EFSC: an Efficient, Flexible and Secure Trading System for Computing Power Network

Qunyang Lin
Inspur Electronic Information Industry Co., Ltd.
Beijing, China
linqunyang@ieisystem.com

Luyang Liu
Inspur Electronic Information Industry Co., Ltd.
Beijing, China
liuluyang@ieisystem.com

Hongyin Zhu
Inspur Electronic Information Industry Co., Ltd.
Beijing, China
zhuhongyin@ieisystem.com

Haonan Tong
Inspur Electronic Information Industry Co., Ltd.
Beijing, China
tonghaonan@ieisystem.com

*Chuang Zhang
Inspur Electronic Information Industry Co., Ltd.
Beijing, China
zhangchuangbj@ieisystem.com

2024 IEEE 49th Conference on Local Computer Networks (LCN) | 979-8-3503-8800-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/LCN60385.2024.10639684

***Abstract*—With the escalating demand for computing power driven by the advancements in deep learning and artificial intelligence (AI), the computing power networks serve as critical infrastructure nowadays. Recently, the emerging blockchain enhanced computing power networks has showed appealing advantages of fair and reliable resource allocation, adaptive and flexible management on heterogeneous computing power network, transparent and trustworthy transactions, thereby alleviating the drawbacks of traditional computing infrastructure. Yet, the efficiency and security concerns associated with blockchain-based transactions are neglected when it is applied to computing power trading scenario. To address these issues, in this paper, we introduces the EFSC (Efficient, Flexible, Secure Computing-power-trading) system, a blockchain and smart contracts-based solution aimed at enhancing the efficiency and security of computing power trading. By leveraging a hybrid mechanism that combines on-chain and off-chain methods and utilizing off-chain transaction channels, the EFSC system achieves high throughput transaction processing while also supporting adjustable on-chain policies. Furthermore, transaction data templates based on the Verifiable Credentials (VC) data model enable flexible computing power transaction patterns, allowing providers to define and register configurable transaction initiation and settlement credential templates. To address transaction security concerns, the system leverages Decentralized Identifiers (DID) for off-chain channel access authentication and utilizes DID and VC mechanisms to facilitate transaction initiation and settlement processing, thereby enhancing the credibility and authenticity of transaction data. The experimental results and analysis demonstrate the effectiveness of proposed system.**

***Index Terms*—Blockchain, smart contract, computing power network, transaction efficiency, transaction flexibility, security**

I. Introduction

With the rapid development of deep learning and artificial general intelligent techniques, the booming artificial applications can facilitate various industries such as medicine[1], social governance[2] and finance[3]. The increasing demand for computing power in these area, including artificial intelligence (AI), machine learning, and big data analytics, has posed new challenge towards current computing infrastructure. Recent works[4, 5] that leverage emerging blockchain to organize and manage computing resources has attracted much attention both from industrial and academic communities. These solutions take advantage of the decentralized and immutable nature of blockchain and programmable smart contracts to manage resources in computing power network. These mechanisms enable fair and reliable resource allocation, flexible management on heterogeneous computing power networking, transparent transactions, and automated execution of agreements, thereby alleviating the drawbacks of current centralized computing infrastructure. Specifically, [4] proposed a holistic framework accommodating heterogeneous computing power from diverse supply source (e.g., cloud, edge, networking devices, and even end devices), and solved the problem of computing-networking resource allocation. [5] focused on solving problems of fair and reliable trading and decentralized reputation. However, in the blockchain-enabled computing power network, there are still several critical issues that need to be addressed: Firstly, due to the involvement of various suppliers, computing power resources may exhibit significant variations in specifications and definitions, resulting in a lack of interoperable data exchange models for computing power management, including resource registration, scheduling, allocation, and transactions. Secondly, owing to the ledger mechanism of blockchain, on-chain transactions often incur high costs and long delays, potentially becoming a bottleneck for system performance. Furthermore, while blockchain data is transparent and traceable to all users, the blockchain itself cannot guarantee the authenticity and reliability of transaction data. Thus, ensuring the reliability of transaction participants' identities and the authenticity of data is also a critical issue.

To address aforementioned issues, in this paper, we present EFSC(Efficient, Flexible, Secure Computing-power-trading) system, a blockchain and smart contracts based system that enhance efficiency and security aspects of computing power networks, offering a decentralized, secure, and sustainable

*Chuang Zhang is the corresponding author.

infrastructure for meeting the growing demands of AI and other computational-intensive applications. To boost efficiency of blockchain enhanced computing power network, we propose an hybrid mechanism combining on-chain and off-chain methods and leverage off-chain transaction channels to achieve high throughput transaction processing. This mechanism also support adjustable time-span on-chain processing policy, which overcomes the issue of system bottleneck due to sudden bursts of on-chain settlement requests. Besides, based on the Verifiable Credentials (VC)[1] data model, transaction data templates support flexible computing power transaction patterns, allowing computing power providers to define and register configurable transaction initiation and settlement credential templates to accommodate diverse computing power transaction scenarios. For transaction security issue, we leverage Decentralized Identifiers (DID)[2] for off-chain channel accessing authentication. Additionally, proposed method utilizes DID and VC mechanisms to facilitate the transaction initiation and settlement processing, encapsulating transaction data in a credential format to enable cross-platform verification, thereby enhancing the credibility of transaction data. To sum it up, our contributions can be concluded as follow:

- Based on blockchain and smart contract techniques, we propose an decentralized computing power trading system, EFSC system, which is capable of efficient and flexible transaction and secured transaction experience.
- We propose a hybrid mechanism combining on-chain and off-chain methods, utilizing off-chain transaction channels for high throughput transaction processing and adjustable on-chain policies, addressing system bottleneck issues caused by sudden bursts in on-chain settlement requests, while also supporting flexible computing power transaction patterns through transaction data templates based on the VC data model.
- To address transaction security concerns, we employ DID identification for off-chain channel access authentication, and utilize DID and VC mechanisms to facilitate the initiation and settlement processing of computing power transactions, encapsulating transaction data in credential format to enable cross-platform verification and enhance transaction data credibility.

II. Related Works

A. Computing power network

The computing power network(CPN) functions as the backbone supporting various computing applications providing the necessary computational resources for tasks such as simulation, data mining, model training, and inference. The typical CPN usually has two-layer structure[6]: the bottom layer consists basic hardware infrastructure such as computing nodes and networking devices. The upper-level module utilizes software-defined networking technology to organize and manage computing nodes within the computational network, enabling them to function as a cohesive entity to provide users with a unified and comprehensive computing service. Current CPN usually adopt centralized computing scheme which fails to achieve fair and reliable resource allocation, flexible resource management on heterogeneous computing resources, transparent transactions, and automated execution of agreements. To tackle these issues, enhancing CPN with emerging blockchain technique becomes a prevalent topic.

B. The transaction efficiency on Blockchain

Blockchain technology, with its characteristics of decentralization, distributed storage, data tamper resistance, traceability, and cryptographic trust endorsement, provides robust technical support for distributed transaction platforms. There are two types of blockchain systems: permissionless (i.e. public) chain and permissioned (i.e. consortium) chain. On public chains like Bitcoin and Ethereum, transactions are often executed using cryptocurrencies such as Bitcoin and Ether. However, in the Bitcoin network, each transaction requires broadcasting to the entire network, notifying miners, and incurring fees to reward miners for ledger maintenance. Moreover, the ledger rules of blockchain significantly restrict transaction speed, rendering it unsuitable for scenarios involving small-value, high-frequency transactions. Although consortium blockchains[7, 8] have greatly improved transaction efficiency, they still cannot meet the demand for instant settlement of high-frequency transactions. In response to these challenges, the industry has proposed off-chain transaction processing techniques. Lightning Network[9] is a notable example of such techniques. It is built on top of the Bitcoin network and adopt an off-chain protocol to enable micro-payment between any two parties on blockchain which only recorded the last transaction state once a settlement was triggered. By establishing off-chain payment channels, the Lightning Network enables fast transactions, significantly improving transaction speed and throughput. [10] summarized 12 payment patterns clarifying state transitions of a token in blockchain-based payment applications. [11] proposed a secure model on Lightning Network for e-commerce platform supporting high volume of transactions and scalability. A similar approach based on off-chain payment channel was applied to Etherum. Etherum Raiden Network[12] took advantage of a network of off-chain payment channels to perform off-chain transactions.

C. The transaction security on Blockchain

While improvements have been made in transaction efficiency via off-chain payment channel, concerns regarding identity and transaction security have arisen. Particularly in blockchain-based distributed systems, ensuring transaction and identity security is of paramount importance. The lack of reliable mechanisms for user identity authentication or trusted transactions can lead to identity fraud issues. For instance, artist Derek Laufman's work was auctioned on the NFT marketplace platform Rarible without his knowledge[13]. To address identity security and trusted transaction issues, the industry has proposed several methods, including identity

[1]https://www.w3.org/TR/vc-data-model-2.0

[2]https://www.w3.org/TR/did-core

verification[14–16], data access control or authorization[17–20], and cryptography[21–23]. Decentralized identifiers and verifiable credentials technologies can be leveraged to address these challenges. Since 2019, with the release of the first working draft of DID by the W3C Decentralized Identifier Working Group, related standards and specifications including DID, DID Documents[3], DID Resolvers[4], DID Specification Registries[5], and VC have continued to expand.

III. Preliminary

The proposed computing power trading system based on blockchain technology differs from traditional centralized trading platforms. It can accommodate various computing power providers, managing the allocation of computing power resources via blockchain and facilitating computing power transactions.

Specifically, the set of computing power providers is denoted as S, where for any computing power provider $s \in S$, the set of computing power specifications Q_s and corresponding price quotations P_s are provided, with the total processing capacity being R_s. On the other hand, the set of computing power consumption users is denoted as C, where for any computing power consumption user $c \in C$, there exists a computing power demand D_c. The trading system, through matchmaking smart contracts, recommends optimized optional solutions for user c, who then decides whether to initiate a computing power transaction. Typically, a computing power transaction commences with a transaction initiation event and lasts for an uncertain period, with periodic settlements occurring during this process. Notably, computing power transactions exhibit characteristics of small-value, high-frequency transactions, thus imposing higher demands on the system's processing performance and efficiency. Moreover, diverse pricing and billing strategy requirements from different computing power providers and consumers necessitate the support of various computing power trading patterns in blockchain-based systems. Additionally, as the blockchain-based computing power trading system involves various computing power providers and consumers in a distributed manner, ensuring the identity and information security of transaction participants poses a significant challenge for the system. Addressing these three aspects, this paper proposes the EFSC(Efficient, Flexible, Secure Computing-power-trading) system to tackle these issues and challenges.

IV. Methodology

The architecture of our proposed EFSC system is depicted in Figure 1, comprising two main parts: the blockchain and off-chain segment. The blockchain part encompasses an identity chain and a transaction chain, while the off-chain segment includes the computing power trading DApp (DAPP) and the transaction channel controller (TCC).

A. Identity Chain

On the identity chain, user DID documents and user-specific verifiable credentials, such as proof of qualification for certain computing power services, are stored. Upon registration of a digital identity (i.e., DID), a DID is assigned to the user, with the corresponding private key held by the user and the associated public key stored within the DID document. Subsequently, the DID document is written onto the identity chain, thereby ensuring its storage on the blockchain.

B. Transaction Chain

On the transaction chain, data relevant to transactions is stored, with the settlement data saved on the transaction chain in the form of evidences of VC. Computing power transactions typically involve a transaction initiation event, signifying consensus between the parties on a specific transaction contract or agreement and the commencement of trading according to said agreement. Additionally, computing power transactions are typically billed based on time usage, necessitating a mechanism for scheduled settlement. Based on the characteristics of computing power transactions outlined above, this proposal presents an efficient, flexible and secure method for computing power transactions. It mainly solved the issues of transaction efficiency, flexibility and security via a combination of on-chain and off-chain method and a data model based on VC.

1) Transaction Efficiency: To enhance transaction efficiency, we propose a hybrid on-chain and off-chain transaction method. A TCC is connected to a transaction chain node, serving as a control program for dynamically initiating or terminating transaction channels. Each transaction channel facilitates data exchange between the transaction parties and can be viewed as a data transmission pipeline.

The creation of transaction channels can be implemented via message publishing subscription mechanisms like message queue (MQ) or Advanced Messages Onchain Protocol (AMOP)[6]. Once a transaction channel is created, the transaction parties can utilize the channel to send and confirm timed settlement messages (e.g., every 1 minute or 5 minutes). These timed settlement messages are exchanged off-chain, and the settlement data is not recorded on the blockchain, thereby significantly improving settlement processing efficiency. Furthermore, each transaction channel program runs on a TCC that is distributed and connected to a transaction chain node, thereby avoiding the occurrence of hub nodes (i.e., localized central nodes). In addition to the aforementioned advantages, the overall load of on-chain settlement processing can be controlled by adjusting the time span of the on-chain settlement strategy. For instance, after N timed off-chain settlement cycles, a transaction channel can initiate a request for on-chain settlement processing to record the evidence of last settlement on the blockchain. When the on-chain data processing queue is lengthy (indicating a high load of on-chain settlement processing), increasing the value of N can reduce

[3]https://w3c-ccg.github.io/did-resolution/#ref-for-dfn-did-document-1

[4]https://w3c-ccg.github.io/did-resolution/#ref-for-dfn-did-resolution-1

[5]https://www.w3.org/TR/did-spec-registries

[6]https://fisco-bcos-documentation-en.readthedocs.io/en/latest/docs/AMOP/README.html

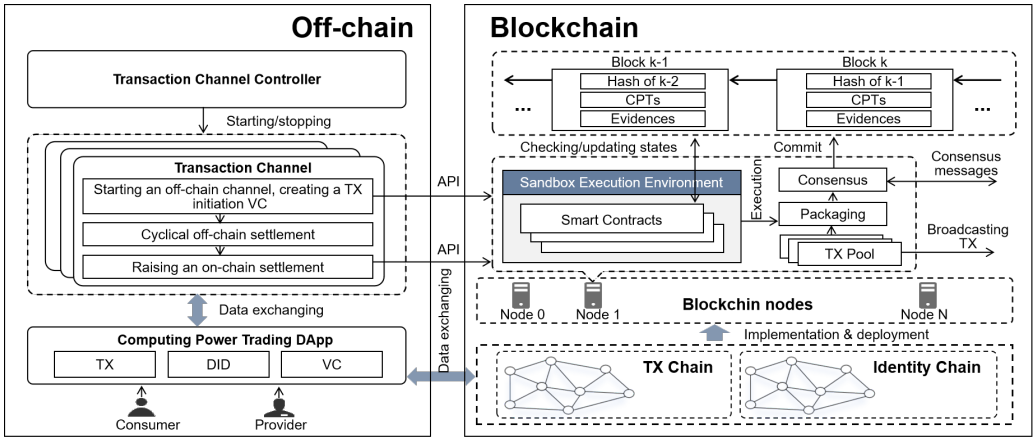

Fig. 1. The structure of proposed EFSC system.

the concurrency of on-chain settlement processing requests, thereby alleviating the system's on-chain processing pressure.

2) Transaction Flexibility: To support flexible trading modes, we designs 4 critical data structures based on the VC data model, including two types of Claim Protocol Type (CPT) templates and two types of VCs. A CPT Template refers to a digital credential template that defines the data fields included in the claim data, along with the data types of each field, and specifies which fields are required. A VC includes issuer ID, issuance time, expiration date, claim data, issuer digital signature etc. The proposed data structures of CPT template and VC are elaborated as follows:

Transaction Initiation Template (TIT) is used to initiate a transaction and is defined and registered by the computing power provider. It can be likened to a transaction contract or agreement template, defining the necessary data fields for initiating the transaction. It typically includes fields such as provider DID, consumer DID, computing power specifications, unit price of computing power, settlement strategy, initial pricing, settlement CPT ID and data encryption method.

Transaction Settlement Template (TST) is a template for conducting transaction settlement off-chain, and is defined and registered by the computing power provider. It defines the data fields involved in a transaction settlement, typically including provider DID, consumer DID, fee, start and end times, and data encryption method.

Transaction Initiation Credential (TIC): is created and applied for by a computing power consumer, and subsequently issued by a computing power provider. Later the issued TICs are recorded on the blockchain. The claim data of the credential is based on the field requirements of the TIT and the actual data provided.

Transaction Settlement Credential (TSC) is used for off-chain settlement. Its creation involves both transaction parties that added their signatures of the claim data. After creation, it is submitted to a TCC via a transaction channel. It is then issued by the TCC on behalf of the associated transaction chain node. The claim data of the credential is based on the field requirements of the TST and the actual settlement data.

Computing power providers are able to define a customized computing power trading pattern according to their requirements (e.g., offering different quotations for different time periods, adding some motivational factors, specific billing strategy) via registering TIT and TST, and later handling corresponding creation or issuance requests for verifiable credentials (such as TIC, TSC).

C. Off Chain Processing Unit

The off-chain processing units mainly consist of the Transaction Channel Controller and the computing power trading DApp:

Transaction Channel Controller (TCC) is a control program for transaction channels, capable of dynamically starting or stopping a transaction channel. A TCC is connected to a transaction chain node and can be deployed as an extension program on the node itself or on a host outside the node, connected to the node via a network. Transaction chain nodes can notify the associated TCC to create or close a transaction channel through remote invocation interfaces or asynchronous message events.

1) Transaction Security: The processing flow of a computing power transaction from initiation to on-chain settlement is illustrated in Figure 2. **Step 1**: The transaction parties obtain transaction quotation information from the transaction chain node through the DAPP, make transaction decisions, and initiate a computing power transaction using a TIT. **Step 2**: the TCC creates a transaction channel for the transaction parties, with parameters including the DIDs of the transaction parties, their public keys, TIC data, and a TST. **Step 3**: After a transaction channel is created, to ensure transaction security, the transaction parties need to use DIDs and their private keys for secure access authentication when connecting to the transaction channel. **Step 4**: the transaction parties conduct periodic settlement through the off-chain transaction channel, with each off-chain settlement data exchanged in the form of VC. Finally, after N off-chain settlement cycles, an on-chain settlement request is initiated by the transaction parties via a TCC, submitting an evidence of the last off-chain settlement credential to the blockchain.

Computing Power Trading DApp (DAPP) is a decentralized application that connects to blockchain nodes through

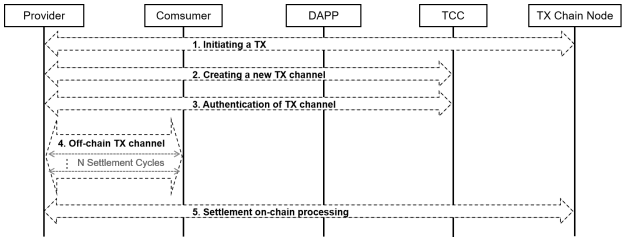

Fig. 2. A TX processing flow from initiation to on-chain settlement

smart contract interfaces or remote call interfaces, while also facilitating blockchain data access and interaction for trading users. The DAPP mainly consists of the transaction module, the DID service module, and the VC service module. The transaction module comprises two main functionalities: transaction initiation processing and transaction closure processing. The DID service module primarily involves registering identity DIDs, identity verification, identity querying and updating. The VC service module encompasses CPT management and credential management functionalities.

V. Simulation Result and Analysis

A. Experiment Settings

We use FISCO BCOS (v3.4.0), an open source consortium blockchain system, initiating four blockchain nodes (the minimum number for PBFT[24] consensus) on the same server, with each node also serving as a consensus node. The detailed environment of our hardware and software environment is given by Tab I.

TABLE I
Detail description of experimental environment.

	data field	description
1	Chassis	NF5280M5
2	CPU	Xeon 8160 (24 cores, 48 threads)
3	RAM	768GB
4	SSD	3.84TB
5	OS	Ubuntu 20.04
6	Software and packages	MySQL, MySQL-Python, JDK 1.8,Python3.6, Docker

Additionally, leveraging the open-source code of WeIdentity (a blockchain solution of DID and VC), we have developed performance testing and verification programs to conduct experiments on both off-chain transaction efficiency and on-chain processing efficiency.

B. Off-Chain transaction processing performance

The primary overhead in off-chain transaction for periodic settlement processing is the issuance of periodic settlement credentials which is performed on a TCC. Concerning the credential issuance performance of a TCC, specifically the number of credentials issued per second, we conducted tests on claim data sizes D of 1KB, 2KB, and 4KB. The experimental results in Tab II indicate that the size of the claim data has minimal impact on issuance performance, with issuance speeds generally exceeding $11K/s$. The total issuance throughput of the system increases with the number of TCCs, and theoretically it is directly proportional to the number of TCCs.

TABLE II
Off-chain processing speed.

	D=1KB	D=2KB	D=4KB
Number of signed VCs per second	11566	11340	11109

C. On-Chain processing performance

An on-chain recording of the last settlement's evidence will be triggered after a certain number of off-chain transaction settlements. An on-chain evidence mainly includes a hash of a settlement credential and the data signed by issuers regarding this hash. Therefore, the size of evidence data is generally fixed and unaffected by the size of the credential claim data. The open-source WID Evidence on-chain smart contract[7] was used as the test smart contract. We conducted a series of experiments to measure the evidence on-chain processing speed which is the number of evidence records that can be written into the blockchain per second. Due to varying influences of the maximum evidence count per block, denoted by variable M, we conducted experiments for different values of M: 1, 2, 4, 8, 16, 32, 64, 128, and 256, respectively, and recorded the number of evidences that could be completed per second for each setting, and the on-chain storage overhead of each evidence record.

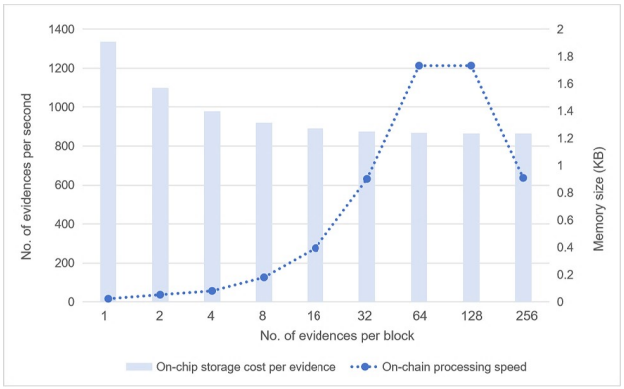

Fig. 3. On-chain processing speed and on-chain storage overhead.

From Fig 3, it can be observed that as the maximum evidence count per block, denoted as M, increases from 1 to 64, the speed of evidence on-chain processing significantly increases, reaching a maximum processing speed of approximately $1.2K/s$. When M increases from 64 to 128, the evidence on-chain processing speed remains relatively unchanged. However, when M is set to 256, the evidence on-chain processing speed shows a noticeable decrease. In addition, the on-chain storage overhead slowly decreases as the maximum number of evidences in block packing increases, from 1.9KB to about 1.2KB per evidence. Analysis of block logs reveals that even when M is set to 256 or higher, the actual number of evidences packed into a block is 160. This reduction in processing efficiency is due to the insufficient number of evidences waiting to be packed after the completion of processing the previous block, failing to meet the requirements for the number of evidences needed for block packing.

[7]https://github.com/FISCO-BCOS/evidenceSample

Consequently, this triggers an internal processing timer within the program, which determines the minimum block packing interval (the default interval is configured as 500 ms), leading to an overall decrease in processing efficiency. Decreasing the value of this timer may result in fewer evidences being packed into blocks, thus impacting processing efficiency. To achieve maximum processing performance on a specific server without modifying the open-source code, it is necessary to optimize and adjust relevant parameter values (such as block packing interval time and M) to maximize overall throughput.

In the above experimental setting, when the off-chain settlement reaches about $11K/s$ the maximum throughput of a TCC, setting the number of off-chain settlements per on-chain processing $n \geq 10$ can ensure the efficiency of evidence on-chain processing (maximum speed $\approx 1.2K/s$). The experiment results demonstrate the transaction efficiency of the proposed hybrid mechanism combining on-chain and off-chain processing, and it largely fulfills the requirement for instant settlement of high-frequency transactions.

D. Settlement Security Analysis

The settlement security mechanism is provided during two phases: Phase-1 Channel-setup and Phase-2 Settlement.

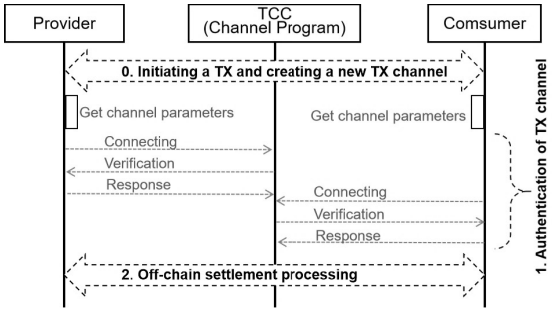

Fig. 4. The process of identity authentication.

Phase 1 Channel-setup: The transaction initiation process involves creating a TIC, completing the PBFT consensus, and then storing the TIC on the blockchain. In the case of a total number of nodes being g, the maximum number of fault-tolerant nodes supported by the PBFT consensus is $(g-1)/3$, thereby tolerating the occurrence of nearly one-third of nodes failing or being maliciously captured as attack nodes.

Once the TIC is stored on the blockchain, the TCC creates an off-chain transaction channel to serve the transaction parties. When the transaction parties access the channel, they need to undergo identity security authentication. As illustrated in Figure 4, transaction parties retrieve transaction channel access parameters from the transaction chain node via the DAPP. Subsequently, they connect to a designated transaction channel of TCC and provide their DIDs. The transaction channel program verifies if the accessing DID is in the admission list based on the parameters passed during creation. If it is, it retrieves the accessing user's DID identity document from the blockchain, reads the corresponding public key, creates random data, encrypts it using the public key, and then returns an identity verification request containing the ciphertext. Upon receiving the identity verification request, the transaction parties decrypt the ciphertext using their private key, and then respond with the plaintext to the transaction channel program to complete the access identity verification. From the above process, it can be observed that the security of channel accessing relies on the security of asymmetric keys, ensuring the security of access identities as long as the keys are not leaked or cracked.

Phase 2 Settlement: Each off-chain settlement is conducted and stored in the form of a TSC, which includes a digital signature V_{proof} of a TCC on behalf of a transaction-chain node, the TCC's DID V_{tdid}, a CPT template ID V_{cptid}, and the credential claim data V_{claim}. The V_{claim} contains the provider's DID C_{pdid}, the consumer's DID C_{cdid}, specific transaction data C_{data}, and a joint signature C_{proof} by both parties involved in the transaction.

During verification:

$$Valid/Invalid \longleftarrow Verify(V_{proof}, V_{tdid}, V_{cptid}, V_{claim}). \quad (1)$$

The Equation 1 indicates that the credential is considered valid only if the verification passes, allowing further validation of the credential claim data.

$$Valid/Invalid \longleftarrow Verify(C_{proof}, C_{pdid}, C_{cdid}, C_{data}). \quad (2)$$

The above equation shows that the data validity is established upon successful verification, ensuring the authenticity of the data; otherwise, it is deemed invalid.

The control and storage of TSC data are autonomously managed by the transaction parties, empowering users with the authority to select their preferred storage methods. Moreover, data interaction revolves around the transaction users, allowing them to provide data verification for any third-party on blockchain nodes according to their preferences, thus ensuring the credibility and security of the data.

After a number of off-chain settlement cycles, the hash of the most recent off-chain settlement credential is recorded as settlement evidence on the blockchain. This integration of off-chain settlement credential with on-chain evidence enhances the credibility and traceability of the transaction settlement.

VI. Conclusion

In this paper, we introduces the EFSC (Efficient, Flexible, Secure Computing-power-trading) system, which addresses the efficiency and security concerns inherent in blockchain-based transactions within the computing power trading scenario. We have demonstrate the proposed system has appealing characteristics on efficient transactions, flexibility in diverse trading patterns and security assurance on both transactions and participants. Experimental results and analysis demonstrate the effectiveness of the proposed EFSC system in addressing the efficiency and security challenges associated with blockchain-enabled computing power networks.

Acknowledgment

Thanks for the anonymous reviewers for their helpful comments. This work was funded in part by the Shandong Key R&D Program (No. 2020CXGC010106) and the Technology Program of Guangzhou, China (No. 202103050004).

REFERENCES

[1] J. Li, B. J. Cairns, J. Li, and T. Zhu, "Generating synthetic mixed-type longitudinal electronic health records for artificial intelligent applications," *npj Digit. Medicine*, vol. 6, 2023. [Online]. Available: https://doi.org/10.1038/s41746-023-00834-7

[2] F. Liu, T. Zhu, X. Wu, B. Yang, C. You, C. Wang, L. Lu, Z. Liu, Y. Zheng, X. Sun, Y. Yang, L. A. Clifton, and D. A. Clifton, "A medical multimodal large language model for future pandemics," *npj Digit. Medicine*, vol. 6, 2023. [Online]. Available: https://doi.org/10.1038/s41746-023-00952-2

[3] Y. Li, S. Wang, H. Ding, and H. Chen, "Large language models in finance: A survey," in *4th ACM International Conference on AI in Finance, ICAIF 2023, Brooklyn, NY, USA, November 27-29, 2023*. ACM, 2023, pp. 374–382. [Online]. Available: https://doi.org/10.1145/3604237.3626869

[4] X. Wang, X. Ren, C. Qiu, Y. Cao, T. Taleb, and V. C. M. Leung, "Net-in-ai: A computing-power networking framework with adaptability, flexibility, and profitability for ubiquitous AI," *IEEE Netw.*, vol. 35, no. 1, pp. 280–288, 2021. [Online]. Available: https://doi.org/10.1109/MNET.011.2000319

[5] L. Lin, J. Wu, Z. Zhou, J. Zhao, P. Li, and J. Xiong, "Computing power networking meets blockchain: A reputation-enhanced trading framework for decentralized iot cloud services," *IEEE Internet of Things Journal*, 2024.

[6] X. Tang, C. Cao, Y. Wang, S. Zhang, Y. Liu, M. Li, and T. He, "Computing power network: The architecture of convergence of computing and networking towards 6g requirement," *China communications*, vol. 18, no. 2, pp. 175–185, 2021.

[7] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, ser. EuroSys '18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https://doi.org/10.1145/3190508.3190538

[8] H. Li, Y. Chen, X. Shi, X. Bai, N. Mo, W. Li, R. Guo, Z. Wang, and Y. Sun, "Fisco-bcos: An enterprise-grade permissioned blockchain system with high-performance," in *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, ser. SC '23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi.org/10.1145/3581784.3607053

[9] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[10] Q. Lu, X. Xu, H. M. N. D. Bandara, S. Chen, and L. Zhu, "Patterns for blockchain-based payment applications," in *EuroPLoP'21: European Conference on Pattern Languages of Programs 2021, Graz, Austria, July 7 - 11, 2021*. ACM, 2021, pp. 28:1–28:17. [Online]. Available: https://doi.org/10.1145/3489449.3490006

[11] R. P. Sarode, D. G. Singh, Y. Watanobe, and S. Bhalla, "High-volume transaction processing in bitcoin lightning network on blockchains," *Int. J. Comput. Sci. Eng.*, vol. 26, no. 4, pp. 445–458, 2023. [Online]. Available: https://doi.org/10.1504/IJCSE.2023.132151

[12] R. Network, "What is the raiden network," *URL: https://raiden. network/101. html*, 2018.

[13] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the NFT ecosystem," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, H. Yin, A. Stavrou, C. Cremers, and E. Shi, Eds. ACM, 2022, pp. 667–681. [Online]. Available: https://doi.org/10.1145/3548606.3559342

[14] Y. H. He, "Research on the network security and identity authentication technology," *Advanced Materials Research*, vol. 926, pp. 2819–2822, 2014.

[15] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *Journal of network and computer applications*, vol. 166, p. 102731, 2020.

[16] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui, and J. Wang, "A privacy-preserving identity authentication scheme based on the blockchain," *Security and Communication Networks*, vol. 2021, pp. 1–10, 2021.

[17] Z. Chen, L. Zhang, S. Zhang *et al.*, "Access control scheme on blockchain and decentralized attributed-based algorithm with identity," *Scientia Sinica Informationis*, vol. 51, no. 8, pp. 1345–1359, 2021.

[18] S. Rouhani and R. Deters, "Blockchain based access control systems: State of the art and challenges," in *IEEE/WIC/ACM International Conference on Web Intelligence*, 2019, pp. 423–428.

[19] S. Malik and M. A. Shah, "Access control using blockchain: A taxonomy and review," in *Proceedings of the 6th International Conference on Information System and Data Mining*, 2022, pp. 46–54.

[20] Y. Liu, M. Qiu, J. Liu, and M. Liu, "Blockchain-based access control approaches," in *2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2021, pp. 127–132.

[21] R. Du, A. Tan, and J. Tian, "Public key searchable encryption scheme based on blockchain," *Journal on Communications*, vol. 41, no. 4, pp. 114–122, 2020.

[22] L. Wang, F. Gao, Q. Li, and Z. Chen, "Blockchain-based multi-recipient multi-message signcryption scheme," *Journal of Software*, vol. 32, no. 11, pp. 3606–3627, 2021.

[23] F. Zhou, Z. Jiao, Q. Wang, and J. Sun, "Bcvse: Verifiable searchable encryption scheme with blockchain supporting fuzzy query," *Arabian Journal for Science and Engineering*, pp. 1–18, 2023.

[24] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, ser. OSDI '99. USA: USENIX Association, 1999, p. 173–186.