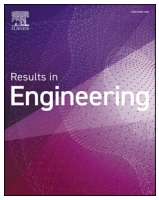
Results in Engineering 18 (2023) 101147

Contents lists available at ScienceDirect

Results in Engineering

journal homepage: www.sciencedirect.com/journal/results-in-engineering



A smart energy IoT model based on the Itsuku PoW technology☆

Jie Li [a], Yansheng Chen [b,*], YanLing Chen [c], Weiping Zhang [d], Zhonghao Liu [e]

[a] School of Finance and Trade, Guangdong Industry Polytechnic, Guangzhou, 510300, China
[b] Dept. of Institute of Big Data and Artificial Intelligence Applications, Guangdong Industry Polytechnic Guangzhou, 510300, China
[c] School of Art and Design, Guangdong Industry Polytechnic, Guangzhou, 510300, China
[d] Dept. of Academic Affairs, Guangdong Industry Polytechnic, Guangzhou, 510300, China
[e] Dept. of Computing, Hong Kong Polytechnic University, Hong Kong, 999077, China

ARTICLE INFO

Keywords:
Blockchain
The proof of work (PoW)
Smart energy networks
Internet of Things(IoT)
Software defined network(SDN)

ABSTRACT

Based on the blockchain + software defined network(SDN) technology, we explore and research a new smart energy networks IoT architecture model of distributed trust to solve the "stuck neck" problems such as bandwidth constraints and trust obstruction of the current centralized network architecture of smart energy networks. In order to achieve efficient data flow and sharing and co-governance. Based on the MTP-Argon2 hash function algorithm in the Itsuku PoW technical solution, we add computing power optimization and correction multi-objective optimization operations, and use the network control right separation technology of the FS-Open Security SDN model to establish local database access policies and storage credentials. The traditional hardware devices are separated from the centralized network architecture of the smart energy network into a hybrid network architecture model of distributed trust. The results show that the distributed trust hybrid network architecture model achieves low latency and circumvents network bandwidth limitations, reflecting the energy efficiency gain and security stability of the model, as well as network load robustness.

1. Introduction

Major countries in the world are accelerating the development of blockchain technology. The integrated application of blockchain technology plays an important role in new technological innovation and industrial transformation. Blockchain is an important breakthrough for independent innovation technology. China attaches great importance to the integration and application of blockchain technology, strives to promote the underlying technical services of blockchain, focuses on the integration with the construction of new smart energy networks, explores the construction of information infrastructure, and uses blockchain technology to promote smart energy networks. Large-scale interconnection to ensure the orderly and efficient flow of production factors within the region. The above discussion clarifies the importance of combining the core technology of blockchain with the construction of intelligent energy network information infrastructure in my country in the future, as well as the response strategy to ensure the orderly and efficient flow of production factors in energy. Based on the above main directions, we strive to overcome the bottlenecks and limitations of the current network architecture of smart cities, and combine the core technology of blockchain with the construction of smart energy networks information infrastructure to solve the key to the orderly and efficient flow of production factors in urban areas. Scientific and technological issues are of theoretical significance in line with the national development strategy of network power and the development of the digital economy.

The Internet of Things (IoT) has given vitality to traditional devices, and its intelligent and autonomous vision is being quietly realized by the commercialization of technologies such as 5G, NB-IoT and eMTC. The "Smarter Planet" concept was proposed by IBM in 2008. Today, with the technological innovation and diffusion of the Internet, big data and artificial intelligence, IoT technology that "everything can be linked" has made the smart energy network a reality. The centralized IT infrastructure of smart energy networks originates from exponentially growing intelligent information processing devices controlled by heterogeneous network systems [1,2], as well as ubiquitous sources of sensor information on the order of millions; however, in the "everything can be linked" of IoT, the massive unstructured data formed by the network connection exceeds the traditional data by several orders of magnitude, and the real-time management, exchange, storage, and

☆ Co-first author: Jie Li, Yansheng Chen, Zhonghao Liu.
* Corresponding author.
E-mail address: yschenchina@qq.com (Y. Chen).

https://doi.org/10.1016/j.rineng.2023.101147
Received 23 March 2023; Received in revised form 28 April 2023; Accepted 4 May 2023
Available online 5 May 2023

mining processing processes of streaming data make the traditional smart energy network architecture still inevitable. Latency, bandwidth bottlenecks, data reliability, privacy and security, and scalability issues. The proliferation of emerging technology innovations will drive the iterative development of future smart energy networks and IoT [3]. It is necessary to rethink the design of an efficient, safe and scalable distributed network architecture based on network energy efficiency and storage resource terminals to solve the current centralized network architecture of smart energy networks. The constraints of data security and the limitations of data security are explored, and the integrated application to realize the transformation of the smart energy Internet of Things to a self-regulating and self-managing distributed network architecture model is explored.

Based on blockchain + SDN technology, we build a prototype of a new smart energy network operation model, which is the main innovation of this paper. We conducted systematic literature mining on the IoT scalability network efficiency and security requirements on which smart energy networks rely, as well as the energy efficiency of IoT by blockchain technology. Looking forward to discovering the use of blockchain to solve IoT technology security issues? And how to achieve a self-regulating, self-managing distributed model transformation of smart energy IoT operations through SDN? We use these two themes as clues to carry out a comprehensive literature study. However, from the existing literature retrieval research, it is found that the research work of smart energy network architecture based on blockchain and SDN is rare. This may also confirm the novelty of the research idea of building a smart energy hybrid network model with blockchain and SDN technologies. Therefore, we find the current research significance from the two aspects of blockchain consensus mechanism technology (BCM) and SDN, and expand the theoretical significance and application value of applied basic research based on the above technologies.

2. Related work

In this section, we summarize the traditional approaches related to blockchain technology resolution services, and provide some background about the blockchain and its latest applications for achieving distributed trusted resolution services.

2.1. Traditional approaches

We found from the research of existing high-cited literature [4] on the theme of blockchain technology, one of which is the focus of financial technology research. Pilkington (2016) outlined the evolutionary technologies of blockchain, such as Ethereum, Ripple, Gridcoin, and blockchain related research based on Markov Chain theory, put forward the practical basis for the non-financial application of blockchain [5]. Tschorsch and Scheuermann (2015) studied robust models based on digital currency technology, discussed the characteristic properties of Bitcoin, and described the consensus mechanism in detail. Second, focus on general applications of blockchain and home IoT [6]. Dorri, Kanhere, & Jurdak (2017) propose a lightweight smart home IoT architecture, focusing on the limitations of blockchain, while proposing solutions to avoid Bitcoin's computationally intensive, TX confirmation delay, and scalability issues [7]. Huh, Cho, & Kim (2017) use blockchain smart contracts to configure and manage IoT devices to circumvent the security and synchronization issues of traditional C/S server architectures [8]. Buterin, Reijsbergen, Leonardos and Piliouras(2020) leverage the trust distributed architecture of blockchain to build Ethereum smart contract configuration and home IoT devices. Third, pay attention to the security technical issues highlighted by digital currency and transactions [9]. Conoscenti, Vetrò and De Martin (2016) different from the blockchain application of the encryption mechanism, a literature review was conducted on the applicability of digital currency transaction security technology to find the Bitcoin such as integrity attacks, de-anonymization and other related vulnerabilities [10]. Dagher, Bünz, Bonneau, Clark, and Boneh (2015) conducted an in-depth analysis of Bitcoin forks based on many Bitcoin security properties, summarized and proposed alternatives to Bitcoin consensus mechanism, user anonymity or privacy technology [11]. Fourth, the operation mechanism of blockchain and smart contracts, and the application of Industry 4.0 have become new topics in the industry. Christidis, and Devetsikiotis (2016) [12]delved into the operational mechanisms of blockchain and smart contracts, such as shared services and resource pooling mechanisms among IoT devices, as well as P2P markets and supply chain management (SCM) mechanisms for renewable sources, expanding A practical case of blockchain and IoT. the paper also focuses on testing the application of blockchain in IoT with low TX throughput, high latency of blockchain based on Proof of work (PoW), user and TX content privacy, as well as the performance characteristics and expectations of smart contracts related legal and transformational issues. In addition, research on the promotion and application of blockchain technology in the manufacturing industry has also become a new topic, such as the strategic route to Industry 4.0 [13] and the prospect of smart factories implementing Industry 4.0 [14].Most of the previous literature focuses on the foundation and theory of independent blockchain technology or SDN [15], or discussions of exploration and verification applications [16], and research on the application of blockchain and IoT in specific scenarios [17]. At present, the most familiar research accumulation with this paper is the subject research on Chain-network Integration between Blockchain and Enterprise Network [18,19], but It is still in the stage of theoretical research and has not been further extended.

The above literature mainly focuses on blockchain-related research based on Markov Chain theory, smart contracts, future manufacturing application exploration, industry 4.0 strategic route support, blockchain privacy protection and efficient aggregation, blockchain and The promotion and application of digital currency technology, DDoS attacks and 51% attacks highlighted by Bitcoin and Bitcoin transactions, as well as problems such as Ethereum mining, energy efficiency and applicability. However, from the perspective of smart energy and the Internet of Things, the related research that explores blockchain technology to solve problems such as the scalability of smart energy networks, data transmission delay, network bandwidth congestion, data privacy and security, etc., has not received extensive attention. , the thematic research has its theoretical contribution to seize the dominance of the new generation of information technology, showing the urgent need of thematic research.

2.2. Blockchain and relevant nonrepudiation applications

Under the background of the national development strategy of building a network power country and developing a digital economy with blockchain technology, it combines the concept of a hybrid network architecture with blockchain and SDN technologies, combining the core technology of blockchain with information infrastructure. Building a scalable smart energy IoT to overcome the bottlenecks and limitations of the current architecture. That will help to enhance access control security, data privacy, network storage and scalability, circumvention of bandwidth limitations, etc., to achieve a transition from an expensive, cumbersome and over-centralized centralized smart energy network architecture to a self-regulating, self-management The transformation of the distributed network architecture model to solve the "stuck neck" problems such as "bandwidth constraints" and "trust obstruction" of the current centralized network architecture, so as to achieve efficient energy flow and resource sharing and co-governance. It is a trend to focus on the integrated application of blockchain technology in smart energy networks and to promote the research and development of blockchain underlying technology services.

First, the shared value system of the blockchain gradually forms a consensus. Traditional industries and emerging industries rely on shared value systems to develop decentralized applications (Dapps) in order to build decentralized trust autonomous organizations and decentralized

autonomous society, (DAS) in central cities around the world. In response to current and future challenges, smart energy may be able to take advantage of SDN and blockchain technology to design solutions specifically to address the challenges of network scalability, data transmission delay, network bandwidth congestion, data privacy and security, etc. A new architectural model shift for self-regulating, self-managing distributed networks to address the limitations of a centralized network architecture for smart energy.

Second, the original intention of the "six ones" planning and design of smart energy makes the construction of smart energy network architecture tend to be centralized IT infrastructure. On the basis of traditional data center network architecture (such as Fat-tree, Portland, VL2, Dcell, Bcube, etc.), combined with the dynamic monitoring characteristics of smart energy construction, a perception layer represented by MEMS, GPS, smart sensors and other technologies is built [1]. The network layer with multiple wireless communication methods as the core and the application layer with multiple specialized capabilities [20]. In the future of highly intelligent cities, smart energy networks can provide all organizations or individuals with a high-quality transaction experience through smart transportation, smart living, smart mobility, smart energy, and smart business models. However, the exponentially growing intelligent information processing infrastructure controlled by heterogeneous network systems, as well as the ubiquitous millions of information source sensors, and the massive data formed by them, give the intelligent energy network framework of the centralized IT infrastructure. , bringing increasing pressure. These include network scalability, data transmission delay, network bandwidth congestion, data privacy and security issues.

3. Preliminary

This section provides the necessary background knowledge of the consensus mechanism and Software Defined Network(SDN) used in this paper.

3.1. Understanding and discovery of the applicability of consensus mechanism technology

The blockchain shared value system is applied by cryptocurrencies, and with the proposal of the blockchain ecosystem, it has evolved and developed, such as Ethereum, smart contracts and asset tokenization (ICO), etc. The sharing economy, and even the blockchain country. Privacy and security of the blockchain ecosystem, and properties such as immutability. It is guaranteed by consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS) and Delegated Proof of Stake (DPOS), as well as distributed ledger consistency. In cryptocurrency and blockchain technology, PoW is the core content that supports large-scale distributed public ledgers. This mechanism makes any block data tampering or attacking behavior, the block must be recalculated and All subsequent blocks form a SHA-256 puzzle. Proof-of-work is powered by the output of a hash function, originally proposed to mitigate spam problems, and later as the Bitcoin protocol. Proof of work is usually iteratively computed based on the double encryption function SHA-256, which is easy to check but difficult to compute [21]. As the core algorithm of cryptographic functions, Argon2 was developed in 2010, became the optimal algorithm in the hash cryptography competition in 2015, and was later fully applied [22]. Biryukov et al. (2016) proposed a proof-of-work scheme using Merkle hash trees on the Argon2 hash chain. It consists of storage encryption and parameter calculation examples for cryptocurrency applications, a proof-of-work model is used to construct a Merkle tree, and a leaf set is selected based on the pseudo-random hash of the root of the Merkle tree as a basis for calculation. In the Argon2 chain, it is difficult for an attacker to find the correct content of the Argon2 chain block through the Merkle tree path. Therefore, if an attacker tries to deceive and store only part of the Argon2 chain, it will be quickly discovered. Currently, the algorithm is considered to be superior to Bcrypt, the most widely used cryptographic hash function today, both in terms of security and cost-effectiveness. In addition to being a cryptographic hash function, the algorithm is also suitable for data privacy and security operations based on consensus mechanisms such as blockchain of PoW.

3.2. Understanding and discovery of the applicability of SDN technology

SDN originated from the Clean Slate research project of Stanford University in 2006. It is a new network architecture model that can define and control the network in the form of software programming. It has the characteristics of separation of control plane and forwarding plane, and open source programmability. Structural research provides a new approach and greatly promotes the development of the next-generation Internet. SDN has the characteristics of openness, standardization, and programmability through the hierarchical distribution settings of the network architecture, replacing the traditional expensive, complicated and excessively centralized network architecture. From the previous literature research, it can be found that there are different network architecture models existing on the SDN architecture. Monshizadeh, Khatri, & Kantola (2017) proposed a multi-layer IDS model [23], which uses programmable SDN control switches to detect and prevent future failures. Authorized attack network, clustered SDN application and control, and detection-as-a-service (DaaS) algorithm functions, highlighting the combination of load balancing technology and clustering of sampled traffic, reducing the computing power cost and network delay in the SDN controller. Machado et al. (2017) propose an ANSwer architecture with network functions virtualization (NFV) and SDN capabilities [16] that can create scalable network policies and feedback control loops to identify and analyze abnormal behavior of network infrastructure. Ammar et al. (2016) propose an enhanced SDN data center security network architecture [24]. The architecture combines the programmability of SDN and detects threats through persistent search and analysis of abnormal behavior of network traffic, and uses security agents to collect and analyze security logs to block attacks. As well as improving data center security performance at the physical network security layer by integrating applications at the adaptive layer. In addition, Sharma et al. (2017) proposed a blockchain-based distributed in-vehicle network architecture in smart cities, which provides ideas for building a safe and reliable distributed network architecture model for transmission management systems [20], and that proposed the DistBlockNet model, a distributed mesh network model for IoT using SDN and blockchain, which defines an update scheme of data flow rules to update and verify the mesh securely of data flow rules in the network. However, due to the lack of standardization of smart energy IoT products, countries around the world have not agreed on a single smart energy network architecture model standard. The layered architectures and their tasks, functions or purposes discussed in different literatures vary according to the scenarios and application practices.

4. Approach

The IoT of a smart energy network system usually consists of three elements: sensor nodes, IoT gateways, and access points. Since sensor nodes in smart energy networks are usually limited in computing and storage resources, when the IoT of SDN is combined with a blockchain system, these sensor nodes are usually divided into transaction nodes in the blockchain system, at each boundary the miner nodes of the network use MiniNET to build SDN support controller nodes. The blockchain system through SDN allows border transaction nodes to only send transactions without mining and storing complete ledger information. The smart energy IoT gateway can be used as the full node (FNs) of the blockchain system SDN, which has abundant computing and storage resources. We use the network control separation technology of the FS-Open Security SDN model to establish local database access policies and storage credentials, so the blockchain system requires full nodes to

perform hash operations to access the ledger and store new blocks. In the SDN model network, we define the access point to determine whether it is the node of the gateway's block transmission by sending an ACK frame, and the access point does not participate in mining, as a backup for the download of the new block gateway, which can be used for blocks sent by the storage gateway.

4.1. Test environment

We use the go-Ethereum experimental platform to build a private blockchain network according to the experimental parameters and performance requirements, and test the distributed properties of the hybrid network architecture through the Mist browser simulation experiment. We use the Argon2 hash function algorithm to define the generated block, and use MiniNET to build the SDN support controller node on the miner node of each border network. The random concurrent big data is generated through the computing power simulation of the combination of distributed computer server groups, and it is defined as the hash transaction of the blockchain. We assume that there are N gateways in IoT, and the computing power of the gateways is constant. The minimum contention window W_{min} on the node is set to 1, the maximum contention window W_{max} is set to 2048, the maximum backoff stage m is set to 8, the packet header H is set to 256 bits, the size of the ACK frame is set to 512 bits, and the channel bit rate is set to 1Mbit/s, the transmission delay is set to 2μs, the time slot size is set to 64μs, the short inter-frame interval SIFS is set to 16μs, the distributed inter-frame interval DIFS is set to 128μs, the size of the block header D_h is set to 512 bits, and the size of the transaction D_t is set to 1 M bits.

4.2. Test process

We adopt the IEEE 802.11 distributed coordination function to transmit blocks, and define Proof of Work (PoW) as the output of the Hash function of the Argon2 hash function algorithm. Essentially, PoW has the characteristics of being difficult to tamper with and verify, which is equivalent to finding a hard solution to the random process of Hash Collision (HC) to reduce the occurrence of block collisions. The PoW algorithm needs to go through the following steps to reach a consensus in the IoT of the smart energy network system: First, the sensor node acts as a transaction node to generate a new transaction and broadcast it to all nodes through a broadcast channel. Second, full nodes collect new transactions and continuously perform hash operations (mining) to compete for the priority of producing legitimate blocks. Third, the gateway that generates the legal block competes for the channel based on the distributed coordination function and obtains the block broadcasting right. Fourth, after the sensor node and the full node accept and verify the new block, the new block is stored in the ledger of the transaction node in the divided blockchain system, and an ACK frame is returned to the full node that sent the block. Fifth, when a new block is stored in the transaction node ledger in the blockchain system, the block has reached a preliminary consensus. Sixth, with the continuous accumulation of subsequent blocks, the probability of the block storage transaction being tampered with will decay exponentially, that is, the more blocks accumulated, the higher the degree of consensus.

5. Results analysis and discussion

5.1. Results analysis

On the premise that the forked block is not broadcast, the PoW algorithm can increase the block generation rate by reducing the difficulty value of the hash operation, so as to achieve the purpose of improving the transaction throughput. In order to verify the performance of the PoW algorithm using the block access control scheme in the hybrid network architecture IoT, we deduced the transaction throughput, block loss rate, block utilization and mining pause time to derive expressions for performance metrics.

- Transaction Throughput

Transaction Throughput is the maximum number of transactions per second that a block can successfully transmit on a network channel. We believe that transaction throughput is equal to the number of blocks successfully transmitted per second on the channel multiplied by the maximum number of transactions a block can hold. In order to reduce the probability of forks and improve the consensus efficiency, consider that the gateway can transmit a whole block after each block rollback, including the block header and all transactions in the block. In this case, a single packet average (bits) can be identified as the size of a block. We deduce the transaction throughput formula with reference to the Markov chain model network throughput calculation formula:

$$V_w = p_1\, d_p \,/\, (\,\mathrm{p0\ t} + \mathrm{p1\ Ts} + (\,1 - \mathrm{p0} - \mathrm{p1}\,)\,\mathrm{Tb}\,) \tag{1}$$

$$T_s = H_d + d_p + 2\lambda + SIFS + ACK + DIFS \tag{2}$$

$$T_b = H_d + d_p + DIFS + \lambda \tag{3}$$

Among them, λ is the block generation rate, *SIFS* is the short inter-frame space, *DIFS* is the distribution coordination function inter-frame space, and *ACK* is the response inter-frame space. Use T_s to represent the size of the block header, T_b to represent the size of a transaction, and d_p to represent the maximum number of transactions that a block can accommodate. Since each successful transmission of a block can accommodate up to d_p transactions, the transaction throughput V_w can be obtained.

- Block discard rate

The block discard rate V_d is defined as the number of forked blocks discarded by the gateways of the entire network per second. This performance indicator can reflect the wasted computing resources of the PoW consensus process from the side. Blocks are discarded in two cases: First, when a successful block transfer occurs in the channel, one or more gateways are in block rollback state V_{d1}. Second, when a block collision occurs in the channel, one or more gateways are in block transfer state V_{d2}. Through integration, the total block discard rate $V_d = V_{d1} + V_{d2}$ can be obtained. According to the transaction throughput formula, the expandable formula is:

$$V\_(d) = \left(\sum_{d_p=0}^{d_p-1} d_p \times P\{V_{d1}\} + \sum_{d_p=0}^{d_p-1} d_p \times P\{V_{d2}\}\right) \Big/ \left(p_1\, d_p + (\,\mathrm{p0\ t} + \mathrm{p1\ Ts} + (\,1 - \mathrm{p0} - \mathrm{p1}\,)\,\mathrm{Tb}\,)\right) \tag{4}$$

● Block utilization and mining suspension probability

In order to study what proportion of blocks can become effective blocks to protect the security of the ledger, the block utilization rate is represented by V_u, which is defined as the steady-state proportion of the number of successfully transmitted blocks to the total number of generated blocks. To get V_u, we first analyze how many blocks the entire IoT can successfully transmit in T time. Let V_{us} be the successful block transmission rate, which means the number of blocks successfully transmitted per second in the entire network, and V_{ud} be the number of blocks discarded by the entire IoT within T time. The block utilization rate can be expressed as:

$$v_u = \lim_{T\to\infty}\left(v_u / \left(v_u + v_{us}\right)\right) \tag{5}$$

We analyze the steady-state probability p_v of mining suspension, and its physical meaning is the long-range proportion of the entire network mining suspension time to the total system time. We can understand it this way, the average number of blocks generated by a gateway per second is λ, and its value is the quotient of the gateway hash rate and the hash operation difficulty value. When the mining strategy is not used to suspend mining, the entire network will generate d_p blocks on average in T time. When affected by the mining strategy, the entire network will only generate d_{ps} blocks on average in T time. From this, we can get:

$$p_v = \lim_{T\to\infty}\left(\left(\lambda d_p - \left(v_u + v_{us}\right)T\right) / \ \lambda d_p\right) \tag{6}$$

5.2. Results discussion

Considering that the actual block size is determined by the number of transactions contained in the block, we use the above formula to calculate the change curve of transaction throughput, block discard rate and mining suspension probability according to the parameter settings. At the same time, we set the number of gateways d_p and the block generation rate λ to 2^3, 2^4, $2^5$and $2^6$for comparative calculation to reflect the impact of the number of gateways on various performance indicators.

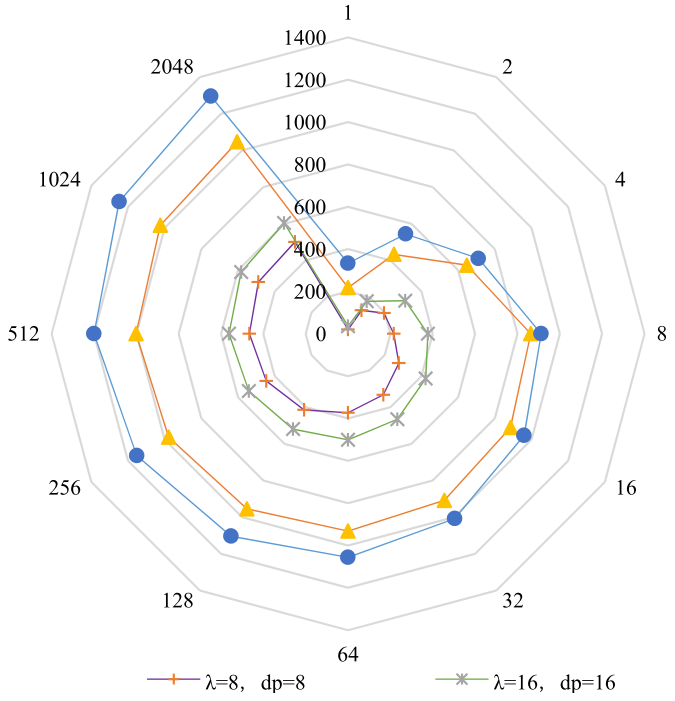


Fig. 1. Evaluation of the impact of the maximum number of transactions throughput.

● The impact of the maximum number of transactions on performance

The results in Fig. 1 show that transaction throughput increases as d_p increases. At the same time, the growth rate of transaction throughput will gradually decrease with the increase of d_p, and eventually become stable. Even when $d_p = 2^{20}$, the four curves have no downward trend. This is because when d_p, increases, each time block rollback ends, a block sent by the gateway can accommodate more transactions. Statistically speaking, the smaller the average backoff latency experienced by a single exchange, the more transactions per second are transferred. On the other hand, the larger the block generation rate λ and d_p, the faster the transaction throughput grows, but the lower the maximum transaction throughput when it reaches a plateau. When $d_p = 2^{20}$, the transaction throughput of λ and d_p equal to 2^3 is 501tps, the transaction throughput of λ and d_p equal to 2^4 is 604tps, the transaction throughput of λ and d_p equal to 2^5 is 1047tps, and the transaction throughput of λ and d_p equal to 2^6 is 1296 tps. This is because when d_p is small, the block transmission delay is small. In this case, the larger λ and d_p, the higher the channel resource utilization, the more transactions per second are transmitted. When the d_p is large, the block transmission delay is large. In this case, the larger λ and d_p, the more congested the channel, and the overload phenomenon occurs. The frequent collision of blocks reduces the maximum transaction throughput when it is stable.

The results in Fig. 2 show that the block discard rate decreases as dp increases. This is because when d_p increases, the block transmission delay increases, making the mining pause time longer. The mining suspension will slow down the block generation rate of the gateway, at the same time, reducing the probability of blocks appearing in the rollback state, and ultimately reducing the block discard rate. When d_p is constant, the larger the λ and d_p, the greater the probability of fork will be generated, and the more blocks will be discarded. According to the block utilization formula, we know that the block utilization does not change with the change of d_p. That is, as d_p increases, the ratio of the successful block transfer rate to the block discard rate is constant. Combining the results in Fig. 1, we can see that with the increase of d_p, the successful block transmission rate and the block discard rate will decrease at the same rate, so that the block utilization rate can be kept constant. The reason for the decrease in the successful block transmission rate is that the channel resources are limited. The longer the transmission time of a single block, the fewer blocks that can be successfully transmitted per second. Since the premise of the test is that the gateway computing power and PoW difficulty value are constant, the decrease in the successful block transmission rate will lead to less

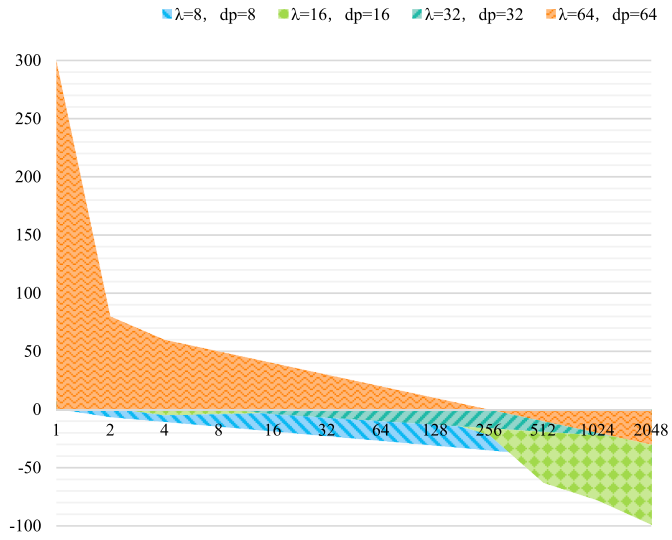


Fig. 2. Evaluation of the impact of the maximum number of transactions on the block discard rate.

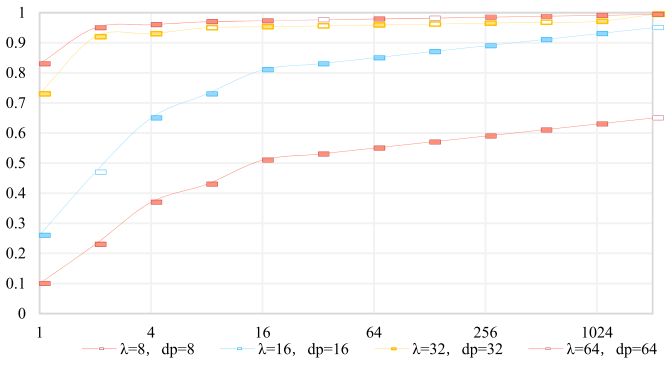


Fig. 3. Evaluation of the impact of the maximum number of transactions on the probability of mining suspension.

- Block Generation Rate and Performance Analysis

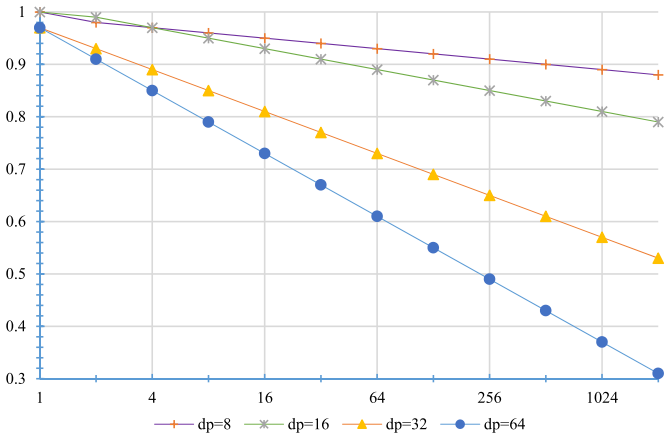


Fig. 4. Comparison and evaluation of block utilization and block generation rate.

cumulative computing power per unit time of the ledger. That is, an increase in d_p reduces security.

The results in Fig. 3 show that the mining suspension probability increases as d_p increases. This is because when the d_p increases, the block occupies the channel for a longer time, so the mining strategy will suspend the mining of the gateway more frequently to reduce the generation of forks and keep the block utilization constant. On the contrary, if the mining suspension strategy is not used, when blocks are transmitted in the channel, forked blocks will be generated, which will reduce the block utilization rate. We can find that the larger the d_p setting, the higher the transaction throughput of the consensus process, but the block utilization will not be affected while the throughput increases. On the other hand, the increase of d_p will increase the block transmission delay, resulting in fewer accumulated blocks per unit time of the ledger, which affects security. Therefore, in actual scenarios, d_p can be set according to specific requirements to achieve a balance between performance and security.

It can be found from Fig. 4 that the block discard rate increases monotonically as λ increases, which is opposite to the effect of d_p on the block discard rate in Fig. 3. This is because when λ becomes larger, more blocks will enter the rollback state at the same time, and only one of these blocks will be successfully transmitted in the end, and the rest will be discarded due to forks. In contrast, when the d_p becomes larger, the probability of the pause time increases, and at the same time, there are fewer blocks entering the rollback state. In addition, we also found that the increase of the number of gateways d_p and the block generation rate λ has a similar effect on the block discard rate, that is, the block discard rate increases. The results in Fig. 4 show that with the increase of λ, the block utilization rate will decrease, that is, the proportion of successfully broadcast blocks in the total generated blocks will become smaller. When the block utilization is less than 0.3, most of the blocks will be discarded due to forks. The reason for this phenomenon is that the increase in the block generation rate increases the number of blocks that enter the rollback state at the same time, and the proportion of forked blocks increases. Since the computing power for generating forked blocks cannot be accumulated on the main chain of the ledger, under the condition that the computing power of the gateway is constant, the increase in the proportion of forked blocks will "dilute" the computing power of the gateway and affect the security.

6. Conclusion and limitations

6.1. Conclusion

Considering that the PoW consensus algorithm has the problems of limited transaction throughput and large consumption of computing resources, we propose a block access control scheme to deal with the fork problem of the PoW algorithm in the smart energy IoT scenario. We speed up the block generation rate while improving the effectiveness of computing resources to achieve the purpose of improving transaction throughput. Next, we established a Markov chain model [25] to analyze the performance of PoW algorithm with block access control scheme in smart energy IoT, including: transaction throughput, block discard rate, block utilization, and mining pause probability.

The analysis results show that the PoW algorithm using the block access control scheme can achieve high transaction throughput in the smart energy IoT. Under ideal channel conditions, transaction throughput can reach up to 1296 tps. In the consensus process, the more transactions a single block contains, the higher the transaction throughput, but this also increases the block transmission delay, which reduces the cumulative blocks per unit time of the ledger, which affects security. When the computing power of the gateway is constant, the system can increase the block generation rate by reducing the PoW difficulty value to achieve the purpose of improving the transaction throughput, but at the same time, the block utilization and security will be reduced. Therefore, in actual scenarios, the block size and difficulty value can be set according to specific requirements to achieve a balanced load among transaction throughput, block utilization, and security. In general, the block access control scheme improves the transaction throughput and block utilization of the PoW algorithm in the smart energy IoT environment, but its resource consumption is still greater than the DAG consensus, and its advantages lie in energy efficiency and security stability, Not easily affected by network load.

6.2. Limitations

Based on the challenges and dilemmas faced by the current smart energy centralized network architecture, we conceive a conceptual model of distributed trust network operation to realize the smart energy IoT network security architecture and sustainable development, but there are still the following limitations:

- Avoid the bottleneck problem of network bandwidth limitation. For the business practices and application scenarios of smart energy, the current centralized network architecture solutions are not suitable for circumventing network bandwidth limitations. Centralized network architectures have to send the massive data collected by sensors to the core network, which consumes a lot of network bandwidth, addresses bandwidth constraints and reduces bandwidth usage. We need to design a network architecture that allows distributed autonomous regulation and management of local data processing and analytical operations.
- Avoid the single point of failure problem. Due to the massive data eruption of heterogeneous networks, the network architecture of

smart energy may be overloaded, resulting in a large number of single points of failure and reducing the quality of service envisaged by smart energy. We need to design a trust network architecture that provides network fault tolerance and tamper resistance.

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.

Data availability

Data will be made available on request.

Acknowledgements

This research was funded by Guangdong Province Philosophy and Social Sciences Planning 2020 Disciplinary Co-construction Foundation (Project#GD20XGL49), 2021 Annual Project of Guangdong Social Science Planning Foundation (Project#GD21CGL13), Guangzhou 2021 Basic and Applied Basic Research Foundation (Project#202102080475), and 2022 Provincial Key Platform Scientific Research Innovation Team (Natural Science) Project of Guangdong Provincial Department of Education (Project#2022KCXTD042).

References

[1] Salem Al-Naemi, Awni Al-Otoom, Smart sustainable greenhouses utilizing microcontroller and IOT in the GCC countries; energy requirements & economical analyses study for a concept model in the state of Qatar, Results in Engineering 17 (2023), 100889, https://doi.org/10.1016/j.rineng.2023.100889.

[2] H.S. Shrisha, Boregowda Uma, An energy efficient and scalable endpoint linked green content caching for Named Data Network based Internet of Things, Results in Engineering 13 (2022), 100345, https://doi.org/10.1016/j.rineng.2022.100345.

[3] Giral-Ramírez, Diego Armando, César Augusto Hernández-Suarez, César Augusto García-Ubaque, Spectral decision analysis and evaluation in an experimental environment for cognitive wireless networks, Results in Engineering 12 (2021), 100309, https://doi.org/10.1016/j.rineng.2021.100309.

[4] Chen, Lin, Business intelligence capabilities and firm performance: a study in China, Int. J. Inf. Manag. (2020), 102232, https://doi.org/10.1016/j.ijinfomgt.2020.102232.

[5] Pilkington, Does the fintech industry need a new risk management philosophy?, Digital Currencies and e-money Services in Luxembourg (March 8, 2016) (2016), doi:10.2139/ssrn.2744899.

[6] Tschorsch, Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials (2016) (2016) 2084–2123, https://doi.org/10.1109/COMST.2016.2535718.

[7] Kanhere Dorri, Jurdak, Towards an optimized BlockChain for IoT, *The second IEEE/ACM conference on* Internet of Things Design and Implementation (2017) 173–178, https://doi.org/10.1145/3054977.3055003, 2017.

[8] Cho Huh, Kim, Managing IoT devices using blockchain platform." 2017 19th international conference on advanced communication technology (ICACT), IEEE (2017) (2017) 464–467, https://doi.org/10.23919/ICACT.2017.7890132.

[9] V. Buterin, D. Reijsbergen, S. Leonardos, G. Piliouras, Incentives in Ethereum's hybrid Casper protocol, Int. J. Netw. Manag. 30 (5) (2020), e2098, https://doi.org/10.1002/nem.2098.

[10] Vetrò Conoscenti, De Martin, Blockchain for the Internet of Things: a systematic literature review, 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (2016) 1–6, https://doi.org/10.1109/AICCSA.2016.7945805, 2016.

[11] Gaby Dagher, Benedikt Bünz, Bonneau Joseph, Jeremy Clark, Dan Boneh, Provisions: privacy-preserving proofs of solvency for Bitcoin exchanges, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15), Association for Computing Machinery, 2015, pp. 720–731, https://doi.org/10.1145/2810103.2813674, 2015.

[12] Christidis, Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303, https://doi.org/10.1109/ACCESS.2016.2566339, 2016.

[13] M. Ghobakhloo, The future of manufacturing industry: a strategic roadmap toward Industry 4.0, J. Manuf. Technol. Manag. 29 (6) (2018) 910–936, https://doi.org/10.1108/JMTM-02-2018-0057.

[14] Wan Wang, Li Zhang, Zhang, Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination, Comput. Network. 101 (4) (2016) 158–168, https://doi.org/10.1016/j.comnet.2015.12.017, 2016.

[15] Kumar, Tripathi, Implementation of distributed file storage and access framework using IPFS and blockchain." *2019 fifth international Conference on image information processing*, ICIIP) (2019) (2019) 246–251, https://doi.org/10.1109/ICIIP47207.2019.8985677.

[16] Machado, Wickboldt, Granville, Schaeffer-Filho, Arkham: an advanced refinement toolkit for handling service level agreements in software-defined networking, J. Netw. Comput. Appl. 90 (JUL) (2017) 1–16, https://doi.org/10.1016/j.jnca.2017.04.009, 2017.

[17] Guizani Al-Fuqaha, Aledhari Mohammadi, Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor 17 (4) (2015) 2347–2376, https://doi.org/10.1109/COMST.2015.2444095, 2015.

[18] Li Chen, Hu Liu, Wang, A study of the theory of chain-network integration between blockchain and Enterprise network, Proc. SPIE (2021), 1207909, https://doi.org/10.1117/12.2622717, 2021.

[19] Liu Chen, Li, Zhang, The integration of blockchain and Enterprise network: a distributed operation solution, IEEE Computer Society (2021) (2021) 965–976, https://doi.org/10.1109/CISAI54367.2021.00194.

[20] Singh Sharma, Jeong, Park, DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks, IEEE Commun. Mag. 55 (9) (2017) 78–85, https://doi.org/10.1109/MCOM.2017.1700041, 2017.

[21] Feige Dwork, Naor Kilian, Safra, Low Communication 2-prover Zero-Knowledge Proofs for NP, springer, 1992, 1992, https://link.springer.com/content/pdf/10.1007%2F3-540-48071-4_15.pdf.

[22] Dinu Biryukov, Khovratovich, Argon2: new generation of memory-hard functions for password hashing and other applications, 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (2016) 292–302, https://doi.org/10.1109/EuroSP.2016.31, 2016.

[23] Khatri Monshizadeh, Kantola, An adaptive detection and prevention architecture for unsafe traffic in SDN enabled mobile networks, Integrated Network & Service Management (2017) (2017) 883–884, https://doi.org/10.23919/INM.2017.7987395.

[24] Rizk Ammar, Abdel-Hamid, Aboul-Seoud, A framework for security enhancement in SDN-based datacenters, Ifip International Conference on New Technologies (2016 (2016) 1–4, https://doi.org/10.1109/NTMS.2016.7792427.

[25] Richardson, Domingos, Markov Logic Networks, vol. 62, Kluwer Academic Publishers, 2006, pp. 107–136, https://doi.org/10.1007/s10994-006-5833-1, 2006.