Internet of Things and Cyber-Physical Systems 3 (2023) 52–60

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems

Consensus mechanism for software-defined blockchain in internet of things

Ruihang Huang [a,*], Xiaoming Yang [a], P. Ajay [b]

[a] Donghua University, Shanghai, China
[b] Faculty of Information and Communication Engineering, Anna University, Chennai, India

ARTICLE INFO

Keywords:
Internet of things
Smart blockchain
Software definition
Consensus mechanism
DPOS-PBFT

ABSTRACT

This article aims to discuss the consensus mechanism of software-defined blockchain in the Internet of Things, analyze the characteristics of the traditional consensus mechanism algorithms, on the basis of comparing the advantages of each model, the traditional consensus mechanism algorithm is improved. Later, a supervisable consensus scheme based on improved DPOS-PBFT (Delegated proof of stake-Practical Byzantine Fault Tolerance) was proposed. In the context of the development of the Internet of Things technology, the decentralized distributed computing paradigm is used to improve the blockchain smart contract technology, and the DPOS blockchain consensus mechanism is optimized based on the DPOS protocol of the credit model. In addition, through the dynamic grouping algorithm of credibility, the research ranks the credit level of the consensus nodes of the blockchain network, thus further realizing the supervision of the Internet of Things system. The results of the case analysis show that the success rate of the mechanism algorithm can still be maintained at about 97% after 3000 user requests, the maximum delay remains below 8s after 3000 user requests, the minimum delay is always around 3s, the average delay is 2.38s, the overall performance of the algorithm is superior. It can ensure the final consistency of data transmission of each node in the Internet of Things, the research on the blockchain consensus mechanism in the Internet of Things has practical reference value.

1. Introduction

With the development of physical network technology, Bitcoin [1] As a new encrypted digital currency, it began to be used in the field of financial security and widely used in the supply chain, as the underlying technology to realize Bitcoin virtualization, Blockchain technology has begun to attract people's attention. The essence of blockchain is a decentralized distributed database, as an emerging technology, Blockchain provides users with a reliable exchange trading platform with its own advantages such as autonomy, synchronicity, and anonymity, provide data integrity to ensure the authenticity of content and user transparency. In the budding period of the development of blockchain [2–4], as the bottom layer of Bitcoin, the application of blockchain is only limited to the use of mathematical methods to calculate and maintain the recorded data of the distributed ledger that will not be tampered with. With the continuous development of blockchain technology, it began to be gradually applied to stocks and bonds in the financial field. In transactions, people introduce "smart contracts" through programs and algorithms, apply blockchain technology to ensure the integrity and reliability of financial transactions. In the current stage of development, Blockchain technology has entered a period of rapid development, the development of technologies such as big data [5] and artificial intelligence [6] has brought about changes in Internet technology, the IoT solution of the autonomous self-organizing network has gradually penetrated into all aspects of social life. The connection between the Internet of Things and advanced technologies such as big data and artificial intelligence is constantly deepening.

As a decentralized distributed computing paradigm, Blockchain integrates cryptography, smart contract [7] (Smart contract), P2P (peer--to-peer) network [8], consensus Mechanism [9] (Consensus Mechanism) and other technologies, using a chained data structure to arrange the data blocks in chronological order, the consensus mechanism is the core of the entire blockchain system. Due to the inherent data divergence that may occur in a decentralized environment, lead to mistrust of the transmitted data, a suitable consensus mechanism can dynamically coordinate the data of each node, ensure the final consistency of the data of each node [10]. The traditional consensus mechanism algorithm has many defects, for example, the POW (Proof of Work) algorithm has a certain degree of waste of resources, and the system has performance bottlenecks [11]; The POS (Proof of Stack) consensus mechanism relies too much on coin

* Corresponding author.
E-mail address: 1209125@mail.dhu.edu.cn (R. Huang).

https://doi.org/10.1016/j.iotcps.2022.12.004
Received 31 May 2022; Received in revised form 12 December 2022; Accepted 28 December 2022
Available online 29 December 2022

age and equity, excessive centralization of resources leads to low throughput [12]; Practical Byzantine Fault Tolerance (PBFT) adopts C/S distributed mode (c/s Distributed Mode), there is a lack of research on the scalability of P2P networks [13]. In summary, in the IoT system, it is particularly important to design the consensus mechanism of the blockchain in combination with specific application scenarios. However, the existing consensus mechanisms are inefficient, unsupervised, and lack of consistency, and other problems are difficult to solve, to solve these problems, a supervisable consensus mechanism based on improved DPOS-PBFT (Delegated proof of stake-Practical Byzantine Fault Tolerance) is proposed. The innovation of the consensus mechanism lies in the combination of DPOS (Delegated proof of stake) and PBFT (Practical Byzantine Fault Tolerance) two consensus mechanisms, both can use the advantages of DPOS to solve the problem of regulatory efficiency, the characteristics of the PBFT consensus mechanism can be used to solve the problem of data consistency with minimal resource consumption. The consensus mechanism proposed by the research can simultaneously guarantee the security of anti-collusion attacks between nodes and the efficiency of transaction consensus, it has practical reference value for the research of blockchain consensus mechanism and the intelligent development of the Internet of Things in the future.

2. Recent related research

2.1. The blockchain smart contract technology

In recent years, the Internet of Things technology continues to develop and innovate, and the research on Internet of Things technology and blockchain smart contract technology has attracted widespread attention. For example, Xiong et al. (2019) [14] studied the data transaction mode of blockchain based on smart contracts, utilizing the tamper-proof and traceability of the blockchain and the programmability of smart contracts to propose a challenge response mechanism between data buyers and data owners, the automatic payment using Ethereum cryptocurrency between transaction participants is realized. Liu et al. (2019) [15] studied the elasticity and cost-effective data carrier architecture of smart contracts in the blockchain, the proposed system does not need to pre-define data format standards in the IoT environment that supports blockchain, it can effectively reduce the deployment cost of each smart contract. Xuan et al. (2020) [16] Research on the incentive mechanism of data sharing based on blockchain and smart contracts, the results show that Blockchain 2.0 with smart contracts has the natural advantages of being able to achieve trust and automatic transactions among a large number of users. Lv(2020) [17] Research on the security performance of edge devices of the Internet of Things, start with the edge devices of the Internet of Things, research the centralized distributed hit rate and average corresponding speed of edge nodes. At the same time, the gateway security of the designed edge device was discussed, research indicates, the proposed cache algorithm is better than other algorithms in terms of hit rate and average response speed, so as to ensure the security of the gateway. Qiao et al. (2021) [18] discussed the future applications of blockchain, introduce cutting-edge blockchain technology from four directions: blockchain system, consensus algorithm, smart contract and scalability, the research results show that the effective integration of blockchain with artificial intelligence, Internet of Things and other fields, it can realize the transformation of most traditional centralized applications to decentralization. Aggarwal et al. (2021) [19] conducted a systematic research on the smart contract of blockchain 2.0, the research results demonstrate the importance of smart contracts in digitally facilitating the negotiation of enforcement contracts. Bhardwaj et al. (2021) [20] studied the smart contract blockchain penetration framework, the results show that the blockchain can fight against traditional cybersecurity attacks on smart contract applications, the results of the proposed penetration testing framework can find more program missing vulnerabilities than the results of automated penetration testing scanners. Through the above research, it can be found that blockchain technology has entered a period of rapid development, however, the development of smart contract technology, which is one of the core of blockchain applications, is obviously lagging behind. Categorize, summarize and discuss the latest related research results of blockchain smart contracts, demonstrating the inevitability of the development of smart contracts and the possible trend of smart contracts is the focus of current research.

2.2. The consensus mechanism of blockchain

In the development process of blockchain, the consensus mechanism can ensure that all participants in the distributed system can maintain, inspect and maintain the distributed system while trusting each other. Therefore, designing a safe and efficient consensus mechanism has always been the focus and difficulty of research. Tsang et al. (2019) [21] conducted a research on the food traceability of the Internet of Things driven by a blockchain with an integrated consensus mechanism, adjust the shelf life by using reliable and accurate data, and use fuzzy logic to evaluate the quality attenuation, decision support can be established in the food supply chain. Huang et al. (2019) [22] studied the blockchain system with a credit-based consensus mechanism in the industrial Internet of Things, extensive evaluation and analysis showed that, credit-based POW mechanism and data access control are safe and effective in IioT (Industrial Internet of Things). Kumari et al. (2020) [23] Research on the dissemination and processing of massive data based on blockchain in the industrial Internet of Things environment, through case studies on smart grid systems, in order to evaluate the effectiveness of the data load balancing, energy management cost and transmission delay parameters of the proposed model. Wang et al. (2020) [24] conducted research on the blockchain in integrated connected autonomous vehicles, designed a novel reputation consensus protocol proof, in order to effectively reach a consensus in the AVSN (Association of Vietnamese Students in Norway) that supports the blockchain, experimental results show, the proposed framework is superior to existing methods, provide in-vehicle content more reliably and securely.

Provide in-vehicle content more reliably and securely, researchers have more research on the consensus mechanism of blockchain. For example, Meshcheryakov et al. (2021) [25] studied typical IoT network scenarios that may destroy system performance, the feasibility of using blockchain technology to protect the data of restricted IoT devices was critically analyzed, proved the rationality of implementing a practical Byzantine Fault Tolerance (PBFT) consensus algorithm on such devices. Li et al. (2021) [26] proposed a blockchain-based collaborative edge knowledge reasoning framework for edge-assisted multi-robot systems, a case study was conducted on the emergency rescue application, the experimental results prove the efficiency of the proposed framework in terms of delay and accuracy. Lashkari et al. (2021) [27] systematically organize and comprehensively review the blockchain consensus mechanism, reviewed an extensive collection of 130 consensus algorithms, and identify the categories related to them, conduct a comprehensive analysis of the consensus mechanism, research results show that BCE (Byzantine Compliant Extension), PCE (Proof Compliant Extension) and PA (Pure Alternatives) are most commonly used to reach consensus within the network [28–30].

In summary, people have widely recognized the importance of the consensus mechanism in the blockchain, scholars have proposed many algorithms on consensus mechanism, but there are always more or less defects. This research combines two consensus mechanisms, DPOS and PBFT, optimize and improve the traditional consensus mechanism algorithm, on the basis of solving the efficiency and scalability of the blockchain, the security and reliability of user transactions on the blockchain platform are guaranteed.

3. Based on the improved DPOS-PBFT supervisable consensus mechanism scheme

3.1. The smart contract operating mechanism of the blockchain

As the core technology of blockchain, smart contracts do not require third party intervention, defined in digital form the contract regulations that require intermediaries to verify in the traditional sense, able to automatically trigger execution through preset conditions, its input and output are completed on the basis of the consensus mechanism between all nodes, the entire smart contract is encapsulated in an isolated environment at the contract layer, the related departure and execution are controlled through intelligent programs, as long as the preset conditions are met, the corresponding regulations will be implemented, it will not cause any impact on the internal environment of the blockchain system [31]. The block chain-based smart contract operating mechanism structure diagram is shown in Fig. 1.

As can be seen from the figure, smart contracts can verify the correctness of transaction signatures, at the same time, the status before and after the transaction output is updated. Smart contracts can be regarded as storing several operating environment packages containing different kinds of initial states in the blockchain, at the same time, the package also contains rules for mutual conversion between states, and the different conditions under which various rules are triggered. There are several packages of different sizes mentioned above in the Internet of Things system, these packages will submit the completed transactions to the consensus layer, the consensus layer will uniformly process the submitted data and return it to form a consistency mechanism, after the final processing is completed, the transaction will be deployed on the blockchain. Throughout the processing of things, the formulation and signing of smart contracts need to be negotiated, communicated and agreed by all participants, therefore, it is necessary to pre-set the preconditions for the execution of the regulations in the contract. When the user initiates a transaction request, the smart contract will be packaged together and submitted in the transaction, after dissemination and verification, it is stored in a specific data block, the next transaction will provide transaction data to the smart contract through the contract address and contract interface reported by the previous system, the contract will make judgments based on data and status information, decide whether to execute the contract according to whether the judgment result meets the conditions or not.

3.2. Workload proof protocol design of credit model

The POW (Proof of work) consensus mechanism algorithm is considered to be the cornerstone of Internet Bitcoin security, however, in this algorithm, nodes solve the hash problem through computing power competition, will cause a lot of waste of computing power and power resources [32]. At the same time, the calculation of each node is independent of each other, and there is repeated verification of the search space, the long consensus cycle has brought difficulties to the popularization of applications. In response to the above problems, the improved POW consensus protocol needs to include a node credit model and a shard rotation model, based on two major models to evaluate node credit, allocate search space. The main application scenarios of the blockchain consensus mechanism are shown in Fig. 2.

In the evaluation elements of node credit evaluation, the collected discrete data is uniformly quantified according to different attribute values, then the attribute value is scaled by the following formula:

$$v' = \frac{v - \min}{\max - \min} \tag{1}$$

Where v is the original attribute value, v' represents the attribute value after scaling,min represents the minimum value of a certain attribute, max is its maximum value.After the quantization is completed, all the index values are converted into function values distributed in the interval (0,1) through the normal distribution function, the functional expression of the normal distribution is:

$$\varphi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi} \times \sigma} e^{\frac{-(x-\mu)^2}{2\sigma^2}} dx, (-\infty < x < \infty) \tag{2}$$

Among them, μ and σ are constants, x is the input value of the model.

For the node credit model, utilize the super non-linear processing ability of neural network algorithm, use historical data to train the network credit evaluation model, determine the weight through algorithm evaluation, avoid the influence of artificial adjustment of weights on the internal connection of input and output. According to the BP (Back Propagation) neural network algorithm, the weight adjustment formula of the model is:

$$\Delta w_{j1} = \eta(d_1 - z)(1 - z)zy_j \quad j = 1, 2, 3 \tag{3}$$

$$\Delta v_{ij} = \eta(d_1 - z)z(1 - z)w_{j1}(1 - y_j)y_j x_i \quad j = 1, 2, 3 \tag{4}$$

$$w_{j1} \Leftarrow w_{j1} - \Delta w_{j1} \quad j = 1, 2, 3 \tag{5}$$

$$v_{ij} \Leftarrow v_{ij} - \Delta v_{ij} \quad j = 1, 2, 3 \tag{6}$$

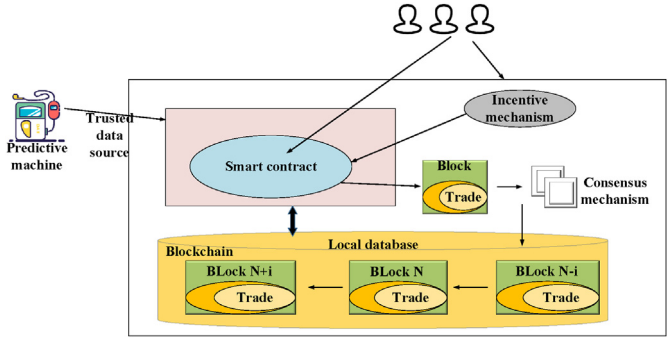

Fig. 1. Blockchain-based smart contract operation mechanism structure diagram.

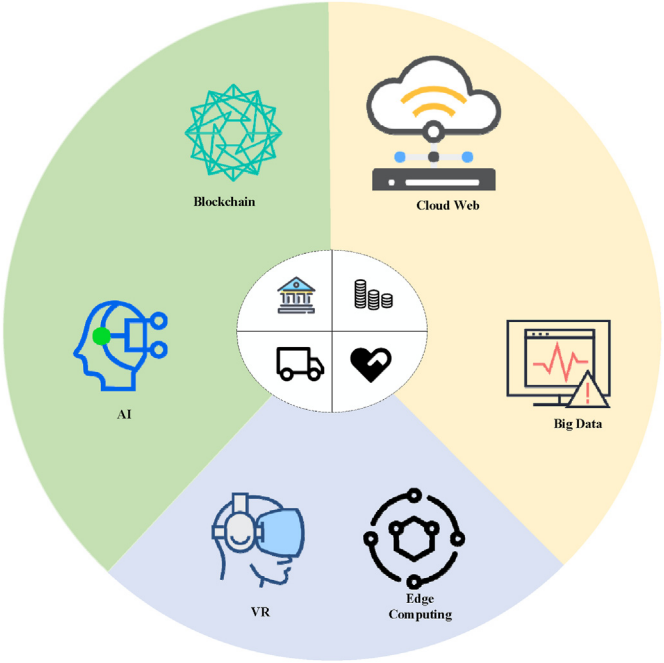

Fig. 2. The main application scenarios of blockchain.

Among them, η represents the learning efficiency of the model, z and d_1 are indicators for judging the termination condition of the algorithm iteration, when the value of $d_1 - z$ meets the experimental error requirements, the algorithm reaches the maximum number of iterations and the training process ends.

In addition, using the shard rotation model to traverse and search all nodes, the nodes are verified by the spatial model according to the level of credit, use the method of dividing the search interval to shorten the consensus cycle, avoid the waste of resources caused by repeated search of nodes. Avoid the waste of resources caused by repeated search of nodes, according to the division rules, the search space obtained by dividing a node with a higher degree of credit is larger. The size of the search space U obtained by node i after the first round of search is:

$$U = \frac{2 \cdot runit \cdot a_i}{(1 + num) \cdot num} \tag{7}$$

Among them, runit is the standard size of each round of search space, *num* is the number of consensus nodes, a_i is the credit ranking of node i, the range V of the first round of search is shown in the following formula:

$$V = \left[\frac{(a_i - 1) \cdot a_i \cdot runit}{(1 + num) \cdot num}, \frac{a_i \cdot (a_i + 1) \cdot runit}{(1 + num) \cdot num}\right) \tag{8}$$

If the node does not solve the hash problem in the first round and does not receive results from other nodes in the network, the following formula can be used, continue to obtain and verify the next round of search space U', where R is the number of rotations:

$$U' = \left[\frac{(a_i - 1) \cdot a_i \cdot runit}{(1 + num) \cdot num} + (R - 1) \cdot runit, \frac{a_i \cdot (a_i + 1) \cdot runit}{(1 + num) \cdot num} + (R - 1) \cdot runit\right) \tag{9}$$

Then the system generates the master node according to the following formula: $p = (q + h) \bmod \text{num}$ (10)

Where h represents the length of the blockchain, q represents the number of stages, the master node is mainly used to initiate the credit ranking request of the consensus node of the whole network, the distribution algorithm flow of the credit ranking by the master node is shown in Table 1.

3.3. Smart contract and DPOS blockchain consensus mechanism

Because traditional distributed algorithms do not have the characteristics of resisting node attacks, therefore, it cannot be directly used as a consensus algorithm for the blockchain. As a centralized consensus mechanism, the accounting rights of the DPOS mechanism are in the hands of a small number of nodes [33]. According to the number of coins held, participants can decide the proportion in the system and take turns as representatives to participate in decision-making, mainly divided into three modules: First, in the blockchain network, all participants use tokens as votes, voting to select a certain number of nodes as trusted nodes, at the same time, perform block accounting operations; Second, the elected nodes perform block processing operations in turn according to the ranking of the votes, and get block rewards; Third, after all nodes have completed the block generation operation, the system re-votes to select a new block producer. Combined with the above description, the structure diagram of the consensus mechanism is shown in Fig. 3.

Table 1
Flow of credit ranking distribution algorithm.

1	**Start**
2	**Input:** Into the Rank array *a*
3	**Output**: the ranked array
4	**For** From the first stage to the *f+1* stage **do**
5	Execution algorithm, broadcast *value(a)*
6	**If** Receive to b at least *num-f* times. **then**
7	broadcast *propose(b)*
8	**End if**
9	**If** receive *propose(c)* at least *f* times. **then**
10	*a=c*
11	**End if**
12	Let node V_i be the master node of the I-th stage.
13	The master node V_i broadcasts the current value *W*
14	**If** The number of times to receive *propose(a)* is strictly less than *num-f* **then**
15	*a=w*
27	**End if**
28	**End for**

Due to the immutability of the blockchain itself, query the number of transactions that already exist for each node through the Merkle root, define the reputation score Score as:

$$Score = \alpha^* \mathrm{T} + \beta^* R_{ij}^t + \lambda^* others \tag{11}$$

$$T = [\chi^* S_a mount - \gamma^* F\_amount] / (T\_amount) \tag{12}$$

$$R_{ij}^t = R^t(P_i, P_j) = \begin{cases} \dfrac{\sum_{k=1}^{n} f(x)}{n}, n \neq 0 \\ 0, n = 0 \end{cases} \tag{13}$$

Among them, the reputation score *Score* is equal to the external static score *T* (that is, the score made on historical transaction record and with internal dynamic points R_{ij}^t (ie points for mutual evaluation of trade fairs between nodes), α, β, λ are the weight, χ andγ are the weight of the success of the transaction and the weight of the failure of the transaction,$S_a mount$ andF_amount represents the number of successful and failed transactions, T_amount represents the total number of transactions, the dynamic score R_{ij}^t represents the score given by node i to j after direct interaction in time t, the integral value can be calculated by the following formula:

$$R_{ij}^t = R^t(P_i, P_j) = \begin{cases} \dfrac{\sum_{k=1}^{n} f(x)}{n}, n \neq 0 \\ 0, n = 0 \end{cases} \tag{14}$$

Where P_i, P_j represent node i and node j respectively, the value of R_{ij}^t is the trust degree of node i to node j, the decay function is used to describe the degree of change in the reputation score of the k-th time period compared to the previous time period:

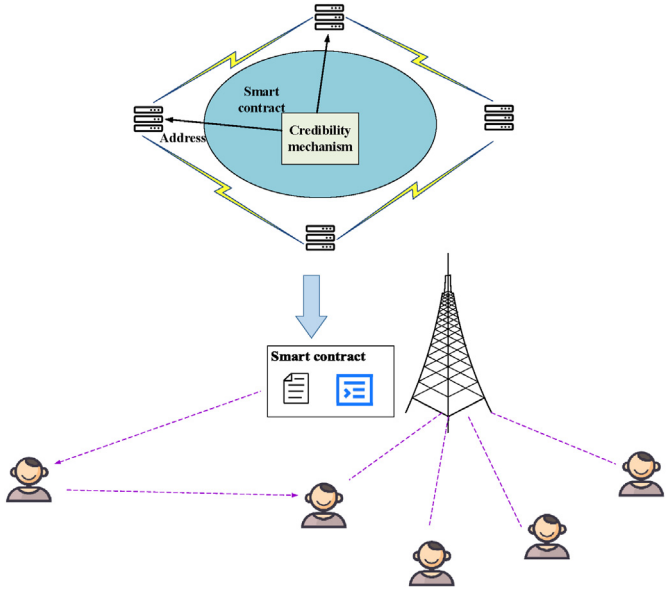

Fig. 3. Schematic diagram of consensus mechanism algorithm structure.

$$f(k) = f_k = \rho^{n-k}, 0 < \rho < 1, 1 \le k \le n \tag{15}$$

If the time period during which a transaction occurs between node i and node j is: $[t\_start\ , t\_end\ ] = [t_1, t_2 \wedge t_n], 1 \le k \le n$ (16)

Then the internal score of i to j is:

$$R_{ij} = \sum_{k=1}^{n} f_k R_{ij}^{t_k} \tag{17}$$

3.4. Dynamic grouping PBFT algorithm based on credibility

The use of the PBFT mechanism is to solve the Byzantine generals problem, achieve the consistency of consensus nodes. Assuming that in the case of satisfying $N \ge 3F + 1$, the network can determine the Byzantine error state of the node through the credibility evaluation model. At the same time, the dynamic PBFT group consensus algorithm based on credibility evaluation greatly reduces the communication complexity of users in large networks, dynamic analysis of different credibility of nodes can increase the credibility of nodes, after reaching a certain threshold, the node grouping can be adjusted, submitted the Byzantine security of the overall network. A schematic diagram of the comparison before and after adding the dynamic grouping PBFT algorithm to the Internet of Things is shown in Fig. 4, it can be seen that after joining the consensus mechanism algorithm, the interaction efficiency of things in the Internet of Things system has been significantly improved, users can call specific services on the blockchain, conveniently complete transactions through smart contracts on the blockchain.

For the network system as a whole, each node processes the information to get the final transaction data, this process is represented by the function f, the nodes communicate with each other using the algorithm p

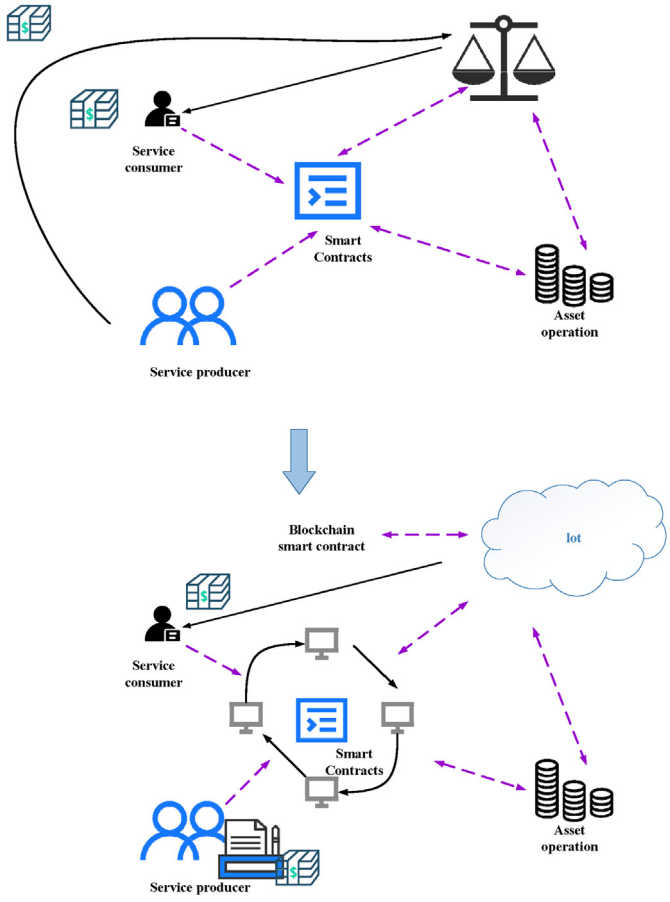

Fig. 4. Comparison before and after adding dynamic grouping PBFT algorithm to interactive things in the Internet of Things.

to make the system finally appear consistent, for any node that runs according to function f, you can get:

$$T = f(T_{0i}, T_{1i}, T_{2i}, \ldots T_{n-1i}) \tag{18}$$

$$Store\_p(T) = true \tag{19}$$

$$Discard\_p(T) = false \tag{20}$$

Through the consensus function f, the consensus node obtains the same transaction information as the original transaction, if the transaction processed by the algorithm is unanimously approved by the node, through transactions and storage, from the client sending a transaction request to confirming that the transaction was successfully recorded by the blockchain, the time interval is calculated by the following formula:

$$t_{\text{latency}} = t_{\text{network}} + t_{\text{concensus}} + t_{\text{write}} \tag{21}$$

The block generation time can be calculated by the following formula:

$$block_{\text{time}\ i} = timestamp_i - timestamp_{i-1} \tag{22}$$

For the block generation speed, as shown in formula (23), the number of transactions per second is measured by throughput, and the calculation formula is shown in (24):

$$block_{\text{speed}\ i} = \frac{1}{\text{block}\ _{\text{time}\ i}} \tag{23}$$

$$\text{tps} = \frac{tx_{\text{count}}}{\text{seconds}} \tag{24}$$

3.5. Scheme based on an improved supervisable consensus mechanism

The purpose of the consensus mechanism design is to solve the efficiency, security and scalability issues, assuming that the production node receives k votes from voting nodes, also set as a timestamp, then the resource amount Rsource can be calculated by the following formula:

$$\text{Rsource} = \left(\oplus_{i=0}^{K-1} \text{Si ngnature}\ [i]\right) \oplus \text{TimeStramp} \tag{25}$$

Perform Hash calculation on Rsource, take the last 32 bits, after being converted to an integer, use the following formula to calculate the random number R:

$$R = \text{StrToInt}\ (\ \text{SubStrend}\ 32(\ \text{Hash}\ (\ \text{Rsource}\ ))) \bmod Np \tag{26}$$

For candidate node k, suppose the total number of candidate nodes is Nc , the probability P1 of each candidate node getting one vote is:

$$\text{P1} = \text{K} / \text{Nc} \tag{27}$$

Furthermore, the probability $P2$ of each candidate node getting x votes is:

$$P2 = C_{N_r}^{X} \times \left(\frac{K}{N_c}\right)^{x} \times \left(1 - \frac{K}{N_c}\right)^{N_r - X} = \frac{N_v!}{i!(N_v - i)!} \times \left(\frac{K}{N_c}\right)^{X} \times \left(1 - \frac{K}{N_c}\right)^{N_r - X} \tag{28}$$

When the candidate node gets more than $\frac{N_v}{2}$ nodes, the probability $P3$ of successfully turning into a production node is shown in (29), another way to calculate the probability of turning into a production node is shown in formula (30):

$$P3 = \sum_{i=\frac{N_v}{2}+1}^{N_v} \frac{N_v!}{i!(N_v - i)!} \times \left(\frac{K}{N_c}\right)^{i} \times \left(1 - \frac{K}{N_c}\right)^{N_v - i} \tag{29}$$

$$P4 = \text{Np} / \text{Nc} \tag{30}$$

Assuming that the transmission size of the data block is Blocksize, the

total number of nodes in the network system is set to N, the calculation formula of the network bandwidth Bandwidth required to complete a data block transmission between all nodes is as follows:

$$\text{Bandwidth} = N \times (N-1) \times \text{Blocksize} \tag{31}$$

If the candidate node has a high or low score and the probability of getting a vote is set to a, then the probability that the candidate node gets a sufficient number of votes and becomes a production node is calculated as P:

$$P = \sum_{i=\frac{N_v}{2}+1}^{N_v} \frac{N_v!}{i!(N_v-i)!} \times \left(\frac{K}{N_c}+a\right)^{i} \times \left(1-\frac{K}{N_c}-a\right)^{N_v-i} \tag{32}$$

The consensus process of PBFT includes a pre-preparation phase, a preparation phase, and a confirmation phase, in the pre-preparation phase, the master node broadcasts the processed request to the backup node, in the preparation phase, the backup node sends the verified message to all nodes participating in the consensus, excluding itself, In the confirmation phase, all nodes participating in the consensus confirm each other, and the total number of communications $S1$ meets:

$$S1 = (n-1) + (n-1) * (n-1) + n * (n-1) = 2 * n * (n-1) \tag{33}$$

In the DPOS-PBFT algorithm model, the consensus phase only includes the preparation phase and the verification phase, Assuming that the total number of nodes participating in the formula process is n, Then the number of communication times of messages sent by the master node in the preparation phase is $n-1$, after the consensus process is completed, the supervisory node needs to send the consensus result to the client node and the master node, therefore, the total number of communications $S2$ should satisfy the following formula:

$$S2 = (n-1) + (n-1) * (n-1) + 2 * (n-1) = (2+n) * (n-1) \tag{34}$$

Then the relationship between the number of communications between PBFT and DPOS-PBFT satisfies the following equation: $S1 - S2 = 2 * n * (n-1) - (2+n) * (n-1) = (n-2) * (n-1)$ (35)

Because of $n \geq 3$, if the result of (35) is greater than 0, then it shows that in the consensus process, when the number of nodes is the same, The number of communications of PBFT is higher than that of DPOS-PBFT, that is, DPOS-PBFT has a lower number of communications. The framework diagram of the improved DPOS-PBFT supervisable consensus mechanism is shown in Fig. 5:

3.6. Case analysis

In order to meet the current requirements of the Internet of Things system for algorithm performance, at the same time, the performance parameters of the improved blockchain consensus mechanism are studied, this research starts from the system architecture, the design of the blockchain management system is based on the consensus mechanism of the blockchain. Different from traditional system design schemes, the system model designed in this research combines the supervisable consensus mechanism and algorithm of the smart blockchain, realized the transformation of design thinking from equipment-centered to user-centered, and completed the design and performance test of the system prototype. The overall system architecture equipment is shown in Fig. 6.

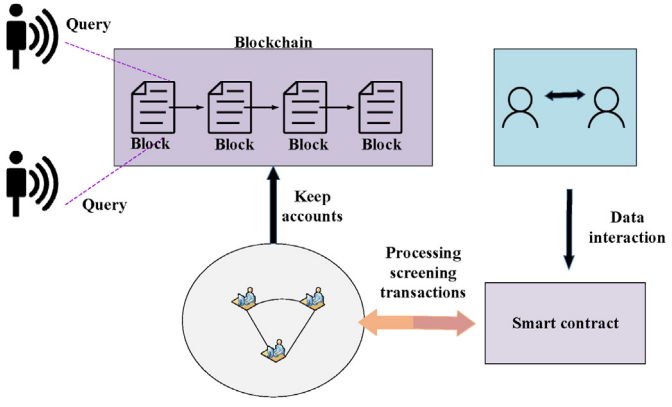

Fig. 5. Framework diagram based on the improved DPOS-PBFT supervisable consensus mechanism.

The experiment is carried out in a local area network environment, and the experimental equipment is shown in Fig. 7, the architecture equipment mainly contains 12 hosts, the host configuration software is CPU (central processing unit): Intel Corei5—7500U, memory: 8G, operating System: Window 10 Enterprise Edition, experiment with Python 3.5 and matplotlib—2.1.0rc1 data visualization module. At the same time, the performance of the DPOS-PBFT supervisable consensus mechanism proposed in this paper is compared with the consensus mechanism algorithms such as Raft [34], POW, POS, DPOS [35], and PBFT [36], analyze the performance pros and cons of each algorithm model.

4. Results and discussion

4.1. Performance test of blockchain consensus mechanism

Compare the performance of the improved DPOS-PBFT consensus mechanism scheme with consensus mechanism algorithms such as Raft, POW, POS, DPOS, PBFT, etc, the relationship between the message delivery success rate and the number of requests/number of iterations is shown in Fig. 7, the relationship between message delivery delay and system network throughput and the number of requests is shown in Figs. 8 and 9, respectively.

It can be seen from Fig. 7(a) that in the Internet of Things system, the success rate of messaging between users will gradually decrease as the number of user requests increases, among several consensus algorithm models, the Raft consensus mechanism increases with the number of user requests, the success rate drops quickly, and after 3000 user requests, the success rate drops below 80%, the proposed DPOS-PBFT supervisable consensus mechanism can still maintain a success rate of over 97% after 3000 user requests, compared with other consensus mechanisms, the power is increased by at least 3.5%. Fig. 7(b) shows that as the number of experimental iterations increases, the success rate also shows an upward trend, however, the performance of the DPOS-PBFT supervisable consensus mechanism is always kept at the optimal level.

As can be seen from Fig. 8, the maximum delay, minimum delay and average delay of message delivery increase with the increase of the number of user requests, however, a larger time delay will increase the waiting time of the user and bring inconvenience to the user's message transmission. A comprehensive comparison of several consensus mechanism algorithms, in the blockchain management system of this research, the comprehensive delay of the proposed DPOS-PBFT supervisable consensus mechanism is kept to a minimum, the maximum delay remains below 8s after 3000 user requests, the minimum delay always remains at

Fig. 6. System overall architecture equipment based on DPOS-PBFT algorithm.

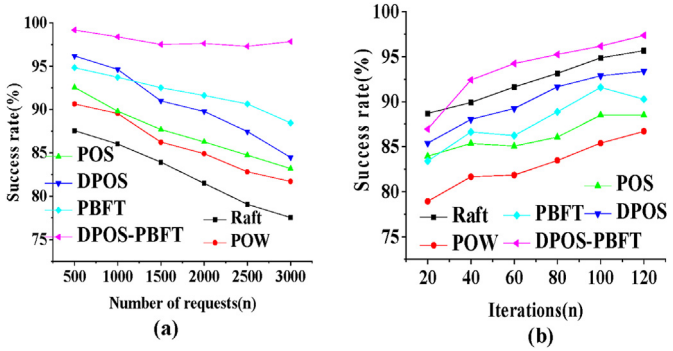

Fig. 7. The relationship between message delivery delay and system network throughput and the number of requests (a. The graph of the success rate of message delivery versus the number of requests; b. The graph of the success rate of message delivery versus the number of iterations).

about 3s, and the average delay is 2.38s.

Regarding the relationship between the throughput of the system network and the number of requests, as the number of user requests increases, the maximum throughput will increase, but the average throughput will decrease accordingly, the average throughput of DPOS-PBFT's supervisable consensus mechanism is not optimal, but the maximum throughput is always maintained at the maximum, and the amount of data transmitted per unit time is also the largest.

4.2. The impact of blockchain consensus mechanism on system hardware efficiency

In order to measure the occupation of system hardware by different consensus mechanisms of the blockchain, in order to measure the occupation of system hardware by different consensus mechanisms of the blockchain, compare the performance of this consensus mechanism with other consensus mechanisms in terms of system memory occupation and disk space occupation, the relationship between the system memory usage and the number of user requests is shown in Fig. 10, the relationship between the disk space and the number of user requests is shown in Fig. 11.

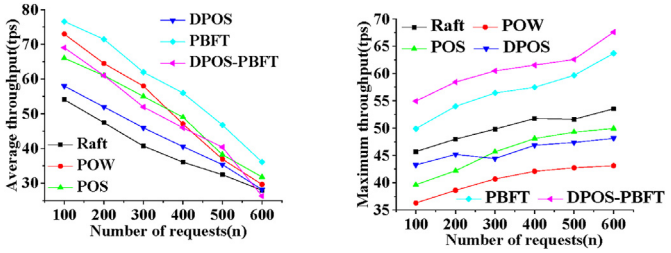

Fig. 9. The relationship between the system network throughput and the number of requests (a. The average system throughput varies with the number of requests; b. The maximum throughput of the system varies with the number of requests.).

It can be seen from the relationship between the system memory usage and the number of user requests that, as the number of user requests increases, both the average system memory usage and the system maximum memory usage will increase, the proposed DPOS-PBFT can supervise the consensus mechanism with a maximum memory occupancy of about 22 MB, the average memory footprint is about 8 MB, and the overall memory footprint is the smallest, compared with the Raft consensus mechanism, the memory footprint is reduced by at least 8 MB. The abscissa in Fig. 10(c) is the type of host CPU for comparison, the

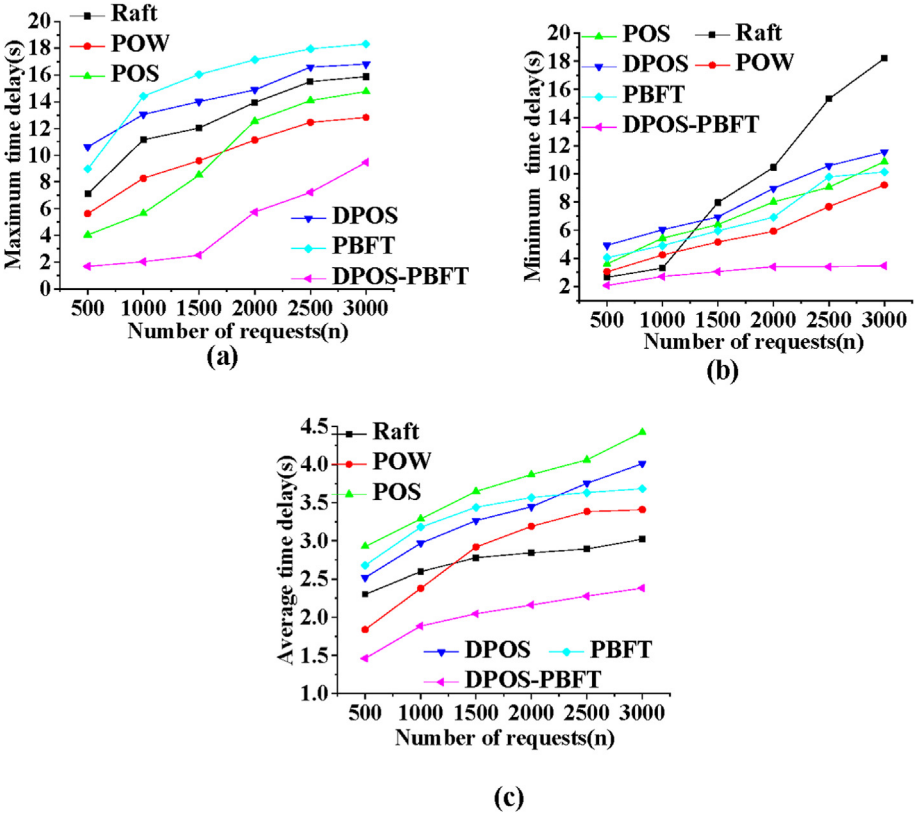

Fig. 8. The relationship between message delivery delay and the number of user requests (a. The maximum delay of message delivery varies with the number of user requests; b. The minimum delay of message delivery varies with the number of user requests; c. The average delay of message delivery varies with the number of user requests).

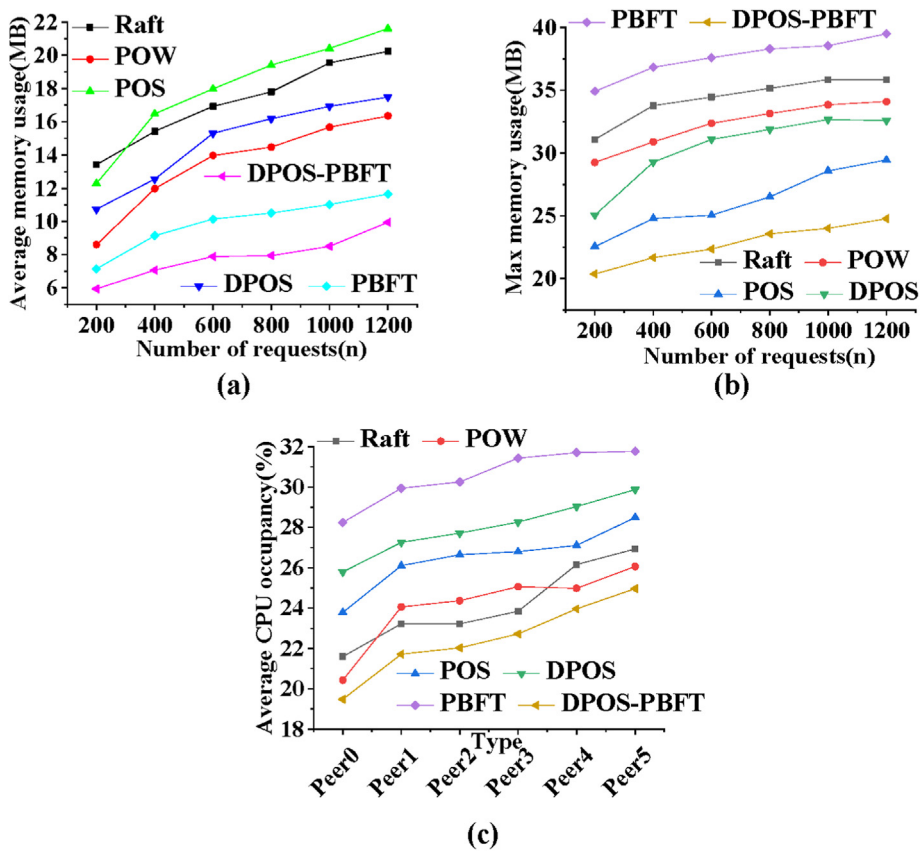

Fig. 10. The relationship between the system memory usage and the number of user requests (a. The average memory usage of the system varies with the number of requests; b. The maximum memory usage of the system varies with the number of requests; c. The average CPU usage of the system varies with the number of requests.).

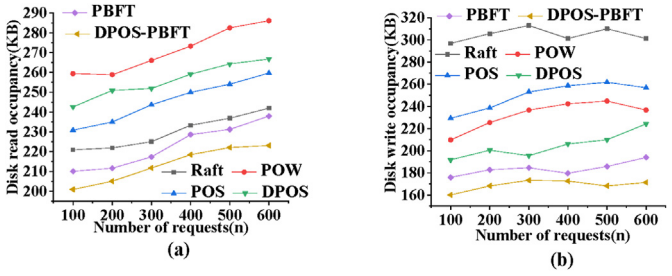

Fig. 11. The relationship between the disk space occupied and the number of user requests (a. The disk read occupancy varies with the number of requests; b. The disk write occupancy varies with the number of iterations).

ordinate is the CPU occupancy rate, it can be found that the performance test results of several hosts show that the CPU occupancy rate of the DPOS-PBFT mechanism is the lowest, always staying below 24%.

The analysis of the relationship between the disk space and the number of user requests can be found, as the number of user requests increases, the disk read space occupied by the DPOS-PBFT mechanism reached 223.12 KB after 600 user requests, and several other consensus mechanism algorithms, after the same 600 user requests, Raft's disk read takes up to 242.05 KB, POS reached 286.11 KB, POW was 259.68 KB, DPOS was 266.81 KB, and PBFT was 237.93 KB, similarly, compared to several other consensus mechanism algorithms, in terms of disk write occupancy, the disk write of the DPOS-PBFT mechanism remains at about 170 KB after 600 user requests, compared with the PBFT algorithm, it saves 14.35 KB of space, compared with the DPOS algorithm, it saves 33.70 KB of space, the overall performance of the system has been greatly improved.

In addition, comparative experiments are conducted to compare and analyze the space occupied by disk read and write during the proposed IoT data transmission process, and the results are shown in Fig. 12.

As can be seen from the results in the figure, after the algorithm optimization of the DPOS-PBFT supervisable consensus mechanism, the disk read space and disk write space of each container type have been greatly improved, the disk read space of the original container Couchdb was reduced from 855.7 KB to 608.88 KB, disk write space is reduced from 858.9 KB to 753.2 KB, the performance of the consensus mechanism algorithm is superior, which greatly improves the efficiency of storage and message transmission.

To sum up, in the Internet of Things system, the success rate of message transmission between users will gradually decrease as the number of user requests increases. The Raft consensus mechanism has a success rate of less than 80% after 3000 user requests, while the DPOS-PBFT supervisable consensus mechanism has a success rate of more than 97%. Furthermore, the maximum, minimum, and average delay of messaging increase with the number of user requests. However, the comprehensive delay of the DPOS-PBFT supervisable consensus mechanism is kept to a minimum, which is lower than that of other blockchain consensus algorithms. The Raft consensus mechanism has a limited capacity to accommodate failed nodes and cannot eliminate database and blockchain risks. Thereupon, it is necessary to redefine and optimize the consensus mechanism of blockchain based on the system network structure.

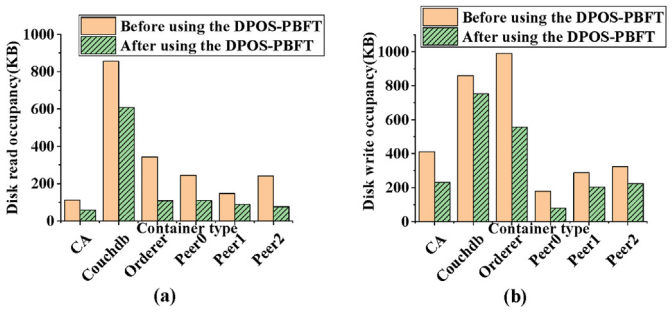

Fig. 12. Comparison of disk read space and write space of IoT data transmission before and after algorithm optimization (a. Disk reading takes up space; b. Disk writing takes up space).

5. Conclusion

With the development of the Internet of Things, the emergence of many decentralized P2P self-organizing network trading platforms makes blockchain technology a hot topic of research quickly, traditional distributed consensus algorithms have problems such as network delay and transmission errors, in order to solve these problems, this research proposes an improved DPOS-PBFT supervisable consensus mechanism based on the traditional consensus mechanism algorithm, and compare the performance with traditional consensus algorithms such as Raft, POW, POS, DPOS, PBFT, etc., the results of the case analysis show that the success rate of the mechanism algorithm can still be maintained at about 97% after 3000 user requests, the maximum delay remains below 8s after 3000 user requests, the minimum delay is always around 3s, the average delay is 2.38s, the overall performance of the algorithm is superior. However, the research still has some shortcomings. First, this research did not consider the issue of secure multi-party computing, in the distributed network to solve the collaborative computing of users who do not trust each other, this problem should be taken into consideration, therefore, secure multi-party computing can be integrated with the consensus mechanism in the future. Second, the number of specific blockchain nodes in the Ethereum environment varies according to the type of application, in the future, different numbers of attack nodes can be added to the Ethereum network for testing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] P. Nerurkar, S. Bhirud, D. Patel, R. Ludinard, Y. Busnel, S. Kumari, Supervised learning model for identifying illegal activities in Bitcoin, Appl. Intell. 51 (6) (2021) 3824–3843.
[2] D. Puthal, S.P. Mohanty, E. Kougianos, G. Das, When do we need the blockchain? IEEE Consumer Electronics Magazine 10 (2) (2020) 53–56.
[3] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, Application-aware consensus management for software-defined intelligent blockchain in IoT, IEEE Network 34 (1) (2020) 69–75.
[4] Z. Lv, L. Qiao, M.S. Hossain, B.J. Choi, Analysis of using blockchain to protect the privacy of drone big data, IEEE Network 35 (1) (2021) 44–49.
[5] X. Zhou, Y. Hu, W. Liang, J. Ma, Q. Jin, Variational LSTM enhanced anomaly detection for industrial big data, IEEE Trans. Ind. Inf. 17 (5) (2020) 3469–3477.
[6] D. Peters, K. Vold, D. Robinson, R.A. Calvo, Responsible AI—two frameworks for ethical design practice, IEEE Transactions on Technology and Society 1 (1) (2020) 34–47.
[7] Y. Zhang, M. Yutaka, M. Sasabe, S. Kasahara, Attribute-based access control for smart cities: a smart-contract-driven framework, IEEE Internet Things J. 8 (8) (2020) 6372–6384.
[8] W. Tushar, T.K. Saha, C. Yuen, D. Smith, H.V. Poor, Peer-to-peer trading in electricity networks: an overview, IEEE Trans. Smart Grid 11 (4) (2020) 3185–3200.
[9] C.E. Ngubo, M. Dohler, Wi-fi-dependent consensus mechanism for constrained devices using blockchain technology, IEEE Access 8 (2020) 143595–143606.
[10] J. Liu, T. Yin, D. Yue, H.R. Karimi, J. Cao, Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks, IEEE Trans. Cybern. 51 (1) (2020) 162–173.
[11] W. Ren, J. Hu, T. Zhu, Y. Ren, K.K.R. Choo, A flexible method to defend against computationally resourceful miners in blockchain proof of work, Inf. Sci. 507 (2020) 161–171.
[12] M. Kandidayeni, H. Chaoui, L. Boulon, S. Kelouwani, J.P.F. Trovao, Online system identification of a fuel cell Stack with guaranteed stability for energy management applications, IEEE Trans. Energy Convers. 36 (4) (2021) 2714–2723.
[13] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, W. Dou, Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain, ACM Trans. Internet Technol. 21 (1) (2021) 1–17.
[14] W. Xiong, L. Xiong, Smart contract based data trading mode using blockchain and machine learning, IEEE Access 7 (2019) 102331–102344.
[15] X. Liu, K. Muhammad, J. Lloret, Y.W. Chen, S.M. Yuan, Elastic and cost-effective data carrier architecture for smart contract in blockchain, Future Generat. Comput. Syst. 100 (2019) 590–599.
[16] S. Xuan, L. Zheng, I. Chung, W. Wang, D. Mans, X. Du, M. Guizani, An incentive mechanism for data sharing based on blockchain with smart contracts, Comput. Electr. Eng. 83 (2020), 106587.
[17] Z. Lv, Security of Internet of Things Edge Devices, Practice and Experience, Software, 2020.
[18] L. Qiao, S. Dang, B. Shihada, M.S. Alouini, R. Nowak, Z. Lv, Can blockchain link the future? Digit. Commun. Network. 5 (2022) 687–694.
[19] S. Aggarwal, N. Kumar, Blockchain 2.0: smart contracts, in: Advances in Computers vol. 121, Elsevier, 2021, pp. 301–322.
[20] A. Bhardwaj, S.B.H. Shah, A. Shankar, M. Alazab, M. Kumar, T.R. Gadekallu, Penetration testing framework for smart contract blockchain, Peer-to-Peer Networking and Applications 14 (5) (2021) 2635–2650.
[21] Y.P. Tsang, K.L. Choy, C.H. Wu, G.T.S. Ho, H.Y. Lam, Blockchain-driven IoT for food traceability with an integrated consensus mechanism, IEEE Access 7 (2019) 129000–129017.
[22] J. Huang, L. Kong, G. Chen, M.Y. Wu, X. Liu, P. Zeng, Towards secure industrial IoT: blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Inf. 15 (6) (2019) 3680–3689.
[23] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, Blockchain-based massive data dissemination handling in IIoT environment, IEEE Network 35 (1) (2020) 318–325.
[24] Y. Wang, Z. Su, K. Zhang, A. Benslimane, Challenges and solutions in autonomous driving: a blockchain approach, IEEE Network 34 (4) (2020) 218–226.
[25] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, Y. Koucheryavy, On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications with Constrained Devices, IEEE Access, 2021.
[26] J. Li, J. Wu, J. Li, A.K. Bashir, M.J. Piran, A. Anjum, Blockchain-based trust edge knowledge inference of multi-robot systems for collaborative tasks, IEEE Commun. Mag. 59 (7) (2021) 94–100.
[27] B. Lashkari, P. Musilek, A comprehensive review of blockchain consensus mechanisms, IEEE Access 9 (2021) 43620–43652.
[28] J.Y. Kwak, J. Yim, N.S. Ko, S.M. Kim, The design of hierarchical consensus mechanism based on service-zone sharding, IEEE Trans. Eng. Manag. 67 (4) (2020) 1387–1403.
[29] Y. Liu, G. Xu, Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value, Comput. Network. (2021), 108432.
[30] C.E. Ngubo, M. Dohler, Wi-fi-dependent consensus mechanism for constrained devices using blockchain technology, IEEE Access 8 (2020) 143595–143606.
[31] Z. Lv, L. Qiao, M.S. Hossain, B.J. Choi, Analysis of using blockchain to protect the privacy of drone big data, IEEE Network 35 (1) (2021) 44–49.
[32] B. Li, R. Liang, W. Zhou, H. Yin, H. Gao, K. Cai, LBS meets blockchain: an efficient method with security preserving trust in SAGIN, IEEE Internet Things J. 9 (8) (2022) 5932–5942.
[33] H. Zhao, S. Deng, Z. Liu, Z. Xiang, J. Yin, S. Dustdar, A. Zomaya, Dpos: decentralized, privacy-preserving, and low-complexity online slicing for multi-tenant networks, IEEE Trans. Mobile Comput. 21 (2) (2021) 4296–4309.
[34] H. Xu, L. Zhang, Y. Liu, B. Cao, RAFT based wireless blockchain networks in the presence of malicious jamming, IEEE Wireless Communications Letters 9 (6) (2020) 817–821.
[35] Y. Liu, B. Wang, W. Ye, X. Ning, B. Gu, Global estimation method based on spatial–temporal kalman filter for DPOS, IEEE Sensor. J. 21 (3) (2020) 3748–3756.
[36] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, M.A. Imran, A scalable multi-layer PBFT consensus for blockchain, IEEE Trans. Parallel Distr. Syst. 32 (5) (2020) 1146–1160.