https://doi.org/10.26599/IJCS.2023.9100025 International Journal of Crowd Science

DareChain: A Blockchain-Based Trusted Collaborative Network Infrastructure for Metaverse

Qingzhong Li[1,2], Lanju Kong[1,2] ✉, Xinping Min[1,2,3], and Baochen Zhang[1]

ABSTRACT

With the continuous development of digital technology, the metaverse, as a concept of virtual and real fusion, is gradually becoming a reality. However, the development of trusted collaborative network technology that underpins the metaverse is still immature. Blockchain can support the construction of trusted collaborative networks due to its own characteristics of decentralization, transparency, and traceability. However, as blockchain can only support simple digital assets such as digital currencies and tokens, it cannot implement the trusted collaboration of complex digital assets in the metaverse. Therefore, this article proposes a blockchain-based trusted collaborative network infrastructure for future digital economy and society—DareChain. DareChain has proposed a novel collaborative-worker multi-chain system, trusted subject-object account model, layered model of smart contracts supporting trusted interactions, hyperlinear ledger consensus algorithm, and transaction model that supports privacy protection. It has been explored in metaverse applications in various scenarios such as government affairs, medical care, and finance to solve problems such as single content expression, few applications of business scenarios, low throughput, and easy leakage of security and privacy when blockchain is used as the underlying trusted collaborative network for the metaverse.

KEYWORDS

metaverse; trusted collaborative network; blockchain

With the continuous development of digital technology, the metaverse, as a concept of virtual and real fusion, is gradually becoming a reality. The metaverse contains various digital assets, applications, and services. In the metaverse, people can engage in various activities such as socializing, gaming, shopping, etc.

The metaverse is supported by various digital technologies. According to the International Alliance for Crowd Science and Engineering[1] (ACE), these mainly include digital life technology, trusted collaborative network technology, natural interaction technology, ubiquitous operating system technology, computational experimental technology and methods, and crowd science theory and technology. However, the most basic and important aspect is to build a trusted collaborative network infrastructure that provides a trusted channel for multi-party interactions in the metaverse. This ensures support for the metaverse digital world and other technologies while supporting interoperability and connectivity between various applications and services in both the metaverse and real world. Therefore, this trusted collaborative network needs to have high autonomy, security, reliability, and transparency to ensure the safety of user identity and assets while supporting orderly operation of the digital society.

Blockchain is a distributed and trusted transmission technology that can provide a decentralized, tamper-proof, trusted storage, and verification mechanism. By using blockchain technology, a decentralized and trusted collaborative network can be established, where secure, reliable, and transparent data exchange can take place between nodes. The advantages of transparency, anti-tampering, and decentralization of blockchain will lay the foundation of trust for the metaverse.

Looking at the history of blockchain development, from blockchain 1.0 of digital currency to blockchain 2.0 of smart contracts, and then to blockchain 3.0 of trusted society, the application of blockchain technology has extended to various fields in metaverse application scenarios[2] such as digital finance[3], Internet of Things (IoT)[4], intelligent manufacturing[5], digital asset trading, etc., playing the role of a secure and trusted transmission channel[6–10]. However, due to many driving factors such as rapid digitization, networking, intelligence, etc., the metaverse presents increasingly strong demands for crowd intelligent, asset generalization, and trusted collaboration. This poses new challenges for trusted collaborative network technology.

(1) Contradiction between the complexity of subject-object models in the metaverse and the singularity of existing trusted collaborative network models. The ability of collaborative networks to express the attributes, relationships, and operations of subjects and objects determines the digital expression ability of the metaverse. Existing blockchain models[11] usually represent subjects with anonymous accounts and objects with contracts, and their subject-object semantics need to be parsed through contract layers or even application layers, which are only suitable for highly standardized digital currencies, digital tokens, and digital collections. However, metaverse subjects require strict identity authentication, while digital objects exhibit new features such as diversity, non-standardization, and one-to-many rights. From a

1 School of Software, Shandong University, Jinan 250101, China
2 Dareway Software Co., Ltd, Jinan 250101, China
3 Joint SDU-NTU Centre for Artificial Intelligence Research, Shandong University, Jinan 250101, China
Address correspondence to Lanju Kong, klj@sdu.edu.cn

vertical perspective, the subject-object models in the metaverse will also change over time. Blockchain needs to have stronger native support capabilities to adapt to the constantly evolving needs of the metaverse.

(2) Challenge of autonomous collaboration and deep interaction trust models. The connection between subjects and objects in the metaverse is more free, universal, and efficient, and its application scenarios can derive various peer-to-peer transaction relationships. Large-scale peer-to-peer autonomous and deep interaction behaviors are prone to produce double-spending problems in a distributed autonomous environment, which poses great challenges to concurrent control protocols and consistency protocols of transaction under decentralized trust models. As a decentralized collaborative interaction channel in the metaverse, trusted collaborative networks need to further clarify the states and operating rules of digital subject-object lifecycles at each stage to support the security, intelligence, and consistency of the circulation process, prevent double-spending problems during subject-object interactions, and ensure the robustness of the metaverse ecosystem's operation.

(3) Privacy and security challenges of the network-wide transmission/storage/computation mode in collaborative networks. Collaborative networks store massive amounts of subject-object and transaction information in the metaverse, so trust transmission and privacy protection must be considered. Existing blockchain platforms[12–15] rely on technologies such as blind signatures and ring signatures to keep user identities confidential, and use zero-knowledge proofs, coin mixing, etc. to protect transaction patterns, transaction content, etc., which to some extent solves the problem of privacy protection. However, these technologies also make it difficult for blockchain platforms to form a consensus and process more complex operations. How to support open sharing of assets and trusted business collaboration while ensuring user privacy is still a challenge faced by current trusted collaborative network technology.

(4) Increasingly severe performance challenges in trusted collaborative networks. Blockchain technology has always been known for being expensive and inefficient[13,16], and the interconnection of all things, deep interaction, and asset generalization have brought even greater performance pressure to the blockchain-based infrastructure of trusted collaborative networks that support the metaverse. There are various relationships between subjects and objects in the metaverse, and existing blockchain platform hardware upgrades, partial centralization, and multi-chip/chain parallel mechanisms cannot be directly applied in metaverse applications. Many collaborative networks face high input costs of resource and difficulties in linear expansion. How to achieve blockchain performance that is suitable for application scenarios in a large-scale decentralized network environment is an urgent problem that needs to be solved to support the benign expansion of the metaverse ecosystem.

Therefore, to address the above issues, this paper proposes DareChain, a blockchain-based trusted collaborative network infrastructure for the metaverse. It addresses the problems of complex subject-object models in the metaverse, lack of trust in collaboration, easy leakage of security and privacy, and insufficient performance of current collaborative networks. The following contributions have been made:

(1) A blockchain-based trusted collaborative network infrastructure for the metaverse is proposed, providing native digital supportive capabilities, trusted collaborative modes, efficient consensus and processing methods for transactions, and privacy protection capabilities to support the construction of the metaverse and other key technologies.

(2) Propose a collaborative-worker multi-chain system architecture based on collaborative chain and worker chain for metaverse, which includes a new-designed subject and object model and a new transaction structure based on the account model separated by subjects and objects, a trusted collaborative smart contract model with a double-layer smart contract architecture based on business contracts-asset contracts, and a new transaction model and mode which enables the hiding and verification of transaction content, providing inherent privacy protection for transaction processing in the metaverse.

(3) A new ledger structure and consensus algorithm—hyperlinear ledger, is proposed, ensuring fast and effective parallel processing and consensus of massive transactions, supporting horizontal expansion capabilities for metaverse applications.

(4) The proposed trusted collaborative network infrastructure—DareChain has been applied in various fields such as healthcare, government affairs, and finance, and these applications have gained some traction and have some scale.

The following sections will be presented in this paper: Section 1 introduces relevant literature on trusted collaborative technology for the metaverse. Section 2 presents the design of the blockchain-based trusted collaborative network infrastructure. Section 3 describes detailed technological innovations of DareChain. Section 4 provides application cases of DareChain. And finally, Section 5 concludes the paper with future work prospects.

1 Related Work

The collaborative network model[17] can provide a trusted underlying support for data storage and sharing interactions in the metaverse[18,19]. Blockchain, as a decentralized distributed technology, is the main approaches of implementing a trusted collaborative network[20]. Firstly, the collaborative network model can provide secure and reliable data storage services[12] by recording various digital assets and transaction records in the blockchain ledger in the metaverse to ensure that they are not tampered with or deleted. Secondly, the collaborative network model can also achieve cross-chain data sharing by using technologies such as smart contracts to implement automation, decentralization, programmability, etc., enabling data exchange and sharing between different applications for more efficient and convenient cross-chain collaboration[11]. Finally, the collaborative network model can also support trusted interactions between different entities and application scenarios in the metaverse, promoting the circulation and value transfer of digital assets while ensuring privacy security. Therefore, we introduce the current work of combining a trusted collaborative network model with the metaverse from three aspects: data storage, data sharing, and specific applications.

1.1 Trusted collaborative network storage model

The metaverse contains a large amount of digital assets and virtual currencies, and the issue of data storage is a very important one. Traditional data storage methods are centralized, easily tampered with, and difficult to trace, which have a significant impact on the security and credibility of digital assets and virtual currencies. Blockchain technology can achieve decentralized data storage, making data independent of centralized institutions or third-party trust mechanisms, thereby reducing data storage costs and risks. Therefore, using blockchain technology for data storage in the

metaverse is of great significance.

Reference [13] proposed a BlockDatabase system based on blockchain technology, which introduces a system that uses blockchain technology to provide secure distributed data storage through keyword search services. It also provides owners of the data with the ability to grant permission for others to search their data, and the system supports private keyword searches on encrypted datasets.

Yue et al.[14] introduced a blockchain-based data cloud storage integrity verification method, which makes the verification process more effective and open. Reference [15] proposed a blockchain-based distributed cloud storage security architecture. This architecture also customizes a genetic algorithm to solve the problem of replica placement of file blocks among multiple users and multiple data centers in a distributed cloud storage environment, ensuring trustworthy data storage and multi-replica storage.

Li et al.[16] proposed a duplicate data removal scheme that distributes files to multiple servers and records storage information on the blockchain. It also designs a protocol based on smart contracts for storing and deleting data without involving central authorities to provide secure duplicate data removal.

Sukhodolskiy and Zapechnikov[21] proposed a prototype of a multi-user system for access control of datasets stored in an untrusted cloud environment, providing access control to data stored in the cloud without involving providers. The main tool of the access control mechanism is a dynamic attribute encryption scheme based on ciphertext policy attributes, using a blockchain-based decentralized ledger to provide an immutable log of all meaningful security events.

While the above research considers the use of trusted collaboration networks to support the storage of data in the metaverse, it lacks a customized design for metaverse scenarios and does not delve into the underlying value of blockchain as a trusted collaboration network for the metaverse.

1.2 Trusted collaborative network data interaction model

The metaverse is a digital world based on virtual reality technology, and timely data sharing is crucial. However, implementing effective consent management, data exchange, and access control policy execution is not easy, especially in a decentralized environment.

Shafagh et al.[3] delegated data access control to users instead of a centralized trusted institution. By using blockchain as the storage layer for an auditable and distributed access control layer, secure and flexible access control management is achieved. A location-aware distributed storage system managed by blockchain technology is used to promote the storage of time-series IoT data at the network edge.

Raja et al.[22] proposed an AI-driven blockchain that provides automatic encoding for smart contracts, simplifying the process of writing smart contracts, facilitating on-chain functional logic implementation for multiple parties, and ensuring security and efficiency in the data interaction process. In addition, this structure provides a fast transaction verification method, optimizing the cost of multi-party data interaction.

Zhang[23] proposed an interactive design method based on big data rule mining and blockchain communication technology to optimize blockchain data transmission performance. On the basis of ensuring stable and reliable data transmission, further optimization of blockchain data transmission efficiency is achieved by proposing an Integrated Factor Communication Tree algorithm (IFT). To address the impact of transmission delay between nodes on communication performance during node-to-node transmission, a weighted multi-link multi-factor communication tree algorithm considering weights is proposed. To improve blockchain data communication efficiency, ensure transmission reliability, and improve service fairness under constraints such as node communication capability, node trustworthiness, weight, and business request priority level, different strategies for optimizing blockchain data communication performance are proposed.

Ju et al.[24] constructed an image-based interactive traceability structure using images as an enhancement tool. By adding pointers in the original image file to form a specific traceable file structure and separating the traceable process from the verification process, "off-chain traceability" distributed traceability and on-chain verification are achieved.

The above studies have designed some methods and paradigms for data sharing using blockchain as a trusted collaborative network for metaverse, but there is still a lack of clarity on the specific data sharing methods for digital and virtual assets and how to make cross-chain data calls between different blockchains, and such cross-chain transactions lack a clear data structure and model.

1.3 Trusted collaborative network supporting metaverse applications

The metaverse can cover all application scenarios in the physical world, and a trusted collaborative network can provide an interoperable and trusted channel for these applications[2]. Currently, the trusted collaborative network has been explored in multiple metaverse application scenarios such as healthcare, smart cities, IoT, and connected vehicles. In these applications, the trusted collaborative network plays a role in data exchange and trusted transmission, ensuring a large amount of data exchange and sharing between users, applications, and devices.

Liu et al.[4] proposed a blockchain-based data integrity service framework for dynamic environments such as IoT. This framework provides more reliable data integrity verification for both data owners and consumers without relying on trusted third parties to ensure the integrity of cloud-based IoT applications.

Su et al.[5] developed a Lightweight Vehicle-mounted Blockchain Security (LVBS) data sharing framework for disaster relief in unmanned aerial vehicle-assisted IoV. Firstly, a new type of unmanned aerial vehicle and blockchain-assisted disaster area collaborative ground-air network architecture was proposed. Secondly, a credit-based consensus algorithm was developed in the lightweight vehicle-mounted blockchain to securely and immutably track improper behavior of unmanned aerial vehicles and vehicles and record data transactions, improving the efficiency and security of achieving consensus. Thirdly, due to the limited explicit knowledge of unmanned aerial vehicles and vehicles about the entire network, a reinforcement learning based algorithm was developed to optimize pricing and quality of data sharing strategies for scheduling data contributors and consumers through trial-and-error optimization.

Liu et al.[6] proposed a Blockchain-based Privacy-preserving Data Sharing (BPDS) scheme for Electronic Medical Records (EMR). In BPDS, the original EMR is securely stored in the cloud while the index is kept on an immutable alliance blockchain. This greatly reduces the risk of medical data leakage while ensuring that electronic medical records cannot be arbitrarily modified. Through blockchain smart contracts, secure data sharing can be

automatically completed based on predefined patient access permissions.

Makhdoom et al.[7] proposed "PrivySharing", an innovative blockchain-based framework for protecting privacy and security in IoT data sharing in smart city environments. Data privacy is protected by dividing the blockchain network into various channels, each consisting of a limited number of authorized organizations that handle specific types of data such as health, smart cars, smart energy, or financial details.

Kang et al.[8] utilized alliance blockchain and smart contract technology to achieve secure data storage and sharing in vehicle edge networks. These technologies effectively prevent unauthorized data sharing while proposing a reputation-based data sharing scheme to ensure high-quality data sharing between vehicles. A three-weight subjective logic model is used to accurately manage vehicle reputations.

Yang et al.[9] proposed a non-interactive, attribute-based access control scheme that applies blockchain technology to IoT scenarios using the Private Set Intersection (PSI) technology. In addition, the attributes of data users and data holders are hidden, protecting the privacy of both parties' attributes and access policies.

Al Omar et al.[10] proposed a patient-centered healthcare data management system that uses blockchain as storage to achieve privacy. By using encryption to protect patient data, patient anonymity is ensured.

These literatures have designed certain trusted collaborative networks to support metaverse application, but there is still no generalized framework that can be applied to all metaverse applications.

2 Trusted Collaborative Network Infrastructure for the Metaverse

2.1 Overall architecture design

This paper proposes a blockchain-based trusted collaborative network infrastructure called "DareChain", which aims to support the one-to-one mapping of physical entities and objects in the real world to digital entities and objects in the metaverse, and provide a trusted self-explanatory semantic model for them and make the real transactions more trusted and collaborative. The DareChain model supports platform self-explanation and flexible expansion, making it adaptable to changing demands in the digital world. This model fundamentally solves problems such as missing attributes and relationships of entities, uncontrollable behavior, and traceability problems, thus supporting a trusted and evolvable digital world.

The overall architecture design of DareChain can be seen in Fig. 1. The DareChain network model can be organically combined with key technologies in the metaverse such as crowd science, digital life, ubiquitous operating systems, computational experiments, and natural interaction to jointly achieve a complete and trusted metaverse ecosystem. The complete trusted self-explanatory semantic model of entities provided by DareChain serves as a foundational support for the implementation of digital life technology and the development of crowd science in the metaverse. This trusted collaborative network proposed in this paper provides users with a trusted interaction mode for the metaverse through smart contracts combined with natural interaction technology. It can also ensure the computation and storage of massive complex transactions through computational experiment technology, ultimately providing users with a simple and easy-to-use infrastructure through ubiquitous operating systems.

DareChain is a comprehensive architecture model that includes multiple elements, such as a collaborative-worker multi-chain system architecture for collaborative chain-worker chain interaction, subject-object model, layered smart contract model, hyperlinear ledger consensus algorithm, and privacy-protected trusted collaborative model. This architecture covers basic elements such as subjects, objects, smart contracts, transactions, ledgers, nodes, and includes basic processes such as subject definition, asset definition, asset transaction, consensus accounting, contract deployment and operation, cross-chain interaction, and integration inside and outside the chain. Through the improved DareChain model, various data and resource elements in the metaverse can be absorbed in DareChain by bidirectional blockchain Oracle, and the trusted DareChain also provides functions, such as developer service, digitalization of assets, and blockchain-based applications. So that on a digital level various data can be integrated and utilized to the fullest extent

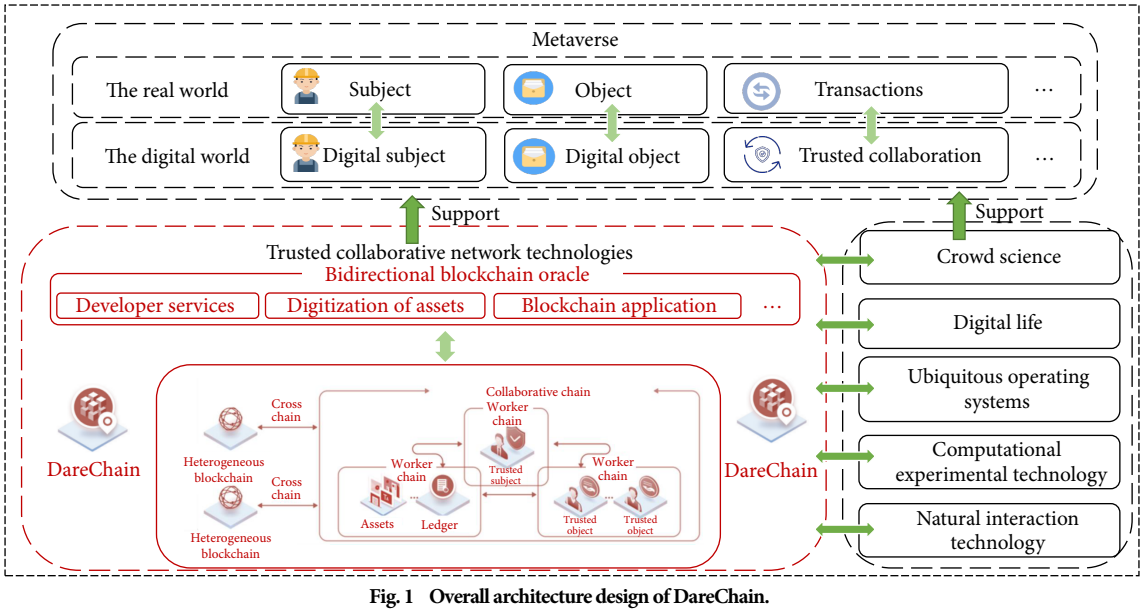

Fig. 1 Overall architecture design of DareChain.

possible while crossing geographical boundaries in reality to maximize their utility. This provides solid support for the construction of the digital world in the metaverse, and implements all users' ownership and control over their digital identity and personal data in the metaverse. It lays a foundation of trust for interaction between subjects and objects in the metaverse.

2.2 Architecture of the collaborative-worker multi-chain system

The metaverse contains multiple application ecosystems, and these application scenarios require secure, trusted, and efficient data exchange and complex transaction patterns to support massive multi-ecosystem application transactions and cross-chain interoperability between different applications. Therefore, DareChain has designed a collaborative-worker multi-chain architecture based on collaborative chain and worker chain, which not only has the ability of horizontal expansion and business isolation, but also provides a cross-chain interaction model for multiple application scenarios in the metaverse.

This multi-chain architecture can effectively meet the needs of different business scenarios in the metaverse while ensuring mutual isolation between various businesses, thereby improving the security and reliability of the entire system. Moreover, under the premise of multi-chain interoperability and eliminating blockchain "data islands", this architecture can greatly reduce collaboration costs, save resource consumption, improve collaboration efficiency, implement an effective mapping of complex business logic in the physical world to the digital world in the metaverse, and solve data sharing and business coordination problems across levels, regions, systems, departments, and businesses.

(1) Collaborative multi-chain system based on collaborative chain and worker chain

As shown in Fig. 2, the multi-chain system of collaborative chain and worker chain adopts methods such as sharding and partitioning, drawing on the pattern of transaction manager and resource manager in the database system. In this multi-chain system, the member management function of the collaborative chain maintains the status of subjects, contracts, worker chains, and nodes. The worker chain management and cross-chain management modules implement the management of multiple worker chains and cross-chain transaction processing. The information routing and relay service module implements the information forwarding and interaction of multiple chains.

The worker chain is responsible for maintaining the status of assets and transaction records. The specific transaction information of assets is recorded in the worker chain, and each worker chain can be homogeneous or heterogeneous. Different application fields can independently build their own worker chains and connect them to the collaborative chain to achieve interaction with other worker chains through the collaborative chain. For example, in the field of intelligent medical care, medical institutions can build a medical metaverse and construct a medical worker chain to upload patients' medical records and medical insurance information. At the same time, the medical worker chain can interact with other field's worker chains through collaborative chain, such as querying patients' historical financial insurance records.

In the collaborative-worker multi-chain system, individuals, institutions, companies, and government departments are all subjects, and the numerous nodes in the worker chain are provided by institutions and governments. They can participate in various aspects of consensus, transactions, storage, etc. in the blockchain-based collaborative network. In order to fully tap the performance potential of each node, we have decoupled the nodes from the architecture level. Specifically, we divide the nodes under the multi-chain architecture into consensus nodes, transaction nodes, light nodes, custody nodes, and asset storage nodes.

The light node is suitable for units with low transaction volume and storage space. It only stores key information such as transactions related to this node. The transaction node stores the entire ledger, but does not participate in consensus and provides external access services. The consensus node participates in

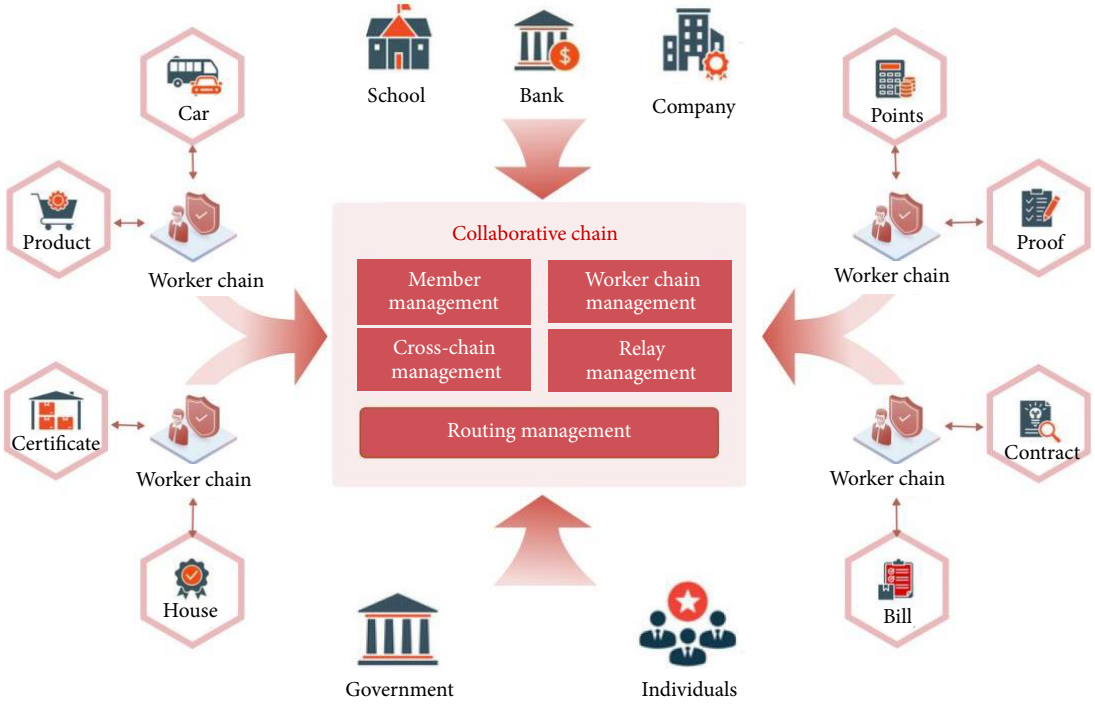

Fig. 2 Collaborative-worker multi-chain system.

consensus while building blocks and ledgers. The custody node provides key custody services. Finally, asset storage nodes only store asset files in ciphertext and store digests in ledgers.

Through this architecture of separating storage from computation and decoupling functions, we can fully leverage the performance of each node and improve the throughput of the blockchain as a whole. This architecture design can also better meet the needs of different business scenarios in the metaverse while ensuring mutual isolation between various businesses to improve security and reliability of the entire system.

(2) Cross-chain model design in the collaborative-worker multi-chain architecture

To address the difficulty of large-scale homogeneous/heterogeneous cross-chain collaboration caused by the differences in blockchain governance systems, architectures, data structures, security systems, service quality, and trustworthiness of operating environments used in different business scenarios in the digital world, DareChain has designed three basic cross-chain interaction types: cross-chain query, cross-chain invocation, and cross-chain transaction. Based on the "relay + gateway" protocol, we have constructed a large-scale homogeneous/heterogeneous cross-chain model.

Firstly, we define that different worker chains maintain different state data. In the multi-chain system, the i-th transaction record is Tx_i, and the subjects are represented as sub_a and sub_b. Different two worker chains are set as $\mathrm{WorkerChain}_1$ and $\mathrm{WorkerChain}_2$. The read set of Tx is $R(\mathrm{Tx})$, and the write set is $W(\mathrm{Tx})$. The three types of interaction we designed are defined as follows:

(a) **Cross-chain query** is a read-only operation. The cross-chain query transaction Tx initiated by $\mathrm{WorkerChain}_1$ to $\mathrm{WorkerChain}_2$ is defined as follows:

The state of Tx and $W(\mathrm{Tx})$ is maintained by $\mathrm{WorkerChain}_2$, not by $\mathrm{WorkerChain}_1$.

(b) **Cross-chain invocation** is a read-only operation, but it will be recorded on the calling party's worker chain. It is defined as follows:

$R(\mathrm{Tx})$ is jointly maintained by $\mathrm{WorkerChain}_1$ and $\mathrm{WorkerChain}_2$, and the state data of $W(\mathrm{Tx})$ are maintained by $\mathrm{WorkerChain}_2$.

(c) **Cross-chain transaction** requires reading and writing of relevant state data of the transaction. Therefore, it is defined as follows:

Both $R(\mathrm{Tx})$ and $W(\mathrm{Tx})$ are jointly maintained by $\mathrm{WorkerChain}_1$ and $\mathrm{WorkerChain}_2$.

In addition, we have designed functions such as heterogeneous chain admission registration, cross-chain gateway registration, cross-chain resource registration, and cross-chain business monitoring. At the same time, we provide various mechanisms such as two-phase cross-chain protocol and hash time locking to achieve subject identity authentication, semantic alignment, and result mutual recognition in the process of cross-chain interaction.

To better support flexible and deep adaptation of homogeneous and heterogeneous blockchains, we also provide a message and interface registration mechanism, and support custom cross-chain messages and interfaces to eliminate "data islands" between blockchains, and support full interconnection of the entire network. In this way, we have constructed a cross-chain interoperable network that supports one-to-one, one-to-many, and many-to-many scenarios. This network can eliminate the barriers between underlying blockchains of different business systems, and support data sharing and communication in all application scenarios of the metaverse.

3 Key Technological Innovations to Support Trusted DareChain

3.1 Account model supporting complex digital assets

The objects of the metaverse maintain the characteristic of uniqueness, which is reflected in DareChain, that is, all the objects that can participate in the transaction have their own accounts, and each account uniquely corresponds to the account address.

The DareChain account model combines the advantages of traditional account models and Unspent Transaction Outputs (UTXO) models. The current status of an account can be obtained at any time through the account state tree, and the relationship between accounts can be traced through transaction inputs and outputs. Multiple assets of the same subject use different accounts, making them relatively independent and effectively supporting concurrent processing under massive transactions. The security and verifiability of accounts are ensured through cryptographic capabilities. DareChain provides multiple key construction and encryption/decryption capabilities for each object's account, and key information can be selectively expanded or reduced based on actual needs of objects and business scenarios.

In DareChain, subjects, digital assets, smart contracts, and other objects are represented by the account model. After authentication, a unique subject account is generated on DareChain for each subject. When a contract is deployed, a unique contract account is generated, and when an asset is created, a unique asset account is generated. The operation of subjects on digital assets essentially involves interaction between subject accounts and digital asset accounts under corresponding contract accounts.

(1) Subject account model

The subject account model is used to describe the subject objects that participate in transactions on DareChain. Subject information includes status, roles, permissions, authentication information, etc., where the subject's status is recorded through a state model, permissions and roles are constrained by relevant contracts. Subjects can acquire digital assets through ownership confirmation, transfer digital assets through authorization, delegate other subjects to operate their own assets, and also operate other subjects' digital assets as a delegatee. Subjects follow contract constraints to operate digital assets. The basic information of the subject itself, its status, the digital assets associated with the subject, and their transactions are all stored on the DareChain. The specific design of the subject account model is as follows:

$$\begin{aligned}\mathrm{Account} = \langle &\mathrm{ID},\ \mathrm{State},\ \mathrm{Authority},\\ &\mathrm{list}_{\mathrm{asset}}\{\mathrm{ID}_{\mathrm{Asset}_1}, \mathrm{ID}_{\mathrm{Asset}_2}, \ldots, \mathrm{ID}_{\mathrm{Asset}_n}\}\rangle\end{aligned} \tag{1}$$

(2) Digital asset model (object account model)

The digital asset model is used to describe the objects that participate in transactions on DareChain, including any valuable data elements, digital products, physical products, or electronic information that circulate between subjects in the digital world.

The digital asset model includes unique identifiers, asset types, status, content, ownership, permissions, and association relationships. The digital asset summary ID is used to identify the characteristics of the asset content. Structured text or multimedia data can be used to compose the content data of a digital asset. The asset content is stored in whole or in part in encrypted form on DareChain to ensure the security of user digital assets. The holder list of digital asset ownership, authorization list, and

operation list are used to describe the ownership relationship between the digital asset and one or more subjects. They are distinguished by a unique asset ID and bound to a subject account. The relationship between subject accounts and asset accounts is one-to-many.

As shown in the following equation, the list of operation is a list of subject accounts with various operation permissions for assets. This article describes the asset account through Eq. (2):

$$\text{Asset} = \langle \text{ID},\ \text{Type},\ \text{State},\ \text{data}\{\},\ \text{list}_{\text{holder}}\{\},\ \text{list}_{\text{authorize}}\{\},\ \text{list}_{\text{op}}\{\},\ldots\rangle \tag{2}$$

3.2 Layered model of smart contracts supporting trusted interactions

In response to the problem of incomplete digital asset information, inconsistent data, and uncontrollable transaction processes caused by the "two-faced" phenomenon of current smart contracts and blockchain in the context of widespread metaverse applications, a layered model of smart contracts as illustrated in Fig. 3 has been established starting from the fundamental issue of functional independence. The contract code is separated into asset contracts and business contracts, while contract storage is directly integrated into the blockchain layer. The asset contract implements complete asset state control at the bottom layer of the blockchain, while the business contract is responsible for executing business logic. By separating the business logic and state control of assets, it ensures semantic consistency between the blockchain layer and the contract layer for assets and ensures data integrity and correctness in the blockchain, ensuring controllability of asset circulation.

Firstly, we define a basic smart contract model where all smart contracts are a string of code on the blockchain deployed by subject accounts as contract accounts that can be called by subject accounts. They only contain functional functions without any asset information and are bound to a certain type of asset rather than a specific asset account. We abstract it as a special type of account that automatically executes related code, represented by Eq. (3). Asset contracts and business contracts are further refinements to smart contracts:

$$\text{Contract} = \langle \text{ID}, \text{State}, \text{Asset\_Type}, \text{code}\{\},\ \text{functions}\{\}, \text{list}_{\text{op}}\{\},\ldots\rangle \tag{3}$$

Asset contracts and digital assets have a template-instance relationship, where asset contracts are templates for assets, and assets are instances of asset contracts. The asset contract model defines and constrains the attributes and behaviors that can be exhibited by the associated digital assets, directly controlling changes in the state of digital assets to ensure consistency in their state on the blockchain and prevent double-spending problems. Asset contracts are validated and transformed according to pre-set rules and expected constraints, ensuring that digital assets mapped from the digital world to DareChain are real, trusted, and controllable. They also ensure that assets exhibit attributes and behaviors that meet user expectations. Therefore, asset contracts include properties such as contract ID, defined asset type, asset attributes, and operations that can be performed on assets. They are specifically defined as follows:

$$\text{AC} = \langle \text{ID}, \text{Asset\_Type}, \text{code}\{\}, \text{Attributes}\{\}, \text{list}_{\text{op}}\{\},\ldots\rangle \tag{4}$$

Business contracts are used to describe and execute business processes mapped from the real world to DareChain. Business processes in the real world are very complex, and business contracts control the state transitions of subjects or assets in DareChain according to prescribed processes, enabling collaborative work between subjects. They can also monitor object states in the blockchain and trigger business process operations, avoiding inconsistencies caused by state changes. Therefore, business contracts include properties such as contract ID, involved business type, list of asset contracts that can be called, business logic code, subject that can call this contract, and operations that can be performed. They are specifically defined as follows:

$$\text{BC} = \langle \text{ID}, \text{Business\_Type}, \text{AC}\{\}, \text{code}\{\}, \text{Subject}\{\},\ \text{Object}\{\}, \text{list}_{\text{op}}\{\},\ldots\rangle \tag{5}$$

Business contracts and asset contracts work together. The operation of an asset contract can trigger the execution of a business contract, and a business contract can also actively call an asset contract to advance the process. The two types of contracts can be flexibly combined, and the execution process strictly follows the contract to ensure process security and reliable results.

3.3 Hyperlinear ledger consensus algorithm for massive and complex transactions

Based on the previous design of the subject-object account model and smart contract model, we propose a transaction model consisting of three elements: subject account, asset account, and

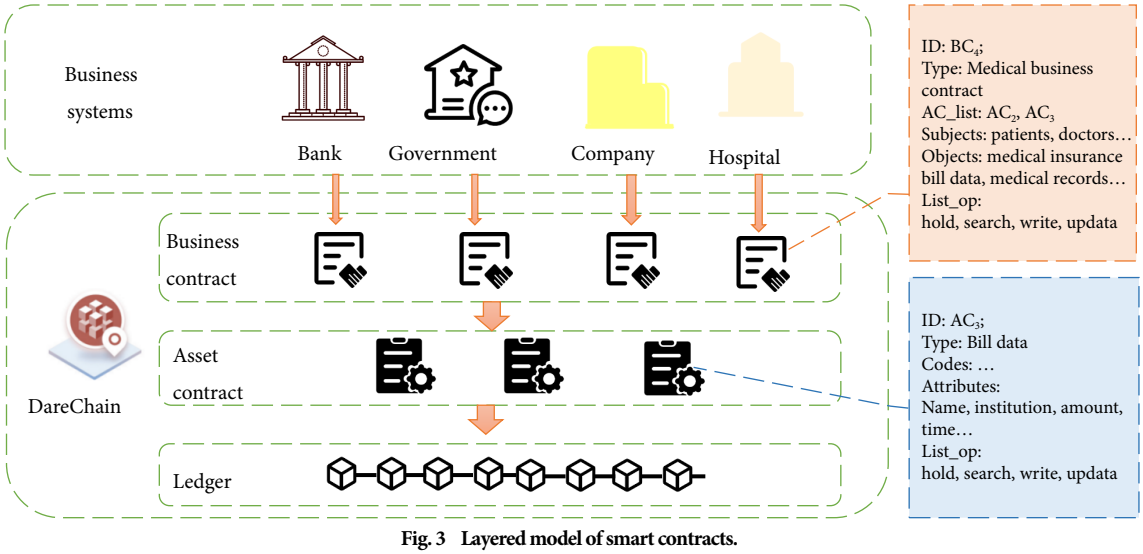

Fig. 3 Layered model of smart contracts.

smart contract account. It is worth noting that the relationship between asset accounts and contract accounts is many-to-many. That is, the same type of asset that completes the same asset operation calls the same contract address. However, since no asset information is stored in the contract and only logical code exists, it belongs to a read operation on the contract and does not cause conflicts.

Furthermore, while separating asset accounts from contract accounts, we redefine the format of transactions as shown in Eq. (6), where a transaction includes the subject account Address_A that sends the transaction, subject account Address_B that receives the transaction, object account Address_C involved in the transaction, other relevant information, and timestamp when the transaction was sent:

$$\text{Tx} = \langle \text{Address}_A, \text{Address}_B, \text{Address}_C, \text{additional}_{\text{field}}, \text{Timestamp} \rangle \tag{6}$$

Based on the above transaction model, to solve the performance bottleneck of low transaction throughput and high transaction latency in blockchain, DareChain achieved a parallel consensus mechanism based on hyperlinear ledger through parallel decoupling at different granularities such as transactions, blocks, and consensus execution stages. This breakthrough overcomes the limitations of traditional serial consensus models, and achieves high transaction throughput and low latency, ensuring that blockchain serves as a trusted collaborative underlying network for the metaverse and can support massive transaction demands for all metaverse application scenarios.

The basic workflow of the hyperlinear ledger is as follows: In hyperlinear ledger, blocks are mainly divided into two types: main blocks (BBLOCK) and transaction blocks (TXBLOCK), as shown in Fig. 4b. Each height has a unique main block and multiple transaction blocks. The main block contains a pointer to the transaction block of this height. The main blocks of different heights are connected by hash digests to prevent tampering.

Hyperlinear ledger consensus is mainly divided into two stages: synchronized consensus stage and asynchronous consensus stage. In the synchronized consensus stage, blockchain nodes are grouped, and the master node packages the transaction block and main block of this height. As shown in Fig. 4b, the transaction block contains a list of transactions (txList) for this height, which are organized into a Merkle tree with the root denoted as tR. The main block contains the Root of an Announcement Tree (ATR), which is also a Merkle tree that includes all transaction blocks that have only passed the first stage of consensus but not yet passed the second stage. The tR of these transaction blocks serves as leaf nodes in the ATR. For a new transaction block at this height, its tR is added as the last two nodes in the ATR, as shown in Fig. 4c. The reconstructed new ATR is then recorded in the main block at this height and verified together with new blocks during the synchronized consensus stage. Therefore, for transactions that have only passed through the synchronized consensus stage, their data can be verified on the main block through Merkle paths, which are public and tamper-proof. Subsequent transactions can be built on these data.

In the synchronized consensus stage, only the legality of transactions and blocks is verified. After this stage ends, asynchronous consensus for this height begins while synchronous consensus for next height starts simultaneously. In asynchronous consensus stage, transaction blocks are distributed to different groups for parallel verification. This verification includes verifying the correctness of the input data, output data, and computational content of transactions. Transactions with errors in the verification process are marked separately. Finally, the entire transaction block is verified by group consensus and then submitted to the master node at the latest height. For this latest height, synchronous consensus is starting. The master node puts the asynchronous verification information into STS of a new main block. Then based on the content in STS, tR of transaction blocks that have passed through asynchronous consensus stage are removed from ATR and new data are updated to Asset State Tree (AST), as shown in Fig. 4d. The root of the new AST is packaged into the main block at this height, and ATR will be further updated and packaged based on transaction blocks at this height. At this point, a complete round of consensus ends.

3.4 Trusted collaborative model supporting privacy protection

There are many scenarios in the metaverse that require privacy protection, such as medical health, financial services, and other fields, especially for non-monetary digital assets such as copyrights and bills that are closely related to the physical world. However, current blockchain technology can only provide contract expression and execution for these digital assets in the metaverse, but cannot meet the needs of transaction records and transaction content that require traceability and auditing while ensuring privacy. Therefore, DareChain has built a new transaction model that balances transparency and privacy by designing transaction content hiding from two dimensions: "transaction obfuscation storage-transaction confidential execution".

In this way, while supporting contract expression of digital

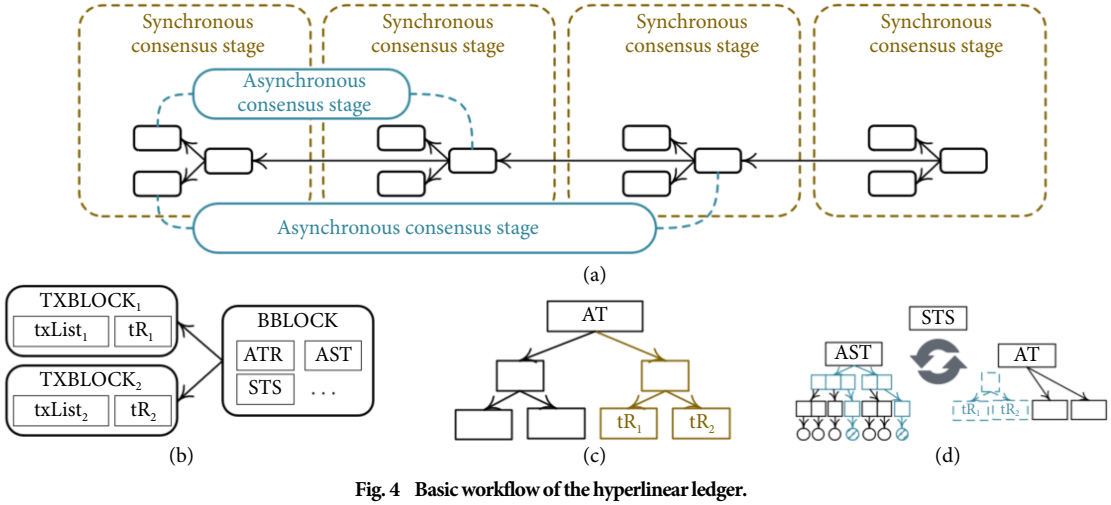

Fig. 4 Basic workflow of the hyperlinear ledger.

assets and executing transactions of digital assets, transactions are split into different nodes for storage based on honest probability, and the execution and verification processes of transactions are split into different nodes to ensure that alliance members cannot analyze user privacy information from the ledger or state tree.

(1) Transaction storage with key information obfuscation

There are two difficulties in protecting the privacy of digital assets during ledger storage and access: on one hand, transaction splitting must be fair and not monopolized by a single node or group of nodes, and transactions must be guaranteed to be restorable; on the other hand, in the process of transaction restoration, it must be ensured that transaction information is not leaked.

Firstly, a transaction obfuscation splitting mechanism is constructed to reduce data transmission volume while ensuring security. As shown in Fig. 5, each consensus node splits the key information of transactions into several different attributes based on multi-party computation, and ensures their integrity and verifiability in the form of a transaction Merkle tree. According to the number of nodes, transaction size, node honesty probability, etc., Reed-Solomon mechanism is used to allocate k transactions $\{tx_1, tx_2, \ldots, tx_k\}$ in the ledger to m ledger storage nodes $\{n_1, n_2, \ldots, n_m\}$, and ensure at least p redundant copies.

Then, a transaction decentralization encryption storage mechanism is constructed. Multiple nodes jointly generate keys to avoid key theft causing privacy leaks. This achieves decentralized encryption Encry(Att) for multiple attributes.

Finally, a transaction restoration mechanism is constructed to reduce computational complexity while ensuring security. The Direct Memory Access and Attribute-Based Encryption (DMA-ABE) scheme is used for fine-grained query permission verification of transaction fragments. In the tree-based access control structure, any possible user attribute corresponds to a leaf node. Leaf nodes merge upwards into non-leaf nodes until they reach the root. Each node including the root hides its own key. Leaf nodes contain one attribute judgment while non-leaf nodes contain threshold judgments. The root hides the key to unlock assets. When a user satisfies an attribute judgment at a leaf node, they obtain the key hidden by that leaf node. Non-leaf nodes collect the key values of all their child nodes and use an m-of-n secret sharing scheme to restore the key hidden by the non-leaf node. This process continues upwards until the key hidden by the root node is obtained.

(2) Fractionalized transaction state machine confidential verification and execution

During transaction execution, the attributes of digital assets in the state tree need to be read and the execution results need to be stored in the state tree. Transaction information is stored in a ledger based on key information obfuscation to ensure its privacy. The privacy of the transaction execution process is ensured by a fractionalized state machine confidential verification and execution mechanism, which mainly solves two problems: one is the privacy protection of the state tree, and the other is confidential execution and consensus for heterogeneous nodes.

Firstly, a verifiable splitting method for key information in the state tree is constructed to solve the problem of possible privacy leaks due to corruption of alliance members. The complete state tree needs to have information such as state tree flag address, state tree verification value, and state tree content at the same time. When executing transactions, it is necessary to restore the complete initial state. This process requires that executing nodes be in a Trusted Execution Environment (TEE), collect state tree content through state tree flag addresses, and restore it through state tree verification values. The restored status is guaranteed by TEE for confidentiality, and no member can restore a complete state tree outside TEE.

Secondly, a confidential execution method for heterogeneous nodes is studied to solve the security leaks and attacks caused by a single TEE execution environment. In an open alliance chain, device heterogeneity is obvious, and it is unrealistic to require all members to have the same hardware environment (such as TEE) and the same service capabilities. This method first divides some alliance members into transaction execution nodes, transaction verification nodes, and clients. The execution node needs to send the transaction execution result in the form of a commitment to the verification node for verification, ensuring the confidentiality of contract transactions. The client performs integrity verification with the support of the verification node, as shown in Fig. 6.

The execution node and verification node construct a confidential transaction execution mechanism based on TEE. This mechanism mainly consists of four parts. The first part is key management, which is responsible for managing asymmetric trusted transmission keys (pk, sk), transmission keys ts, and storage keys ss. The second part is encrypted transmission, which encrypts transactions using transmission keys ts. The encrypted ciphertext is published as a public transaction on the blockchain, and ts is distributed by TEE after being encrypted one by one using other members' public keys pk. The third part is confidential execution, which embeds smart contracts in TEE. The fourth part is encrypted storage. Before the transaction result is taken out of TEE, it will be symmetrically encrypted using storage key ss by TEE. The same applies when data are taken into TEE. Between the verification node and client, cross-privacy transaction cross-validation mechanism is used for data cross-validation.

4 Application Based on DareChain

As shown in Fig. 7, currently, based on DareChain, a series of urban chains, industry chains, and regional chains have been implemented to support the integration of large industries, city clusters, and key regions. This has helped to form a new generation of digital networks such as the blockchain public data internet and the crowd intelligent network. It has also created a new type of digital ecosystem with numerous entities, diverse

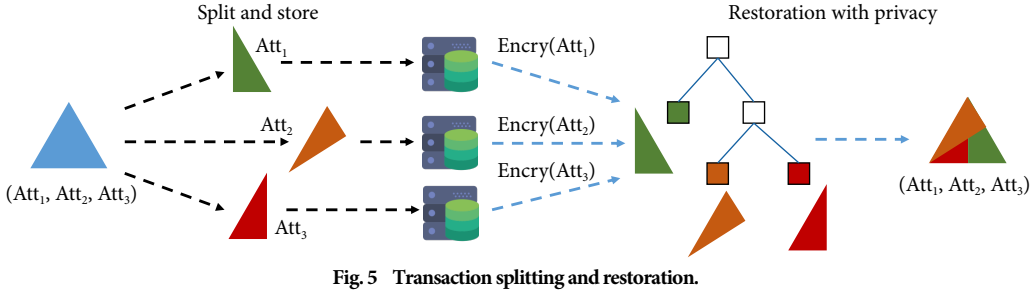

Fig. 5 Transaction splitting and restoration.

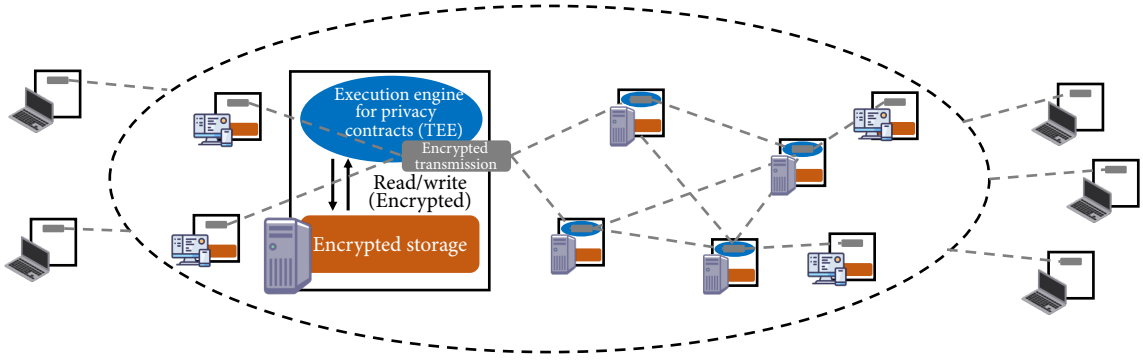

Fig. 6 Cross-confidential transaction execution.

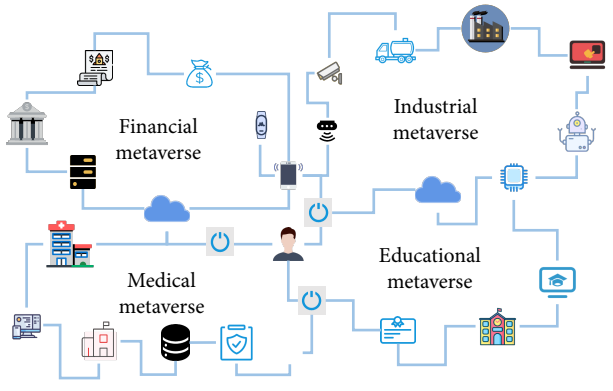

Fig. 7 Metaverse including different fields.

objects, huge interactions, and rich scenarios. Innovative applications have been carried out in multiple scenarios such as public data open sharing, data element transactions, smart governance, inclusive finance, medical insurance and health care, social insurance, supply chain finance, joint credit reporting, public disclosure and notarization services, data security, and more using the new blockchain-based trusted collaborative network infrastructure. The social and economic benefits are significant.

Currently there are more than 20 city-, industry-, and region-based blockchain platforms that have been established including "Quancheng Chain", "Jining Chain", "Gangcheng Chain", "Shandong Province Medical Insurance Chain", "National Human Resources and Social Security Chain", "Shandong Provincial Economic Circle (Yellow River Basin) 10-city Integrated Blockchain", "Digital Yellow River Chain", etc., which provide trusted infrastructure for data element circulation and information openness in various fields of social economy of metaverse. In the field of inclusive finance, public data are being opened up to financial institutions in an orderly manner to help solve financing difficulties for citizens and small- and medium-sized enterprises. In Jinan, 20 commercial banks have launched 38 credit products online; In the field of inclusive insurance, Shandong Province Medical Insurance Chain supports "preferential medical insurance for the people" in various cities in Shandong Province by providing medical insurance data legally compliantly to commercial insurance companies for underwriting claims processing. It achieves one-stop settlement automation for claims processing with a maximum business volume of over 50 thousand transactions per day per city; In the field of government services, based on the blockchain infrastructure platform, entities can open up "My Digital Twin" on the metaverse and blockchain to establish a full life-cycle data archive; In the digital economy field, a supply chain finance system platform has been established to provide financing services for small- and medium-sized enterprises on the supply chain through accounts receivable debt transfer, asset securitization issuance, and other forms.

Taking the medical metaverse as an example, trusted collaboration is currently a major concern for individuals, medical institutions, and government regulatory agencies. Taking the medical metaverse as an example, trusted collaboration is currently a major concern for individuals, medical institutions, and government regulatory agencies. A user's (patient's) medical data may be stored on his/her personal cell phone, bracelet, blood pressure meter, and other sensors, or autonomously uploaded to the cloud, while the government stores data such as the user's health insurance records, hospitals store the user's electronic case data, and insurance companies store the user's health insurance enrollment information, which are in reality segregated, and when interacting with the data, it requires the user to go back and forth many times to different organizations. However, in the metaverse, the data can be shared and circulated credibly through the underlying trusted collaboration network, and the user's medical data can be circulated in different institutions and devices under the user's authorization, while the user can also control the openness and closure of the data.

To be more specific, firstly, patients expect to be able to access their own and their family's medical data anytime and anywhere, without having to carry around various test results when transferring hospitals or repeating tests. In addition, medical institutions at different levels and in different regions hope to interact each other in order to provide scientific diagnosis and treatment services. Medical research institutions also hope to obtain authoritative data as research materials or teaching resources to support medical technology research and the cultivation of high-level medical personnel.

However, due to the relatively independent information systems of medical institutions, resources are distributed heterogeneously, making interconnection difficult and resulting in information silos. Moreover, due to the wide coverage of data sources, it is difficult to achieve comprehensive collection of patient medical records, resulting in low completeness and value. At the same time, problems such as prescription fraud and privacy security make it difficult for patients' medical records and prescriptions to be shared. In the process of health and medical data circulation, how to determine the rights of all parties involved, how to inform patients, how to make medical institutions controllable, how regulatory agencies can conduct trusted supervision, and how privacy protection can be ensured during circulation are all issues that currently lack relevant technical means.

In order to ensure that patients are informed and voluntary about the use of their data by legitimate users in compliance with

regulations, patients, medical institutions, and government regulatory agencies are the subjects in the medical metaverse who will register on a trusted collaborative network. So as shown in Fig. 8, medical data such as patient insurance data, pharmaceutical institution data, patient insurance participation data, etc., which serve as digital assets for patients will be opened on the accounts with corresponding subjects associated with them so that trusted transmission between subjects can be achieved. Medical institutions can share and view data with each other after being authorized by patients, which can help patients avoid repeating medical examinations. The health and medical trusted collaborative network encrypts storage, and only authorized medical institutions can view it, protecting patient privacy. This also creates the basic conditions for remote diagnosis and treatment, transforming the current uneven distribution of medical resources and achieving the sinking of medical resources.

5 Conclusion and Future Work

This paper proposes a blockchain-based trusted collaborative network infrastructure for the future digital economy and society—DareChain, aimed at solving problems such as the complexity of the subject-object model in the metaverse, lack of trust in collaboration, easy leakage of security and privacy, and insufficient performance of blockchain. DareChain includes innovative designs such as a collaborative-worker multi-chain system, a trusted subject-object account model, a layered smart contract architecture, a hyperlinear ledger consensus algorithm, and a transaction model that supports privacy protection. It has been implemented in multiple metaverse application scenarios such as government affairs, healthcare, finance, etc., solving the above problems when blockchain is used as the underlying trusted collaborative network in the metaverse.

In the future, our trusted collaborative network will continue to operate efficiently to support comprehensive and trusted applications in the metaverse ecosystem. We will take typical metaverse application scenarios in key economic and social fields such as agriculture, industry, services, military affairs, and social governance as entry points to implement the trusted support role of our collaborative network infrastructure in these metaverse pilot applications. Through DareChain's trusted collaborative network, we ensure that all subjects and objects related to economic and social activities in the physical world are fully mapped into the digital world to form a complete digital twin of the physical world. Moreover, we guarantee that there are numerous digital companions living in the digital world to provide various professional services for economic and social activities in both physical and digital worlds. By connecting every subject and object, providing trusted collaborations and systematic promotion of economic-social metaverse applications, we will push forward development stages for metaverses towards higher levels.

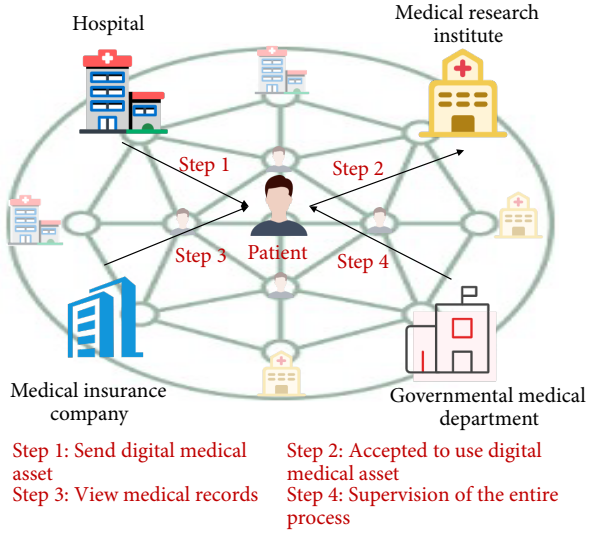

Fig. 8 Data sharing in medical metaverse by DareChain.

Dates

Received: 17 August 2023; Revised: 21 September 2023; Accepted: 28 September 2023

References

[1] Association for Crowd Science and Engineering (ACE), Scientific research of ACE, http://www.crowdscience.org/en/research, 2023.

[2] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, MetaChain: A novel blockchain-based framework for metaverse applications, in *Proc. 2022 IEEE 95th Vehicular Technology Conference* (*VTC2022-Spring*), Helsinki, Finland, 2022, pp. 1–5.

[3] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, Towards blockchain-based auditable storage and sharing of IoT data, in *Proc. 2017 on Cloud Computing Security Workshop*, Dallas, Texas, USA, 2017, pp. 45–50.

[4] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, Blockchain based data integrity service framework for IoT data, in *Proc. 2017 IEEE Int. Conf. Web Services* (*ICWS*), Honolulu, HI, USA, 2017, pp. 468–475.

[5] Z. Su, Y. Wang, Q. Xu, and N. Zhang, LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue, *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 19–32, 2022.

[6] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, BPDS: A blockchain based privacy-preserving data sharing for electronic medical records, in *Proc. 2018 IEEE Global Commun. Conf.* (*GLOBECOM*), Abu Dhabi, United Arab Emirates, 2018, pp. 1–6.

[7] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities, *Comput. Secur.*, vol. 88, p. 101653, 2020.

[8] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, 2019.

[9] Q. Yang, M. Zhang, Y. Zhou, T. Wang, Z. Xia, and B. Yang, A non-interactive attribute-based access control scheme by blockchain for IoT, *Electronics*, vol. 10, no. 15, p. 1855, 2021.

[10] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, MediBchain: A blockchain based privacy preserving platform for healthcare data, in *Proc. SpaCCS 2017*: *Security*, *Privacy*, *and Anonymity in Computation*, *Communication*, *and Storage*, Guangzhou, China, 2017, pp 534–543.

[11] H. Xu, Z. Li, Z. Li, X. Zhang, Y. Sun, and L. Zhang, Metaverse native communication: A blockchain and spectrum prospective, in *Proc. 2022 IEEE Int. Conf. Commun. Workshops* (*ICC Workshops*), Seoul, Republic of Korea, 2022, pp. 7–12.

[12] M. Ersoy and R. Gürfidan, Blockchain-based asset storage and service mechanism to metaverse universe: Metarepo, *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 1, p. e4658, 2023.

[13] H. G. Do and W. K. Ng, Blockchain-based system for secure data storage with private keyword search, in *Proc. 2017 IEEE World Congress on Services*, Honolulu, HI, USA, 2017, pp. 90–93.

[14] D. Yue, R. Li, Y. Zhang, W. Tian, and C. Peng, Blockchain based data integrity verification in P2P cloud storage, in *Proc. 2018 IEEE 24th Int. Conf. Parallel and Distributed Systems* (*ICPADS*), Singapore, 2018, pp. 561–568.

[15] J. Li, J. Wu, and L. Chen, Block-secure: Blockchain based scheme for secure P2P cloud storage, *Inf. Sci.*, vol. 465, pp. 219–231, 2018.

[16] J. Li, J. Wu, L. Chen, and J. Li, Deduplication with blockchain for secure cloud storage, in *Proc. Big Data: 6th CCF Conf., Big Data 2018*, Xi'an, China, 2018, pp. 558–570.

[17] Z. Lin, X. Peng, Z. Li, F. Liang, and A. Li, Towards metaverse manufacturing: A blockchain-based trusted collaborative governance system, in *Proc. ICBCT'22: The 2022 4th Int. Conf. Blockchain Technology*, Shanghai, China, 2022, pp. 171–177.

[18] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, A survey on metaverse: Fundamentals, security, and privacy, *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 319–352, 2023.

[19] F. Y. Wang, R. Qin, X. Wang, and B. Hu, MetaSocieties in metaverse: MetaEconomics and MetaManagement for MetaEnterprises and MetaCities, *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 1, pp. 2–7, 2022.

[20] T. Huynh-The, T. R. Gadekallu, W. Z. Wang, G. Yenduri, P. Ranaweera, Q. V. Pham, D. B. da Costa, and M. Liyanage, Blockchain for the metaverse: A review, *Future Generation Computer Systems*, vol. 143, pp. 401–419, 2023.

[21] I. Sukhodolskiy and S. Zapechnikov, A blockchain-based access control system for cloud storage, in *Proc. 2018 IEEE Conf. Russian Young Researchers in Electrical and Electronic Engineering* (*EIConRus*), Moscow and St. Petersburg, Russia, 2018, pp. 1575–1578.

[22] G. Raja, Y. Manaswini, G. D. Vivekanandan, H. Sampath, K. Dev, and A. K. Bashir, AI-powered blockchain—A decentralized secure multiparty computation protocol for IoV, in *Proc. IEEE INFOCOM 2020 - IEEE Conf. Computer Commun. Workshops* (*INFOCOM WKSHPS*), Toronto, Canada, 2020, pp. 865–870.

[23] J. Zhang, Interaction design research based on large data rule mining and blockchain communication technology, *Soft Comput. A Fusion Found. Methodol. Appl.*, vol. 24, no. 21, pp. 16593–16604, 2020.

[24] C. Ju, Z. Shen, F. Bao, Z. Wen, X. Ran, C. Yu, and C. Xu, Blockchain traceability system in complex application scenarios: Image-based interactive traceability structure, *Systems*, vol. 10, no. 3, p. 78, 2022.