Journal of Electronic Research and Application, 2025, Volume 9, Issue 5
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Data Elements and Trustworthy Circulation: A Clearing and Settlement Architecture for Element Market Transactions Integrating Privacy Computing and Smart Contracts

Huanjing Huang

440306198511260035, Shenzhen 518000, Guangdong, China

Abstract: This article explores the characteristics of data resources from the perspective of production factors, analyzes the demand for trustworthy circulation technology, designs a fusion architecture and related solutions, including multi-party data intersection calculation, distributed machine learning, etc. It also compares performance differences, conducts formal verification, points out the value and limitations of architecture innovation, and looks forward to future opportunities.

Keywords: Data elements; Privacy computing; Smart contracts

Online publication: October 15, 2025

1. Introduction

With the rapid development of the digital economy, the importance of data as a key factor of production is becoming increasingly prominent. The Opinion on Building a More Comprehensive System and Mechanism for Market-Oriented Allocation of Factors, released in 2020, emphasizes the need to accelerate the cultivation of the data factor market. In this context, the marketization of data elements faces many challenges and opportunities. From the perspective of production factors, there are problems in defining property rights, forming value, and market-oriented transactions; There are dual technical requirements for analyzing trustworthy circulation from the perspectives of information security and process trust. This article focuses on these issues and proposes an architecture that integrates privacy computing and smart contracts. It explores its application and related technical solutions in the clearing and settlement of data element market transactions, which have important academic and practical significance.

2. Theoretical basis of the data element market and trustworthy circulation

2.1. The core characteristics and operational mechanism of the data element market

From the perspective of production factors, data resources have unique attributes. The definition of its property rights is complex, and due to the replicability and multi-source nature of the data, it is difficult to clarify ownership. The formation of value is influenced by various factors, including data quality, application scenarios, etc. In terms of market-oriented transactions, data ownership is a key prerequisite, but current technology is difficult to accurately determine the rights holders of data. Pricing also faces challenges, as the value of data varies depending on application scenarios and users, and there is a lack of unified pricing standards. There are also problems with supply-demand matching, as the diversity and dispersion of data make it difficult to efficiently achieve supply-demand integration. At the same time, technological constraints and institutional bottlenecks coexist, and there is a lack of effective data protection and transaction security measures in technology. Relevant laws and regulations in the system are not yet sound, which affects the healthy operation of the data factor market [1].

2.2. Dual technical requirements for trustworthy circulation

Analyze the dual technical requirements of trustworthy circulation from the perspectives of information security and process trust. In terms of information security, data privacy protection is crucial. With the development of the data element market, it is necessary to ensure that data is available and invisible in circulation to protect the privacy and rights of data owners. Privacy computing technology plays a crucial role in this regard, as it enables data analysis and utilization without compromising data privacy. In the dimension of process trust, the reliability and automatic execution of the transaction process are key [2]. Smart contracts, with their advantage of automated execution of transaction rules, can ensure the fairness and transparency of transactions, reduce human intervention and errors, enhance the trust of the transaction process, and promote the trustworthy circulation of data elements.

3. The overall design framework of integrated architecture

3.1. Hierarchical system architecture design

The fusion architecture design includes a hierarchical system architecture with four layers. The data resource layer is responsible for storing and managing data, providing a data foundation for the upper layer. This layer ensures that data is properly organized, indexed, and accessible, which is crucial for the smooth operation of the entire system. The privacy computing layer utilizes technological means to calculate and analyze data while protecting data privacy, ensuring the security and compliance of data during circulation and use. This layer incorporates advanced encryption techniques and secure multi-party computation methods to safeguard sensitive information without compromising functionality. The smart contract layer standardizes the transaction rules and processes of data elements through the form of smart contracts, achieving automated transaction execution and supervision [3]. This layer ensures that all transactions are conducted in a transparent, fair, and tamper-proof manner, reducing the need for intermediaries and minimizing the risk of fraud. The clearing and settlement layer is mainly responsible for clearing and settling data element transactions, ensuring the accuracy and fairness of transactions. This layer provides robust mechanisms for financial transactions, ensuring that all parties receive accurate and timely settlements. Each layer has clear functional positioning and interface standards, and efficient collaboration and data transfer between layers are achieved through reasonable interface design. This architecture not only ensures data security and privacy but also enhances the efficiency and transparency of data transactions, making it a robust framework for promoting the trustworthy circulation of data elements in a complex digital environment.

Additionally, the architecture is designed to be scalable and adaptable, allowing for future enhancements and integration with emerging technologies such as blockchain and artificial intelligence, which further strengthen its ability to support the evolving needs of the data-driven economy.

3.2. On-chain and off-chain collaboration mechanism

In the element market transaction clearing and settlement architecture that integrates privacy computing and smart contracts, the collaborative operation of the blockchain-based contract execution layer and privacy computing nodes is crucial. This collaboration ensures that the strengths of both blockchain and privacy computing are fully leveraged to enhance the security, transparency, and efficiency of the entire transaction process. By designing a reasonable collaborative operation model, the responsibilities and interaction methods of all parties involved can be clearly defined [4]. For data flow and control flow, specialized interaction protocols need to be established to ensure accurate transmission and interaction of data on and off the chain. Meanwhile, the verification mechanism is indispensable as it can rigorously verify the authenticity, integrity, and compliance of the interaction process of data, prevent data leakage and erroneous operations, and ensure the security and efficiency of clearing and settlement of factor market transactions. This architecture not only addresses the challenges of data privacy and security but also provides a robust framework for trustworthy and efficient transactions in the element market.

4. Key technology implementation path

4.1. The integrated application of privacy computing technology

4.1.1. Application of secure multi-party computation in data comparison

Design a multi-party data intersection calculation scheme based on secret sharing, utilizing secure multi-party computing technology to protect sensitive fields of transaction subjects during data comparison. By using a secret sharing mechanism, data is segmented and distributed to multiple participants for computation without leaking the original data. Each party performs calculation operations based on its own data shares, and finally combines the results through specific algorithms to obtain the intersection information of multi-party data [5]. This approach not only ensures the privacy and security of data but also provides a highly efficient and scalable solution for data comparison. It enables effective verification and processing of relevant data during the clearing and settlement process of data element market transactions while protecting sensitive information. Additionally, the scheme is designed to be resilient against potential collusion attacks among participants, ensuring robustness and reliability in a variety of complex scenarios. This makes it an ideal choice for enhancing the trustworthiness and security of data transactions in the digital economy.

4.1.2. Federated learning modeling framework

Build a distributed machine learning model training mechanism and use homomorphic encryption technology to ensure the privacy protection of model parameters during the aggregation process [6]. Homomorphic encryption allows specific computational operations to be performed directly on ciphertext, enabling parameter aggregation in model training without leaking the original data. In the federated learning modeling framework, the data of each participant is kept locally, and collaborative training of the model is achieved through encrypted transmission and aggregation of model parameters. This approach not only avoids direct data sharing but also enhances the security of the entire training process by ensuring that sensitive information remains encrypted throughout. It protects the privacy and security of data from all parties while fully utilizing the value of data to improve the performance and

accuracy of the model. Additionally, this mechanism is designed to be highly scalable and adaptable to various data environments, making it suitable for large-scale distributed machine learning applications where data privacy is paramount.

4.2. Enhanced design of smart contracts

4.2.1. Verifiable calculation contract template

Developing a universal contract framework that supports zero-knowledge proofs requires consideration of multiple factors. Firstly, it is necessary to clarify the basic structure and functional modules of the framework, including the design of input and output interfaces, which should be able to adapt to different privacy computing scenarios and data formats. In the selection of zero-knowledge proof algorithms, it is necessary to comprehensively consider computational efficiency, security, and scalability. For the collaborative verification mechanism between on-chain verification and off-chain computing, it is necessary to establish an efficient communication protocol to ensure that the off-chain computing results can be accurately verified on-chain [7]. At the same time, it is necessary to design reasonable verification rules and processes, conduct comprehensive inspections of off-chain computing processes and results, and prevent malicious tampering and uploading of erroneous results. Through these technological means, the effective enhancement of smart contracts in a private computing environment can be achieved, ensuring the credibility and efficiency of data element market transaction clearing and settlement.

4.2.2. Automated clearing and settlement logic

In the enhanced design of smart contracts, automated clearing and settlement logic is crucial. One of the key paths is to design a multi-stage transaction processing model that includes fund freezing, account splitting settlement, and dispute arbitration. The fund freezing stage ensures the security of transaction funds and prevents issues such as fund misappropriation during the settlement process. During the sub-account settlement stage, funds are accurately allocated to various stakeholders based on preset rules. The dispute arbitration stage provides a mechanism for resolving potential transaction disputes. At the same time, a specification for off-chain data access based on oracle machines will be developed to enable smart contracts to obtain reliable external data, better support the execution of clearing and settlement logic, and ensure the accuracy and fairness of transactions [8].

5. System implementation and verification analysis

5.1. Prototype system construction

5.1.1. Implementation of distributed storage architecture

In the implementation of a distributed storage architecture, a hybrid storage solution combining IPFS and blockchain is adopted. IPFS has advantages such as content addressing and distributed storage, and can efficiently store data shards. By designing a data shard encryption storage mechanism, the security and privacy of data are ensured, and data leakage and tampering are prevented [9]. Meanwhile, establish an integrity verification mechanism to ensure the integrity of data during storage and transmission. By utilizing the tamper-proof and traceable properties of blockchain, the storage and verification of data information is recorded, providing a guarantee for the trustworthy circulation of data. This hybrid storage solution combines the advantages of IPFS and blockchain, providing a reliable distributed storage architecture foundation for the trustworthy circulation of data elements.

5.1.2. High concurrency processing optimization

It is crucial to adopt sharded blockchain technology to achieve high concurrency processing optimization. This technology can effectively improve system throughput and meet the needs of a large number of data element transactions [10]. Sharding divides the blockchain network into smaller, more manageable pieces called shards, each capable of processing transactions independently. This not only enhances the overall efficiency of the system but also ensures that the network can handle a significant increase in transaction volume without compromising on speed or security. At the same time, building a horizontally scalable computing node cluster architecture that can flexibly expand according to business load is essential. When transaction traffic increases, it is convenient to add computing nodes to ensure the stability and efficiency of the system in high-concurrency situations. This architecture allows for the dynamic allocation of computing resources, preventing any single node from becoming overloaded and thus improving the reliability and availability of the entire system. By doing so, it provides strong support for efficient transaction clearing and settlement of data elements in a trustworthy circulation environment, ensuring that the system can adapt to varying levels of demand while maintaining high performance and security standards.

5.2. Typical scenario testing verification

5.2.1. Joint risk control case of financial credit

In the case of joint risk control in financial credit, it is crucial to simulate the joint modeling process of multiple data sources. By constructing practical scenarios and integrating credit data from different financial institutions, including customer basic information, credit records, loan history, etc. Utilizing privacy computing technology for data fusion and analysis without disclosing sensitive data. At the same time, establish smart contracts to standardize the use of data and transaction settlement rules. During this process, the focus is on verifying the balance between privacy protection and model accuracy. By continuously adjusting privacy protection parameters and algorithms, observe the accuracy of the model in risk assessment. The results indicate that reasonable privacy protection settings can maintain high model accuracy while ensuring data security, effectively improve the effectiveness of financial credit joint risk control, and provide a more reliable risk decision-making basis for financial institutions.

5.2.2. Medical data trading scenarios

It is crucial to conduct testing on the encrypted transaction process for sensitive information, such as genetic data, in medical data trading scenarios. By constructing a simulated trading environment, verify the security and accuracy of the ciphertext in various stages of the transaction. Observe the processes of data encryption, transmission, decryption, and transaction confirmation to ensure that the privacy of genetic data is not compromised. At the same time, evaluate the effectiveness of implementing compliance audit functions. Check the completeness and accuracy of audit records, whether they can effectively trace transaction behavior, and ensure that every transaction involving sensitive information complies with relevant regulations and ethical standards. This not only ensures the legality of medical data transactions but also provides a reliable trust foundation for market participants, promoting the healthy development of the medical data element market.

5.3. Performance comparison analysis

5.3.1. Comparison of calculation efficiency indicators

Compare the performance differences between traditional centralized solutions and the architecture proposed

in this paper in terms of response latency and throughput dimensions. In terms of response latency, traditional centralized solutions often suffer from congestion due to centralized processing of large amounts of data and transaction requests, resulting in high response latency. The architecture presented in this article utilizes privacy computing and the distributed processing capabilities of smart contracts to enable parallel processing of multiple tasks, effectively reducing the waiting time for individual tasks and significantly reducing response latency. In terms of throughput, traditional centralized solutions are limited by server performance and network bandwidth, resulting in limited throughput growth in high concurrency situations. The architecture of this article relies on the collaborative work of distributed nodes, which can flexibly expand processing capabilities and maintain high throughput when facing large amounts of data and transactions, demonstrating better computational efficiency and performance advantages.

5.3.2. Safety strength assessment

Based on the Dolev Yao threat model, formal verification is conducted to analyze the security of the architecture that integrates privacy computing and smart contracts through rigorous mathematical logic and reasoning. This model assumes that the attacker has strong computing power and complete control over network communication, and evaluates the security of the system in this extreme case. By analyzing the performance of the system in the face of various potential attacks, the effectiveness of enhancing its resistance to attacks can be quantified. From the perspective of privacy computing, verify its level of protection for data privacy to ensure that data is not leaked during circulation and transactions. From the perspective of smart contracts, verifying the accuracy and immutability of contract execution ensures the fairness and reliability of transaction clearing and settlement, comprehensively evaluates the security strength of the architecture, and provides strong guarantees for the trustworthy circulation of data element markets.

6. Conclusion

This architecture integrates privacy computing and smart contracts, bringing innovative value to the clearing and settlement of data element market transactions. By using relevant technological means to break down data silos and achieve trustworthy circulation of data, the trust cost of all parties involved in transactions has been reduced, and market efficiency has been improved. However, the current architecture has research limitations in cross-chain interoperability and dynamic access control. The imperfect cross-chain interoperability limits the data exchange and collaboration between different blockchain networks, affecting the widespread application of the architecture. Insufficient dynamic access control may lead to increased data security risks. Looking ahead, the integration of 5G edge computing and hardware envelope technology will bring new opportunities for architecture development. This integration is expected to further enhance data processing capabilities and security, provide new ideas and methods for solving existing problems, and promote the continuous improvement of the data element market transaction clearing and settlement architecture.

Disclosure statement

The author declares no conflict of interest.

References

[1] Wang S, Ouyang L, Yuan Y, et al., 2019, Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11): 2266–2277.

[2] Rouhani S, 2021, Data Trust Framework Using Blockchain and Smart Contracts, dissertation, University of Saskatchewan.

[3] Serrano W, 2022, Verification and Validation for Data Marketplaces Via a Blockchain and Smart Contracts. Blockchain: Research and Applications, 3(4): 100100.

[4] Perera S, Hijazi AA, Weerasuriya GT, et al., 2021, Blockchain-Based Trusted Property Transactions in the Built Environment: Development of an Incubation-Ready Prototype. Buildings, 11(11): 560.

[5] Afraz N, Wilhelmi F, Ahmadi H, et al., 2023, Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis. IEEE Access, 11: 95653–95666.

[6] Di Nenno A, 2019, Incentive-Compatible and Privacy-Preserving Data Analytics System enabled by Blockchain and Multiparty Computation, dissertation, Politecnico di Torino.

[7] Mvula F. A Conceptual Secure Blockchain-Based Settlement and Clearing House for Mobile Financial Services in Zambia, dissertation, The University of Zambia, 2020.

[8] Honari K, Rouhani S, Falak NE, et al., 2023, Smart Contract Design in Distributed Energy Systems: A Systematic Review. Energies, 16(12): 4797.

[9] Peters GW, Panayi E, 2016, Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, Springer International Publishing.

[10] Asante M, Epiphaniou G, Maple C, et al., 2021, Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey. IEEE Transactions on Engineering Management, 70(2): 713–739.