.

Selfish Mining Testing: For each miner, ICE is defined as the obtained credits divided by its computation power. As shown in Fig. 4, resource-sufficient miners (in clusters 1, 2) maintain the highest ICE when they serve as individual macroblock miners. If they attend the mining pool, their ICE will decline due to the reward distribution. For resource-constrained peers (in clusters 3, 4), they can hardly mine macroblocks, especially for the devices in cluster 4. Thus, they acquire very low credits (with an ICE of individual: less than 48.76×10^{-10}, mining pool: less than 53.34×10^{-10}) as macroblock miners. However, if they change to microblock miners, the ICE is drastically improved (individual: 82.15×10^{-10}, mining pool: 76.22×10^{-10}). Since their computing power is small, they even acquire a higher ICE than power-sufficient peers when individually mining microblocks. Obviously, both kinds of miners no longer need to join mining pools to ensure the rewards, which can effectively weaken the attackers' power. Therefore, Spacechain can effectively defend against selfish mining.

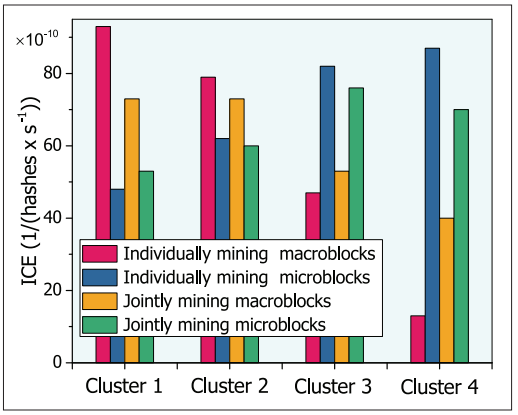

FIGURE 4. Comparison of ICE among heterogeneous clusters under selfish mining.

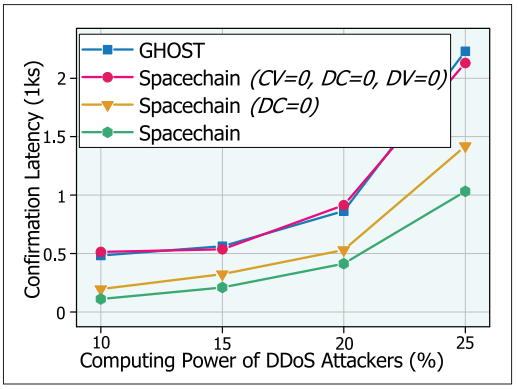

FIGURE 5. Comparison of confirmation latency under different DDoS attack power.

DDoS Attack Testing: Suppose that the confidence coefficient is 0.99, which means the probability that attackers overturn the honest main-chain and double-spend transactions is less than 1 percent. We validate the DDoS defense effect of two blockchain protocols by comparing the transaction confirmation latency, where the ratio of the attacker's computing power to the total computing power of the whole P2P network increases from 10 percent to 25 percent.

As shown in Fig. 5, Spacechain outperforms GHOST by up to 4.48, 36.32, and 53.72 percent, respectively. In the case where CV (for microblocks), DV, and CD are all fixed to zero, the 3D-GHOST protocol almost degenerates into the ordinary GHOST, which uses a fixed weight. As we mentioned before, DW can reflect the network workload and security, especially DV and CD. Therefore, enabling both DV and CD can maximize the optimization effect.

Since the transaction processing of microblock miners is in parallel, both normal and conflicting transactions will be packed into microblocks, then assigned to leaders. In this way, helpers no longer affect the confirmations while the sequence of two transactions relies on the latency from the microblock miners, thereby defending against double-spending attacks.

Using blockchain for privacy preserving in IoT systems shows promising prospects. It is insufficient to achieve anonymity only through public keys. Thus, a combination of several encryption technologies to achieve complete anonymity is an effective solution. For instance, we can comprehensively apply linkable ring signatures, homomorphic encryption, and zero-knowledge proofs to effectively guarantee identity privacy.

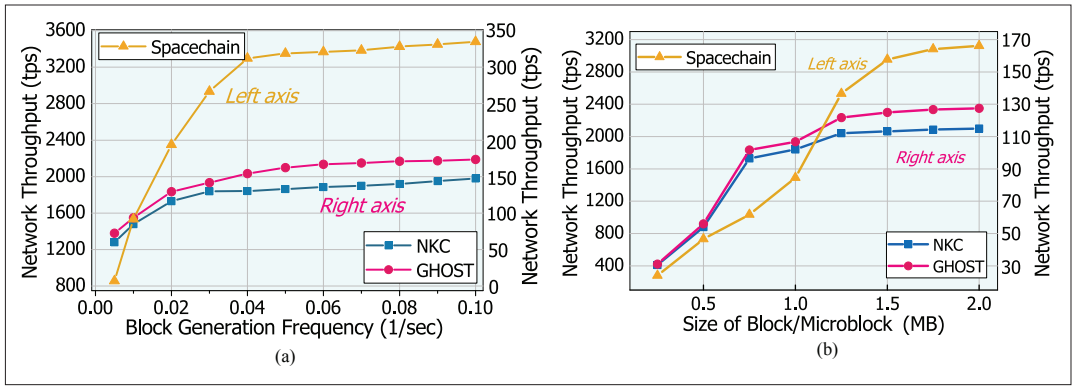

FIGURE 6. Comparison of throughput: a) block creation rate; b) block size limitation.

Such optimizations are due to the fact that in Spacechain, the block creations are distributed to numerous microblock miners rather than single miners in traditional blockchain designs. In many cases, more than one leader exists in the blockchain systems due to propagation delays. As a result, DDoS attackers will encounter great difficulties in selecting targets; thus, the defense effect of Spacechain toward DDoS attacks will be much better than others.

Network Performance

We further compare Spacechain with NKC and GHOST in terms of network throughput and scalability.

We define the size limitation of block/microblock n between 0 kB and 2 MB with increments of 250 kB each time in the experiment. Similarly, we define the creation rate of block/macroblock f between 0.01 s^{-1} and 0.2 s^{-1} with increments of 0.01 s^{-1} each time.

Network Throughput: As shown in Fig 6a, the network throughput of Spacechain outperforms 19× that of NKC and 12× that of GHOST, respectively. The outstanding performance is attributed to the high-level parallelism from parallel workflows and the increased efficiency from 3D-GHOST.

Scalability: In terms of scalability, we observe that the parallel data broadcast exceeds its capability when n = 1.5 MB and f = 0.06 s^{-1}, and n = 1.75 MB and f = 0.02 s^{-1} in Fig. 6b. We find that the major reason for limiting scalability is that NKC or GHOST only processes the transactions on the main-chain, while wasting the transactions on the side-chain. In contrast, 3D-GHOST ensures that all concurrent forks can be processed, achieving high scalability.

To this end, we can conclude that Spacechain can effectively resist selfish mining and DDoS attacks in terms of security performance. Meanwhile, Spacechain also shows sterling scalability and network throughput.

Open Issues

On the basis of the proposed three-dimensional blockchain architecture, we summarize the following open issues for the further security study.

Privacy Preservation: Using blockchain for privacy preservation in IoT systems shows promising prospects. It is insufficient to achieve anonymity only through public keys. Thus, a combination of several encryption technologies to achieve complete anonymity is an effective solution. For instance, we can comprehensively apply linkable ring signatures, homomorphic encryption, and zero-knowledge proofs to effectively guarantee identity privacy [13].

Honeypot: Honeypot is a smart contract that seems to have obvious flaws in its design, but is actually a trapping mechanism [15]. It allows any user to withdraw virtual currency from the contract, assuming that the user has transferred a certain amount of virtual currency to the contract in advance. However, once a user attempts to exploit this apparent vulnerability, a second undiscovered trap will appear, preventing the successful discharge of blockchain systems.

Zero-Knowledge Proofs: Zero-knowledge proofs allow assets to be transferred in a fully secure distributed P2P blockchain network. In a conventional blockchain transaction, when an asset is sent from one party to another, all of the transaction information is visible to other parties in the network. In contrast, in zero-knowledge transactions, others only know that a valid transaction has occurred, but the specific information (e.g., the sender, receiver, and quantity) cannot be obtained. Moreover, the amount of identity and cost can be hidden, and some security problems such as "front-running" [15] can be avoided.

Conclusion

We present Spacechain, a three-dimensional blockchain architecture for IoT security. Specifically, we first design a unique data structure and parallel workflows to address the heterogeneity and scalability of IoT networks. Then we propose the 3D-GHOST consensus mechanism to ensure the security and network performance under high workload. In addition, we analyze some security issues on the proposed Spacechain from the perspective of selfish mining and double spending, respectively. Experimental results demonstrate that Spacechain outperforms NKC and GHOST on security and network performance. Finally, some open security issues are summarized for future work.

Acknowledgments

This work is supported by the National Key Research and Development Program of China under Grant No. 2018YFB1003500; the National Natural Science Foundation of China under Grant Nos. 61872195, 61772286, and 61872310; the General Research Fund of the Research Grants Council of Hong Kong (PolyU 152221/19E);

and the U.S. National Science Foundation under Grant 1718375.

References

[1] K. Wang *et al.*, "Attack Detection and Distributed Forensics in Machine-to-Machine Networks," *IEEE Network*, vol. 30, no. 6, Nov./Dec. 2016, pp. 49–55.
[2] M. Du and K. Wang, "An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things," *IEEE Trans. Industrial Informatics*, vol. 16, no. 1, Jan. 2020, pp. 648–57.
[3] H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things J.* DOI:10.1109/JIOT.2019.2920987.
[4] M. Wu *et al.*, "A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond," *IEEE Internet of Things J.*, vol. 6, no. 5, Oct. 2019, pp. 8114–54.
[5] Y. Liu *et al.*, "Lightchain: a Lightweight Blockchain System for Industrial Internt of Things," *IEEE Trans. Industrial Informatics*, vol. 15, no. 6, June 2019, pp. 3571–81.
[6] Y. Yu *et al.*, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, Dec. 2018, pp. 12–18.
[7] S. Huh, S. Cho, and S. Kim, "Managing IoT Devices Using Blockchain Platform," *Proc. 2017 19th Int'l Conf. Advanced Commun. Technology*, 2017, pp. 464–67.
[8] C. Xu *et al.*, "Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach," *IEEE Trans. Parallel and Distributed Systems*, vol. 30, no. 4, Apr. 2019, pp. 870–82.
[9] C. Xu, K. Wang, and M. Guo, "Intelligent Resource Management in Blockchain Based Cloud Data Centers," *IEEE Cloud Computing*, vol. 4, no. 6, Nov. 2017, pp. 50–59.
[10] P. H. Kuo, A. Mourad, and J. Ahn, "Potential Applicability of Distributed Ledger to Wireless Networking Technologies," *IEEE Wireless Commun.*, vol. 25, no. 4, Aug. 2018, pp. 4–6.
[11] H. Liu, Y. Zhang, and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Network*, vol. 32, no. 3, May/June 2018, pp. 78–83.
[12] H. Li *et al.*, "Trust-Enhanced Content Delivery in Blockchain Based Information-Centric Networking," *IEEE Network*, vol. 33, no. 5, Sept./Oct. 2019, pp. 183–89.
[13] M. Du *et al.*, "Big Data Privacy Preserving in Multiaccess Edge Computing for Heterogeneous Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 8, Aug. 2018, pp. 62–67.
[14] I. Eyal and E. G. Sierer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable"; https://arxiv.org/abs/1311.0243.
[15] Y. Liu *et al.*, "Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach," *IEEE Internet of Things J.*, vol. 7, no. 2, Feb. 2020, pp. 1273–86.

Biographies

MIAO DU is currently a research assistant in the College of Internet of Things, Nanjing University of Posts and Telecommunications (NJUPT), China. His current research interests include wireless sensor networks, social networks, security, game theory, smart grid communications, and cyber-physical systems.

KUN WANG [SM'17] received two Ph.D. degrees from NJUPTin 2009 and the University of Aizu in 2018. He was a postdoctoral fellow at the University of California Los Angeles (UCLA) from 2013 to 2015 and a research fellow at the University of Aizu in 2016. He is currently a research fellow at Hong Kong Polytechnic University and a professor at NJUPT. His research interests include big data, wireless communications and networking, energy Internet, and information security technologies.

YINQIU LIU is working toward an undergraduate degree in the College of Internet of Things, NJUPT. His current research interests include wireless communications, the Internet of Things, and blockchain.

KAI QIAN is a postgraduate student in information networks at NJUPT. His current research interests include network security, blockchain systems, big data, and th4 Internet of Things.

YANFEI SUN is a full professor with the School of Automation and School of Artificial Intelligence, NJUPT. He is also a director of the Jiangsu Engineering Research Center of HPC and Intelligent Processing, Nanjing, China. His current research interests are mainly in the areas of future networks, Industrial Internet, energy Internet, big data management and analysis, and intelligent optimization and control.

WENYAO XU received his Ph.D. degree from UCLA in 2013. He got both his M.S. degree in 2008 and his B.S. degree in 2006 (both with honors) from Zhejiang University, China. He is an associate professor with the Computer Science and Engineering Department at the State University of New York at Buffalo, where he founded and directs the Embedded Sensing and Computing (ESC) Group. He has published over 150 technical papers, co-authored 2 books and is a named inventor on many international and U.S. patents.

SONG GUO [SM'11, F'19] received his Ph.D. degree in computer science from the University of Ottawa. He was a professor with the University of Aizu, Aizuwakamatsu, Japan. He is a full professor with the Department of Computing, Hong Kong Polytechnic University. His research interests include big data, cloud computing and networking, and distributed systems with more than 400 papers published in major conferences and journals. He currently serves as an officer for several IEEE ComSoc Technical Committees and is ßethe Director of the ComSoc Board of Governors.

In a conventional blockchain transaction, when an asset is sent from one party to another, all of the transaction information is visible to other parties in the network. In contrast, in zero-knowledge transactions, others only know that a valid transaction has occurred, but the specific information cannot be obtained.