Securing Collaborative Environment Monitoring in Smart Cities Using Blockchain enabled Software-Defined Internet of Drones

Siyi Liao, Jun Wu, Jianhua Li, Ali Kashif Bashir and Wu Yang

***Abstract*—Internet of Drones (IoD) is a layered network control architecture, which is having a revolutionary impact on the monitoring and preserving of environment. Large-scale drone-assisted environmental monitoring can provide a better perspective and high-quality data by monitoring the operation of critical components of smart cities. However, as the continuous expand of IoD scale and the increase of multi-drone collaboration tasks, the large-scale drone-assisted service in smart cities monitoring will inevitably encounter the problem of relay and transfer of drone control. Lack of trust collaboration paradigm between drone controllers will bring huge security challenges to real-time monitoring of the environment, collaboration of tasks, data and location privacy of drones, etc. To address this important issue in IoD, this paper proposes a paradigm that uses smart contracts and blockchain to ensure trusted collaboration between controllers of software defined IoD (SD-IoD). First, we propose a novel SD-IoD architecture to enhance the support for heterogeneity and flexibility of IoD for the monitoring of environment. Second, we proposed a controller consortium blockchain for secure and efficient cooperation and interoperability of drone controllers, which includes a new cryptographic currency cooperation coin and a new consensus mechanism Proof-of-Security-Guarantee (PoSG). Third, we have designed a novel incentive mechanism to encourage controllers to maintain their own security and provide safer services to other controllers. The security analysis and performance simulation results indicate the effectiveness of the proposed mechanism.**

***Index Terms*—Environment monitoring, Software-Defined Internet of Drones (SD-IoD), blockchain, smart cities.**

I. Introduction

Efficient, real-time, and secure environment monitoring systems using the Internet of Drones (IoD) are becoming more and more important in nowadays smart cities. IoD is deeply integrated with smart cities in pollution monitoring, meteorological monitoring, traffic monitoring and other aspects. Due to the limited maneuverability and coverage of a single drone, large-scale environmental monitoring often requires secure and reliable coordination of multiple task drones. Therefore, the stability and trust cooperation of IoD are extremely dependent on complex control relationships and precise scheduling [1]. Meanwhile, the heterogeneity and complexity of the IoD system also relies on a more efficient and flexible network architecture to ensure its operation [2].

Software Defined Networking (SDN) focus on the isolation of control plane and data plane, greatly enhancing the support of the network for heterogeneity and flexibility [3]. The advantages of software-defined technology provide a suitable and reliable platform for complex drone-assisted applications of environment monitoring in smart cities. However, although the programmable network greatly improves the performance of the network, trusted service of different service provider still challenges the deployment of Software-Defined Internet of Drones (SD-IoD) [4].

Compared with public blockchains, consortium blockchains have advantages in terms of efficiency, cost, flexibility, and privacy protection [5]. The application of blockchain can realize distributed and trusted transactions, which are traceable and irreversible [6]. This provides opportunities for cross-vendor SD-IoD controller collaboration and interoperation, including the coordination of tasks between drones and the management of drones from different service providers by the controllers. Due to the decentralized and immutable characteristics of blockchain, the cooperation paradigm and security of different vendors can be guaranteed. The potential advantages of blockchain in terms of distribution provide a new perspective on the solution of drone-related technologies. Authors of [7] present a novel neural-blockchain-based drone-caching approach, designed to ensure ultrareliability and provide a flat architecture via blockchain. In [8], blockchain technology is used for the storage of collected data from the drones and update the information into the distributed ledgers to reduce the burden of drones.

Although some efforts have been made in combining blockchain with drone systems, there are still some major challenges remained [9] [10]. First, mechanisms for drone collaboration across service providers remain to be resolved. The further large-scale application of Unmanned Aerial Vehicle (UAV) systems requires the guarantee of a reasonable and efficient cooperation patterns. Second, Existing drone systems lack a blockchain mechanism suitable for drone scenarios. Due to its special characteristics, UAV systems need customized blockchain solutions in terms of security and energy supply. Third, SDN is deeply integrated with many specific applications, such as Internet of Vehicles (IoV) and Internet of Things

This work was supported in part by the National Natural Science Foundation of China under Grant 61972255 and 61831007.(*Corresponding author: Jun Wu.*)

Jianan Li, Jun Wu, and Siyi Liao are with Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China.(e-mail: junwuhn@sjtu.edu.cn)

Ali Kashif Bashir is with Department of Computing and Mathematics, Manchester Metropolitan University, UK, and School of Electrical Engineering and Computer Science, National University of Science and Technology, Islamabad (NUST), Islamabad, Pakistan.

Wu Yang is with Information Security Research Center, Harbin Engineering University, Harbin 150001, China.

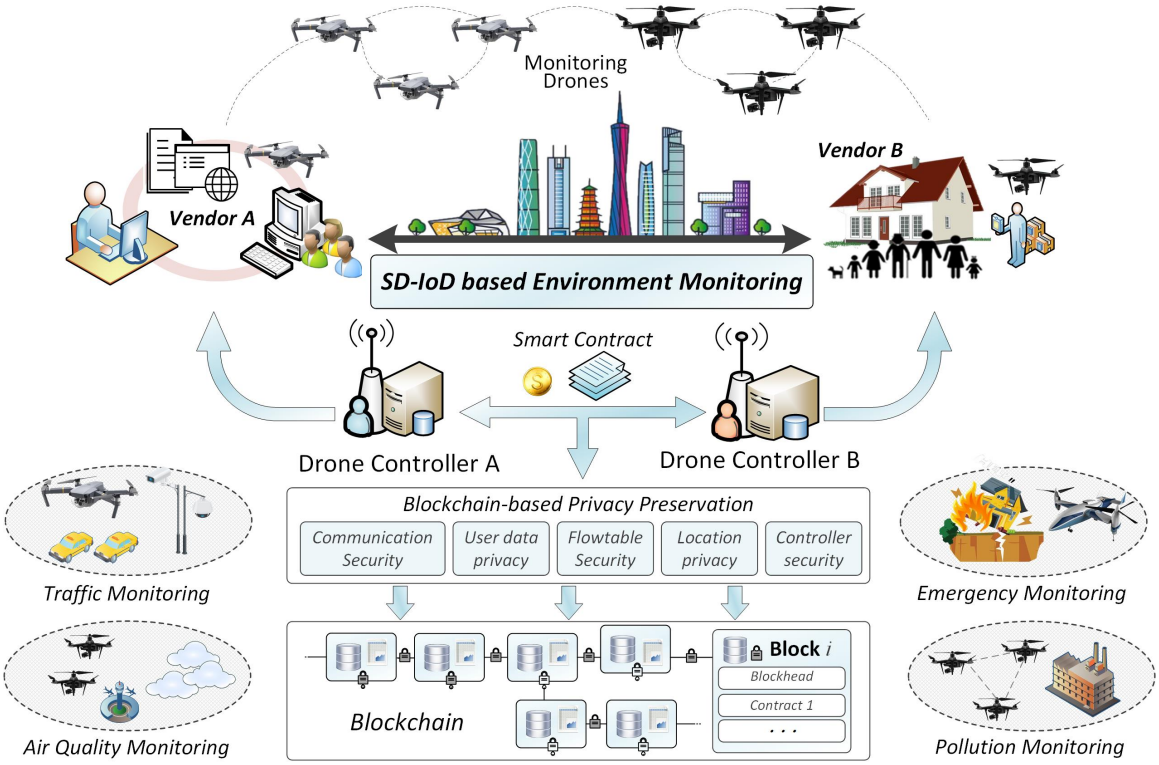


Fig. 1: The Application Scenario of the Environment Monitoring Using Software Defined Internet of Drones.

(IoT). But it does not yet have a paradigm for deep integration with drone systems.

The goal of this paper is to provide a detailed description of how blockchains can realize and guarantee the cooperation of controllers from different SD-IoD service providers for the monitoring of environment. Therefore, motivated by previous works, we exploit the blockchain technologies (consortium blockchain/consensus mechanism/smart contract) and SD-IoD monitoring and evaluation to achieve cross-vendor collaboration and interoperation in SD-IoD enabled smart cities [11] [12].

- We propose the SD-IoD monitoring architecture based on SDN for environment monitoring in smart cities, which is used for efficient multi-UAV collaborative, real-time environment monitoring and task collaboration.
- Based on the consortium blockchain, a novel mechanism for the secure cooperation of SD-IoD for the environment monitoring is proposed. Secure and reliable SD-IoD services are provided between different controllers, and smart contracts are written into the blockchain.
- A novel consensus mechanism Proof-of-Service-Guarantee (PoSG) and a new crypto-currency called Cooperation Coin (CC) are proposed to encourage and motivate the security services of each controller.

II. Application Scenario and Proposed Architecture

In this section, we introduced the application scenario of drone-assisted applications in smart cities monitoring, architecture and design principal of blockchain enabled SD-IoD.

A. Application Scenario

There are three parts in the application scenario as shown in Fig.1: task drones, drone controllers and blockchain. It shows a common mode of drone-assisted monitoring in smart cities. Controllers from different SD-IoD service providers work together to achieve large-scale drone-assisted services. The details of these three parts are illustrated as follows.

Cross domain task drones: In smart cities, there are often many drone service providers that provide large-scale drone-assisted services. Many applications in smart cities require multi-drone collaboration, e.g. large-scale drone delivery, real-time monitoring of traffic, daily surveillance of smart cities, etc. Task drones often need to be controlled by different controllers from various service providers.

Drone controllers: The main function of the drone controllers is to control the flight and positioning of the drone. They not only integrate into the existing SDN network, perform regular network communication and packet forwarding, but also guarantees the safety and stable operation of the SD-IoD. Based on blockchain, different drone controllers from various service providers can reach cooperative relationships through smart contracts to jointly ensure the safe scheduling and collaboration of the SD-IoD.

Blockchain: The smart contracts that have been formed in the past are stored in the blockchain to ensure the safe and stable operation between the drone controllers. The new cooperation agreement reached between the controllers is packaged into new blocks and added to the existing blockchain. As shown in Fig.1, drone controllers are widely deployed and

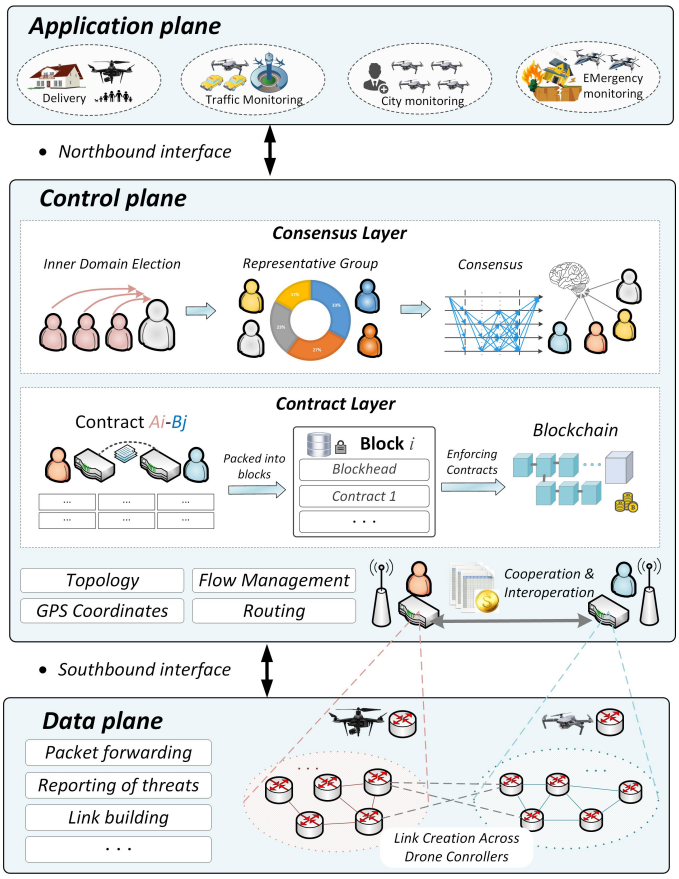


Fig. 2: Architecture of Software Defined Internet of Drones.

are deeply integrated with smart cities. In order to achieve full flexibility and scalability of SD-IoD, controllers from different drone-assisted service providers implement full trust and interoperability by smart contracts. The smart contracts are not only related to the specific details of the drone service, but also requires the security resources provided by the controllers of both parties. The controllers that form a collaborative relationship using blockchain will jointly protect the privacy of drone-related services, e.g. user data privacy, drone location privacy, flowtable security, etc.

B. Proposed SD-IoD Architecture

According to the specific scenarios of large-scale drone applications, we propose the basic architecture of SD-IoD shown in Fig.2 based on the SDN architecture. The specific functions of each plane are described as follows.

Application plane: The application plane contains a variety of drone-assisted applications, e.g. UAV delivery, drone-assisted traffic monitoring system, drone disaster relief in emergency situations, etc. SD-IoD users do not need to care about the technical details of the underlying equipment, and can quickly deploy new applications through task publication. Although the underlying devices may come from different SD-IoD service providers, users at the application plane do not need to consider their collaboration and interoperability issues.

Control plane: The control plane contains relatively centralized drone controllers that are responsible for maintaining the network view and running control strategies. Control collaboration and interoperability across service providers are mainly achieved on this plane. Each drone service provider manages multiple drone controllers and task drones. Drones belonging to the same service provider can easily achieve collaboration, interoperation and scheduling. Collaboration between drones and related equipments, especially drones from different service providers, need to be realized by the consensus layer and the blockchain layer. The blockchain layer mainly implements the construction of the consortium blockchain, while the consensus layer mainly implements the operation of the PoSG proposed in this paper.

(1) Blockchain layer: Due to the large number of drone controllers in SD-IoD, adding them all to the blockchain will bring large unnecessary costs and reduce the system efficiency. Therefore, the consortium blockchain has become a solution to replace the traditional blockchain. The consortium blockchain has the advantages of greater controllability and faster transaction speed, and is more suitable for SD-IoD scenarios. For controllers from the same service provider, part of the controllers are elected as representatives based on the security status and resources in order to form a consortium blockchain. Due to the advantages of consortium blockchain in speed, energy consumption, and computing cost, it is suitable for drone systems that require fast response. New contracts generated over a period of time are packaged into a block and added to the current blockchain, enabling automatic execution, non-tampering, and easy traceability.

(2) Consensus layer: In the mechanism we designed, each drone service provider elects some trusted nodes as representatives to participate in the consensus process of the blockchain. The representatives elected by each service provider jointly guarantee the trusted cooperation between different controllers through a consensus mechanism. In each time period, the nodes participating in the consensus will elect the block verifier and the backup verifiers to verify the effectiveness of the smart contracts. The validator will receive a portion of the smart contract transaction amount as reward. The proposed cryptocurrency and consensus mechanism will be introduced in detail in section III.

As the core of the entire SD-IoD architecture, control plane not only completes the traditional SDN control functions, but also exercises the control scheduling of underlying task drones. Besides, the drone controller also provides navigation and energy supply related services for the drones it controls.

Data plane: The data plane is composed of network devices such as switches from different providers and various task drones. The communication equipment is mainly responsible for basic SDN functions such as data forwarding. The task drone obtains instructions from the controller through the southbound interface and cooperates to complete the tasks issued by the upper-layer equipment. Devices of data plane also regularly report the view and topology to the controllers.

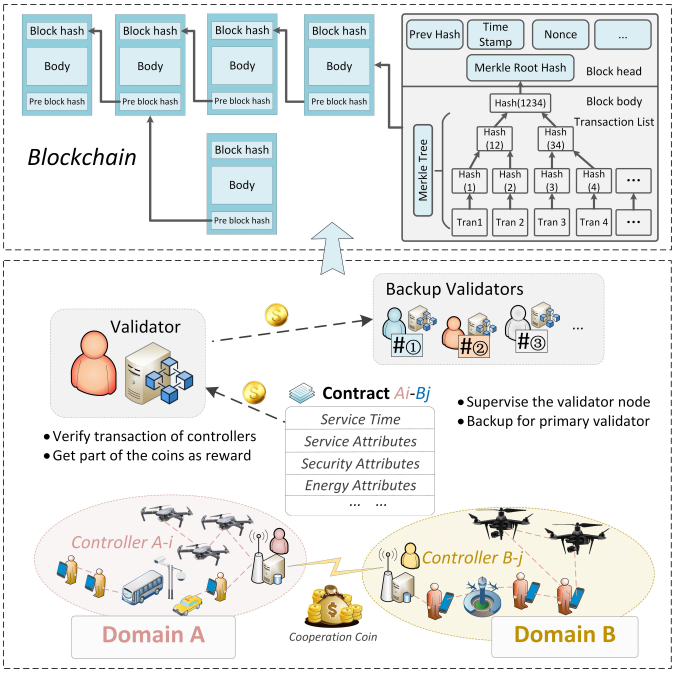


Fig. 3: Blockchain enabled Cooperation Coin.

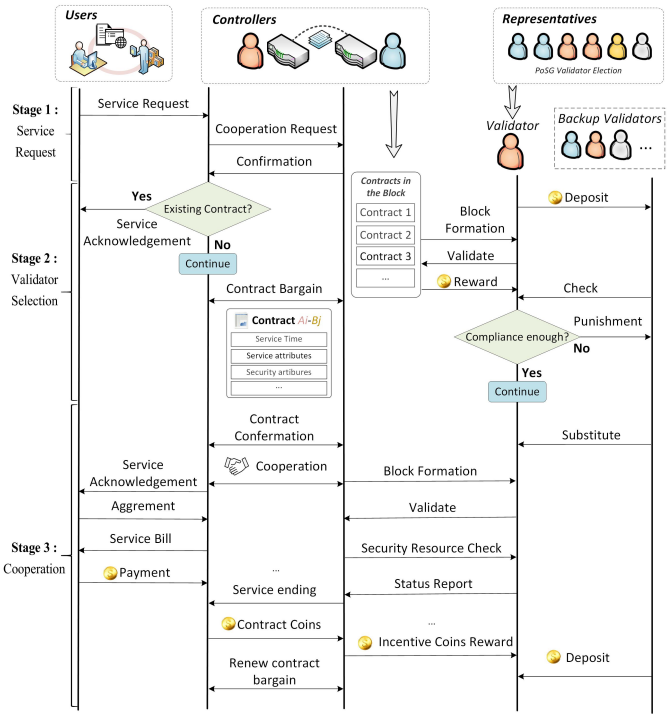


Fig. 4: Workflow of the Blockchain-based SD-IoD.

III. Proposed Cooperation Coin and Proof-of-Security-Guarantee

A. Blockchain-empowered Cooperation Coin

As shown in Fig.3, we assume that controllers $A-i$ and $B-j$ (controller i from drone service provider A and controller j of service provider B) that do not form a trust relationship need to achieve task coordination. The two parties form smart contracts based on the resources and services provided to each other. The contents of the contract include: the agreed service period, the contract amount of the two parties, the details of the security services provided by the other party, the energy protection required for the drone, etc. The elected validator needs to verify the transaction execution process of the contract. As a bonus, it can get a portion of the contract amount signed by both parties. In addition, in order to prevent selected contract verifiers from failing to fulfill their obligations, we have also designed a backup verifier mechanism to monitor the verifiers. Before a representative becomes a validator, it needs to pledge some cooperation coins to the backup validators. The deposit is refunded after the validator has verified all transactions. If the amount of the deposit is greater than the potential benefits that the verifier may get from the transaction, it can effectively restrict the behavior of the verifier. The specific workflow of the PoSG is shown in the following Fig.4.

Stage 1 Users of the application plane have released drone services that require multi-controller collaboration, that is, they publish business to the underlying controllers. Therefore, the drone controllers participating in the service request a cooperative relationship with each other and negotiate a contract.

Stage 2 The block validator first pays a deposit to the backup validators, and the backup validators monitor whether the behavior of validator is legal. The selected validator verifies whether the transaction in the block is valid and gets a portion of the operation coin as reward. If the verifier fails to perform its duties, the first backup validator becomes the validator.

Stage 3 After the validator has verified all the transactions in the block, the backup validators return the deposit. All the controllers in the block who signed the smart contract have also reached a cooperation agreement to ensure the safe operation of their control equipment. The controllers settle the cooperation coin according to the smart contracts they signed.

In the mechanism we designed, the cooperation between controllers and the signing of smart contracts need to be completed by cooperation coin. This means that cooperation coin is a medium for obtaining services and security from other service providers. On the other hand, only the elected representatives have the opportunity to become the validator and further receive coins from the smart contract. Therefore, the controllers in the same consortium will try to meet and improve the security indicators. The cooperation coin can be used to purchase the security services from the controllers of other providers to achieve multi-party trusted cooperation. Therefore, only by improving the security guarantee provided by the controller for the task drones, the controller will have a higher probability to obtain block verification rights and obtain cooperation coins as reward.

B. Proof-of-Security-Guarantee Consensus Mechanism

Controllers from different service providers elected several representatives. Suppose there are service providers $\mathbb{V} = \{A, B, C, D, ...\}$ each provider's controllers form an consortium group, electing representative controllers, represented as

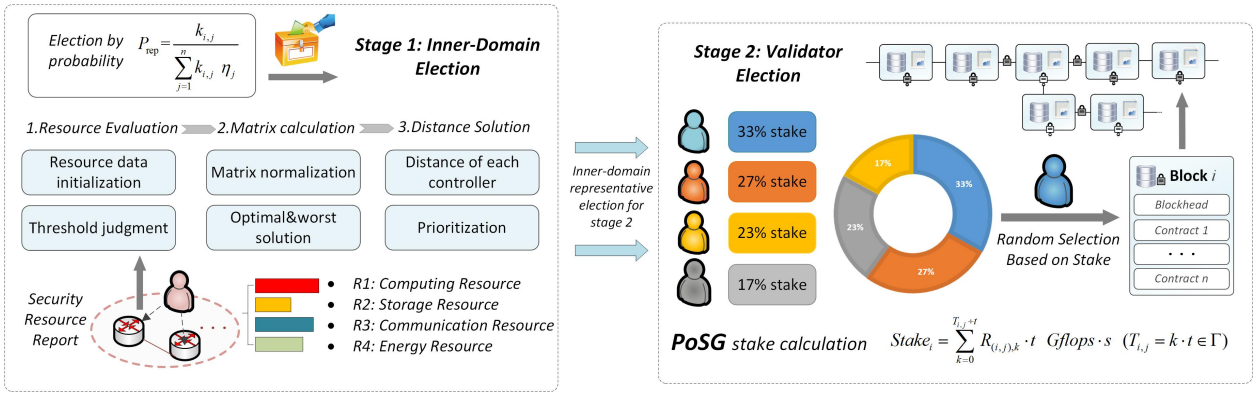


Fig. 5: Proposed Proof-of-Service-Guarantee Consensus Mechanism.

$\mathbb{R} = \{(A_1, A_2, \cdots, A_3), (B_1, B_2, \cdots, B_j), \cdots\}$. The principle of election is to give higher probability to controllers with higher security indicators. Therefore, our goal is to design a distributed transaction validator election mechanism for $r \in \mathbb{R}$ from different $v \in \mathbb{V}$, in order to ensure trusted cooperation between cross-provider controllers. The elected transactions validator V^* and backup validators is selected by probability based on the consensus mechanism Proof-of-Service-Guarantee (PoSG) we designed.

The PoSG proposed in this paper is an improvement of the traditional Delegated-Proof-of-Stake (DPoS), which is giving a higher probability of nodes with better security evaluation results to obtain the right to record blocks. Fig.5 shows the basic idea of PoSG consensus mechanism. In the PoSG, we assume that the controller will provide multiple resources to ensure the safe operation of the drone, including computing resources, communication resources, energy and storage resources. Therefore, we need to comprehensively measure the multiple aspects of security resource of a drone controller. On the other hand, in order to ensure the multi-aspect security of SD-IoD, a certain amount of computing resources must be guaranteed. Each resource must meet the minimum threshold to participate in the election. For the controller j of provider i, whether a controller can participate in the election of a representative should be determined by its minimum resources, which is $R_{i,j} \geq R_{threshold}$. The process of PoSG is mainly divided into two steps. The first step is the election of representatives within the domain of each drone service provider. The second step is the election of validator and backup validators from representatives of different service providers.

Stage 1: Inner-Domain Election

Through resource evaluation, we can get all the nodes participating in the inner-domain election. But the various security resources need to be measured in a uniform way. Therefore, Technique for Order Preference by Similarity to an Ideal Solution (TOPSIS) is used to sort the safety resources of the controller. For all nodes participating in the representative election in the consortium, we construct the resource matrix X according to the different resource of the controllers.

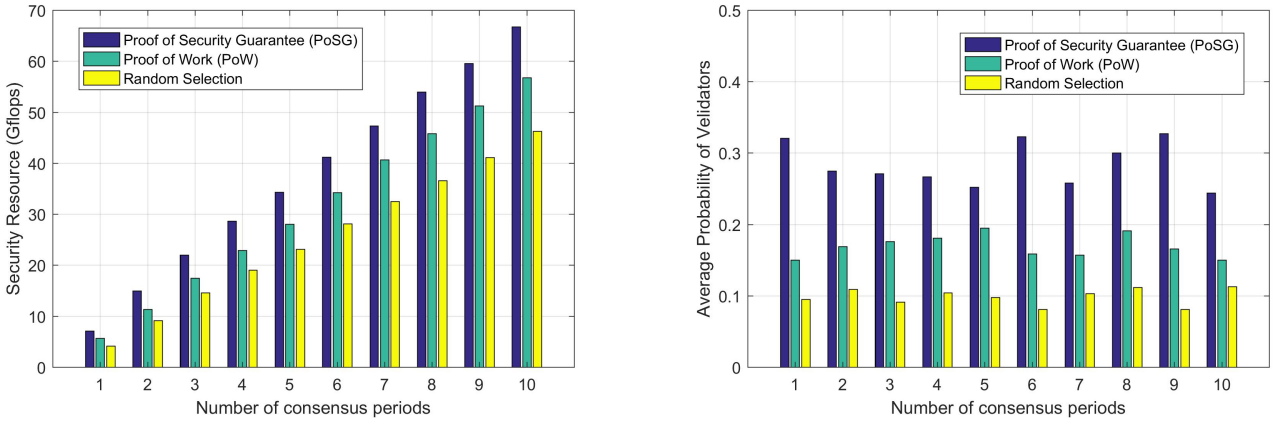
However, the above resource matrices are absolute values of resources, not relative values used for resource evaluation. So we normalize the matrix into $A_{m\times n} = (a_{ij})_{m\times n}$ and $a_{ij} = x_{ij}/\sqrt{\sum_{i=1}^{n} x_{ij}^2}$. For the matrix $A_{m\times n}$, we take the best solution and the worst solution to its columns, which is $A^+ = (max(a_{i1}), \cdots, max(a_{in}))$ and $A^-(min(a_{i1}), \cdots, min(a_{in}))$. In this way, we can get the distance between the various resources of each controller and the optimal solution and the worst solution as $S_i^+ = \sqrt{\sum_{i=1}^{n} \omega_i (a_{ij} - a_j^+)^2}$ and $S_i^- = \sqrt{\sum_{i=1}^{n} \omega_i (a_{ij} - a_j^-)^2}$. So based on the above distance we can calculate the weight of each controller as $Z_i^* = s_i^-/(s_i^+ + s_i^-)$ This distance Z represents the relative situation between various aspects of the controller's resources and other controllers participating in the election. A larger value indicates that the comprehensive situation of each aspect is closer to the optimal solution, otherwise it is closer to the worst solution.

Stage 2: Election of Validators

In our mechanism, the controller with stronger security resources will have a greater chance to represent its own vendor. Therefore, according to the weight of each controller obtained by the above method, the probability that each controller becomes a representative is as $Prep_j = k_{i,j}/(\sum_j k_{i,j} \cdot \eta_j)$. $\eta_j = 1$ for all the controllers that satisfy the minimum resource threshold condition, otherwise, $\eta_j = 0$. According to this probability, each controller can only select a part of the representative at most. Let us record this ratio as $\tau\%$. So each vendor can only elect at most $v_i \cdot \tau\%$ representatives. After a representative is elected, each node conducts election of validators according to the time maintained by its secure resources. It is measured as $k_{i,j} = \sum_{k=0}^{T_{i,j}/t} R_{(i,j),k} \cdot t$ Gflops. $T_{i,j} = k \cdot t \in \mathbb{T}$, where t denotes the basic time period of service contract signing in this mechanism and T has an upper limit. Therefore, we can get the probability that each representative becomes the final block verifier as follows $P_{i,j} = k_{i,j}/(\sum_i \sum_j k_{i,j} \cdot \delta_{i,j})$. Based on the above probability, we can guarantee that nodes with stronger resources have a greater probability to become validators or backup validator.

IV. Simulations

In this section, we describe the superiority of the PoSG mechanism we designed in detail through simulation experiments. We compared the designed consensus mechanism with traditional Proof-of-Work (PoW) and the method that



(a) Comparison of security resources of selected validator

(b) Probability comparison of nodes becoming validators

Fig. 6: Comparison of node parameters under different consensus mechanisms

randomly select validator. Traditional PoW mainly relies on consuming computing resources to calculate SHA-256. The miner constantly constructs block data and checks whether the result of each calculation meets the workload, thereby determining whether the block meets the network difficulty. We set up 5 different drone service providers and 200 drone controllers belonging to them respectively for this simulation experiment. Each drone provider selects t = 10 controller as a representative to participate in the consensus process of PoSG. We select 1 validator and 9 backup validators for the controllers participating in PoSG. And each validator has a probability of p = 0.1 to not perform its duties, and is replaced by a backup validator. We measure the comprehensive safety resources that a controller can provide by 1)computing resources, 2)communication resources, 3)storage resources and 4)energy resources. Our main evaluation index is the security resources of the selected validator, and the probability that a controller with strong security resources becomes the validator. The specific simulation experiment results are shown in the following two figures.

We first evaluated the cumulative security resources of selected validator over time. As shown in Fig.6, the proposed PoSG mechanism has significantly stronger security resources than the other two methods. Since the two stages of PoSG elections mainly consider the security resources of the controller, the validators elected in each time period are relatively strong security resources. PoW election is mainly based on the speed at which it calculates SHA-256. The validator elected by PoW may not have strong security resources, but it is still superior to the method of randomly selecting validator.

We not only evaluated the PoSG mechanism from the perspective of the validator, but also evaluated the probability of a controller with strong security resources becoming a validator. As shown in Fig.7, we simulated the average probability that the top 10 percent of controllers with strong security resources will become validator under the three mechanisms. We can clearly see that the probability that a controller with strong security resources in the PoSG mechanism becomes a validator is significantly higher than the other two mechanisms. Since the PoW mainly relies on computing resources, it can also select some nodes with strong security resources. And the probability that the top 10 controllers in the randomly selected way become validators is also around 10.

V. Open Issue

Inspired by the advantages of the blockchain and IoD, several future open issues that worthy of further study are summarized as follows:

Energy efficient monitoring in 5G enabled drone system: Due to the limitations of battery technology and the characteristics of drones, the energy reserve of drones has become a short board in large-scale IoD services [13]. Therefore, energy efficient drone system for environment monitoring has become an important issue to be resolved. The improvement of the drone energy system can greatly promote the task scheduling efficiency of the drone and expand its service range.

Secure data delivery and collection of drone system: Due to the energy, volume, and weight limitations of drone systems, drone equipment often uses lightweight solutions in communications and security [14]. However, drone systems are often an important part of data delivery and collection, e.g. real-time video streaming, monitoring, etc. Therefore, how to ensure the safe transmission of data from drones in communication systems deserves further attention.

Collaboration and scheduling scheme for multi-drone montoring: Environment monitoring in smart cities often requires the collaboration of multiple drones [15]. How to reasonably schedule drones with a single function or weak capabilities and quickly respond to the demand for drone-assisted services remains an open issue.

VI. Conclusion

This paper focused on realizing the trust and efficient drone-assisted collaboration by using software defined technologies and blockchain for the environment monitoring of smart cities. Based on the consortium blockchain, a SD-IoD

architecture is proposed for the environment monitoring of smart cities. For the secure cooperation and interoperation of the SD-IoD controllers, this paper proposed a novel consensus mechanism PoSG. The security analysis and performance simulation showed the superiority and effectiveness of the SD-IoD architecture and PoSG mechanism.

REFERENCES

[1] S. H. Alsamhi, O. Ma, M. S. Ansari and F. A. Almalki, "Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities," in IEEE Access, vol. 7, pp. 128125-128152, 2019.

[2] Q. Fan and N. Ansari, "Towards Traffic Load Balancing in Drone-Assisted Communications for IoT," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3633-3640, April 2019.

[3] M. Alharthi, A. M. Taha and H. S. Hassanein, "An Architecture for Software Defined Drone Networks," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-5.

[4] A. Chowdhary, D. Huang, A. Alshamrani, M. Kang, A. Kim and A. Velazquez, "TRUFL: Distributed Trust Management Framework in SDN," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.

[5] M. Belotti, N. Boi, G. Pujolle and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3796-3838, Fourthquarter 2019.

[6] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019.

[7] S. Aggarwal, M. Shojafar, N. Kumar and M. Conti, "A New Secure Data Dissemination Model in Internet of Drones," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.

[8] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina and K. R. Choo, "Neural-Blockchain-Based Ultrareliable Caching for Edge-Enabled UAV Networks," in IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5723-5736, Oct. 2019.

[9] T. Rana, A. Shankar, M. K. Sultan, R. Patan and B. Balusamy, "An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 162-167.

[10] T. Li, J. Ma, Q. Pei, C. Ma, D. Wei and C. Sun, "Privacy-Preserving Verification and Root-Cause Tracing Towards UAV Social Networks," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.

[11] S. Mumtaz, A. Bo, A. Al-Dulaimi and K. Tsang, "Guest Editorial 5G and Beyond Mobile Technologies and Applications for Industrial IoT (IIoT)," in IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2588-2591, June 2018, doi: 10.1109/TII.2018.2823311.

[12] X. Cheng, Y. Wu, G. Min, A. Y. Zomaya and X. Fang, "Safeguard Network Slicing in 5G: A Learning Augmented Optimization Approach," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 7, pp. 1600-1613, July 2020, doi: 10.1109/JSAC.2020.2999696.

[13] M. B. Ghorbel, D. Rodrguez-Duarte, H. Ghazzai, M. J. Hossain and H. Menouar, "Joint Position and Travel Path Optimization for Energy Efficient Wireless Data Gathering Using Unmanned Aerial Vehicles," in IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2165-2175, March 2019.

[14] Y. Chen and L. Wang, "Privacy Protection for Internet of Drones: A Network Coding Approach," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1719-1730, April 2019.

[15] D. Wang, P. Hu, J. Du, P. Zhou, T. Deng and M. Hu, "Routing and Scheduling for Hybrid Truck-Drone Collaborative Parcel Delivery With Independent and Truck-Carried Drones," in IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10483-10495, Dec. 2019.

Siyi Liao received the B.S. degree from School of Electronic Information Engineering in Beijing Jiao Tong University, Beijing, China, in 2017. Now, he is a candidate Ph.D. at School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. His research interests are focusing on Multi-access Edge Computing (MEC), Internet of Vehicles (IoV), etc. He is a student member of IEEE.

Jun Wu received the Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He was a Post-Doctoral Researcher with National Institute of Advanced Industrial Science and Technology (AIST), Japan, from 2011 to 2012. He was a Researcher with the Global Information and Telecommunication Institute, Waseda University, Japan, from 2011 to 2013. He is currently a professor and the vice dean of Institute of Cyber Science and Technology, Shanghai Jiao Tong University, China. His research interests include security and artificial intelligence of IoT.

Jianhua Li got his BS, MS and Ph.D. degrees from Shanghai Jiao Tong University, in 1986, 1991 and 1998, respectively. He is currently a professor/Ph.D. supervisor of School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. He was the chief expert in the information security committee experts of National High Technology Research and Development Program of China (863 Program) of China. He got the Second Prize of National Technology Progress Award of China in 2005.

Ali Kashif Bashir is a Senior Lecturer at the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. He is also with School of Electrical Engineering and Computer Science, National University of Science and Technology, Islamabad (NUST), Islamabad, Pakistan. He is a senior member of IEEE and Distinguished Speaker of ACM. His research interests include internet of things, wireless networks, distributed systems, network/cyber security, cloud/network function virtualization, etc. He is serving as the Editor-in-chief of the IEEE FUTURE DIRECTIONS NEWSLETTER.

Wu Yang received the Ph.D. degree in computer system architecture specialty from the Computer Science and Technology School, Harbin Institute of Technology. He is currently a Professor and a Doctoral Supervisor with Harbin Engineering University. His main research interests include wireless sensor networks, peer-to-peer networks, and information security. He is a member of ACM and a Senior Member of CCF.

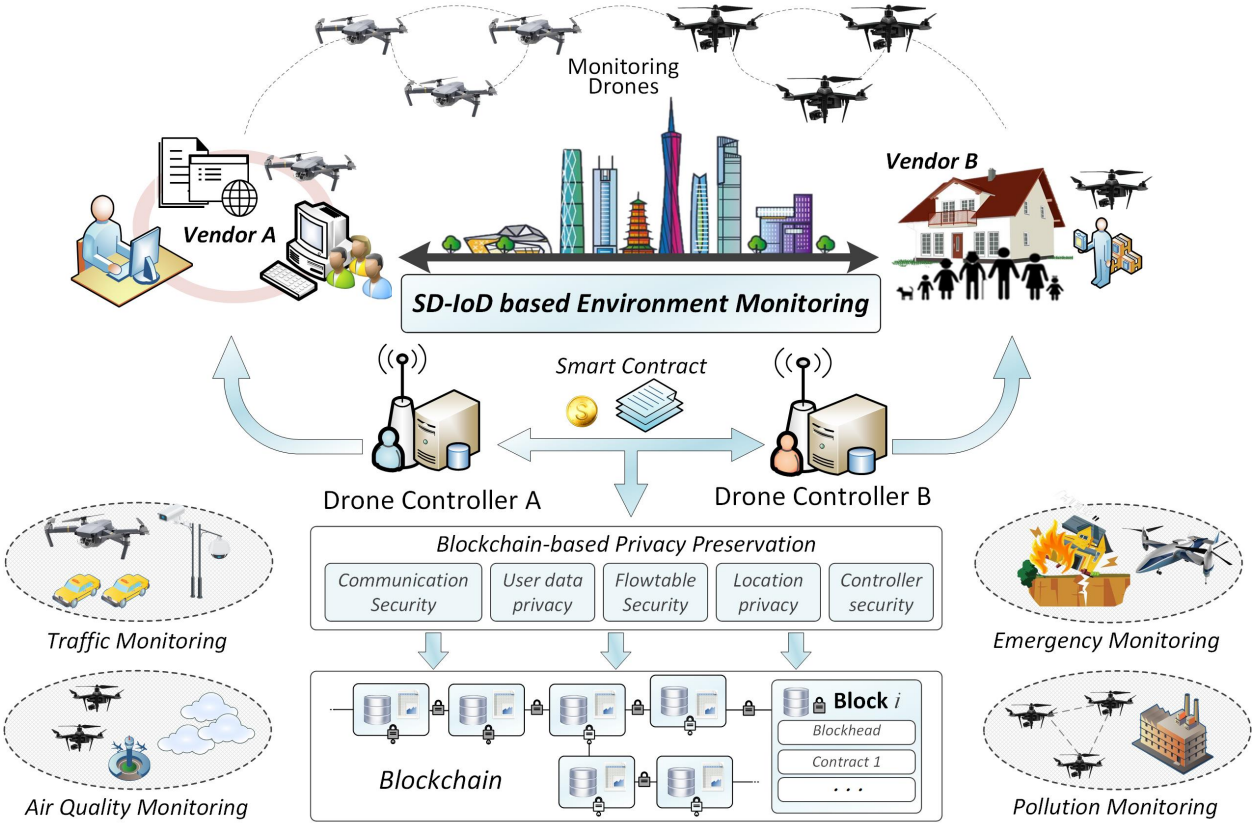


Fig. 1: The Application Scenario of the Environment Monitoring Using Software Defined Internet of Drones.

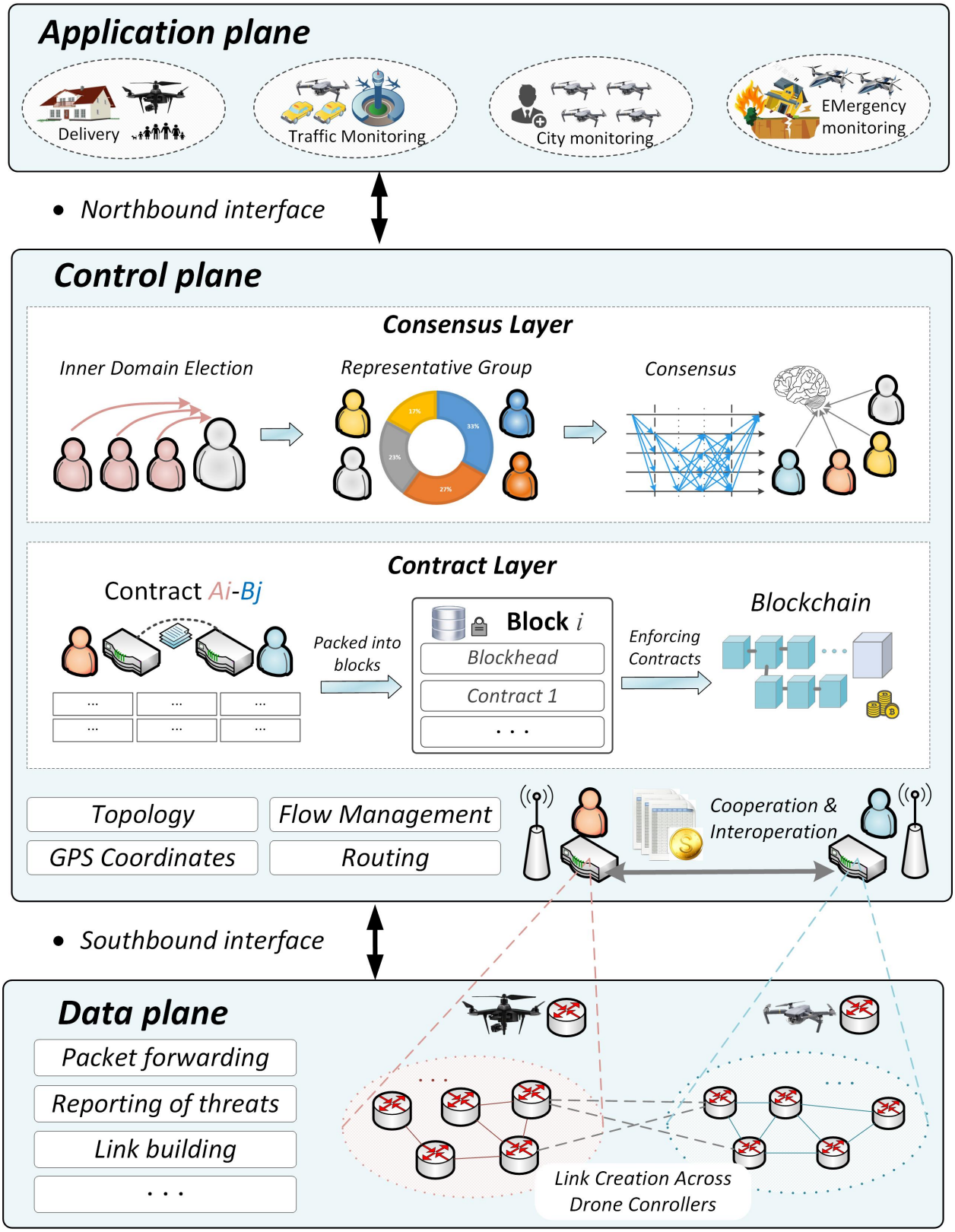


Fig. 2: Architecture of Software Defined Internet of Drones.

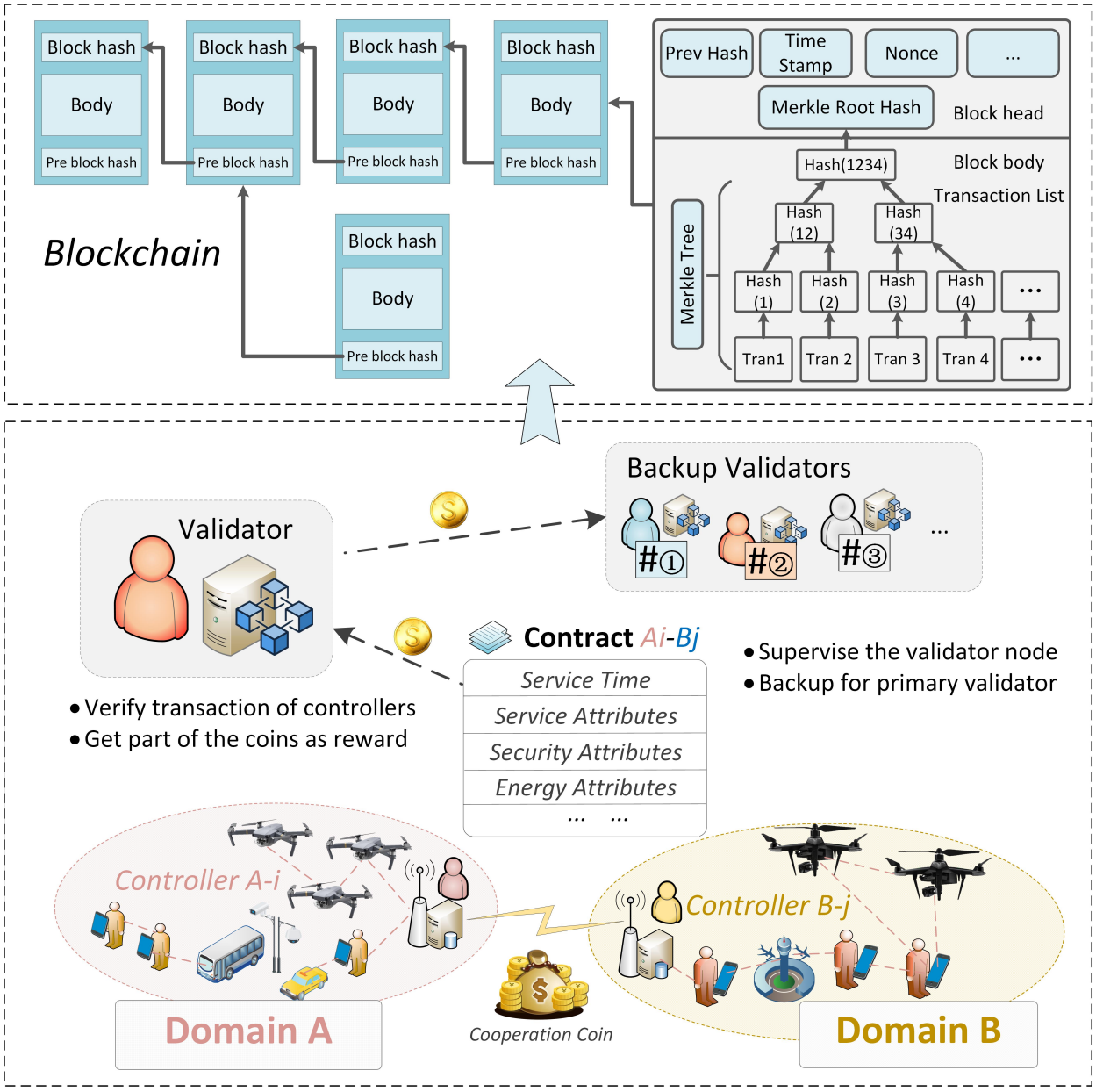


Fig. 3: Blockchain enabled Cooperation Coin.

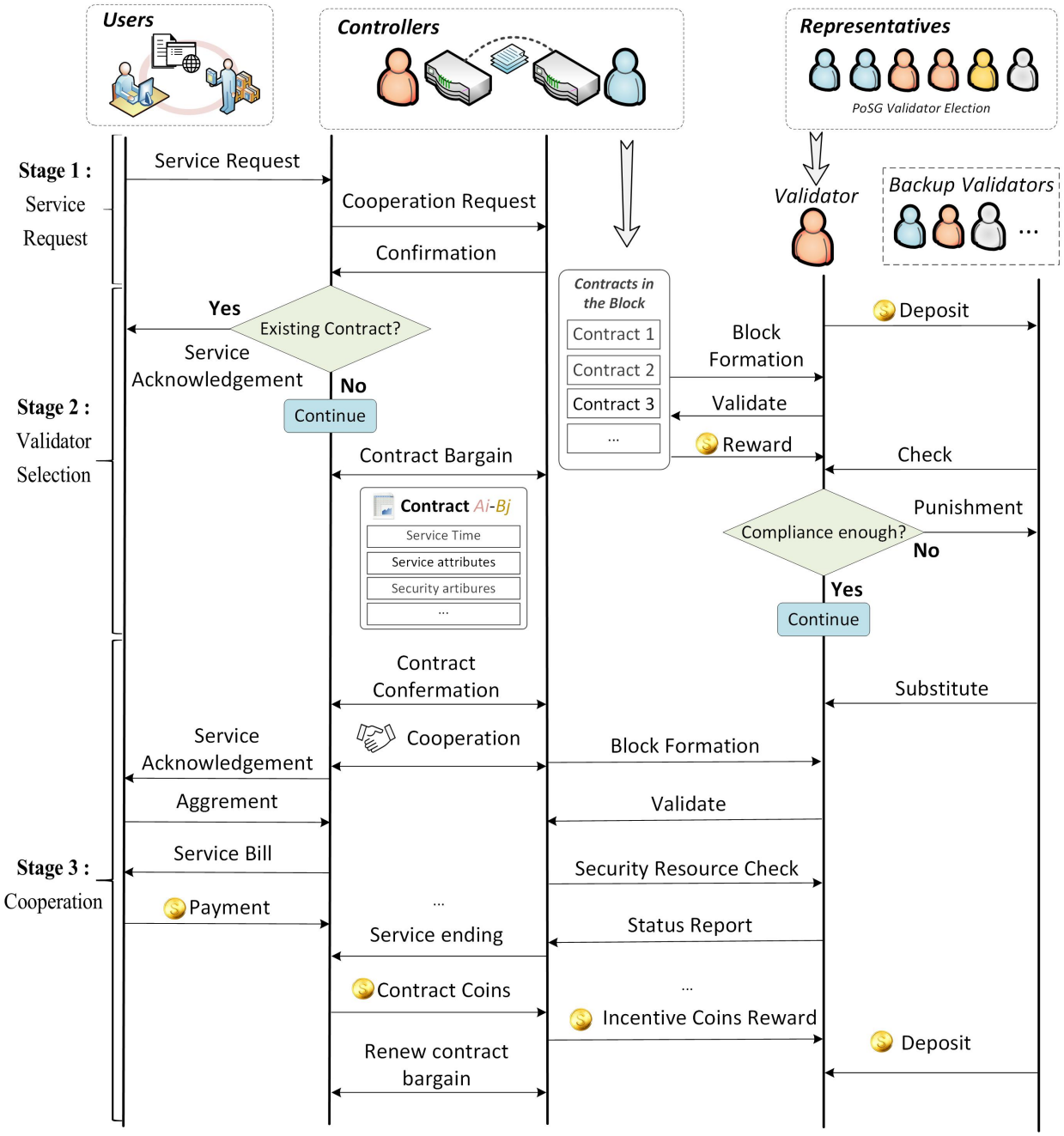


Fig. 4: Workflow of the Blockchain-based SD-IoD.

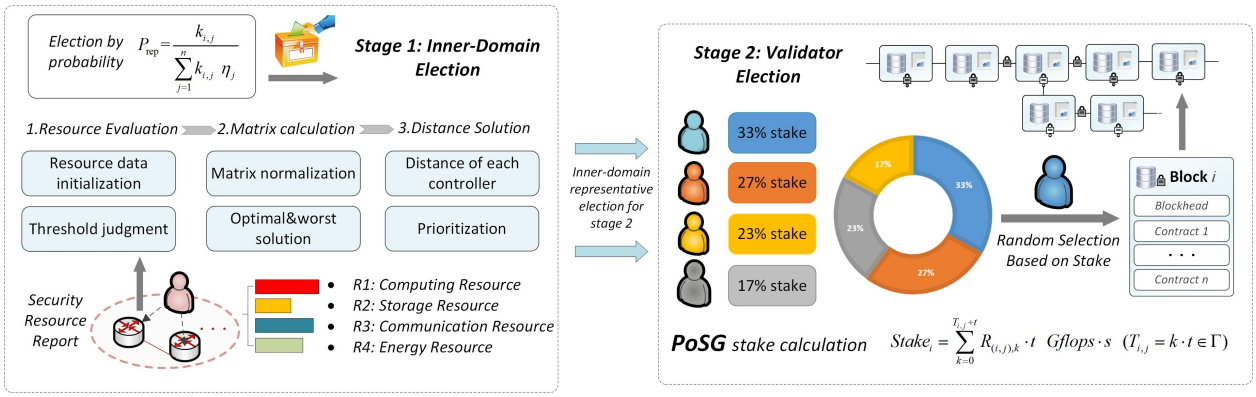
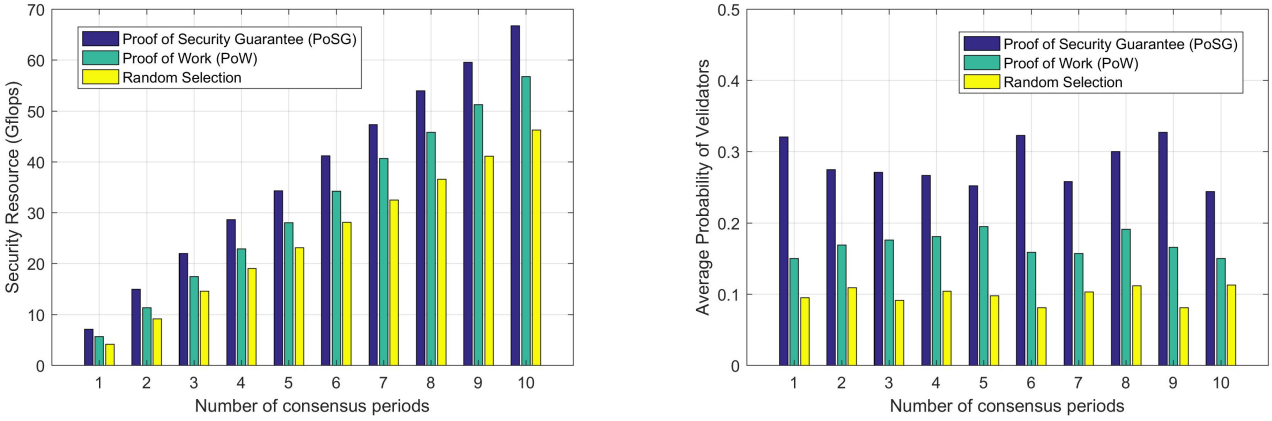


Fig. 5: Proposed Proof-of-Service-Guarantee Consensus Mechanism.



(a) Comparison of security resources of selected validator

(b) Probability comparison of nodes becoming validators

Fig. 6: Comparison of node parameters under different consensus mechanisms