Blockchain-Based Data Sharing System with Decentralized Identifier for the Industrial Internet of Things

***Abstract*—The current landscape of data sharing predominantly relies on centralized platforms, encountering several inherent challenges: (1) Inadequate identity management mechanisms for facilitating large-scale data sharing; (2) Absence of a standardized data discovery and description model; (3) Insufficiency in dynamic sharing mechanisms to support extensive chains of data exchange. Leveraging the characteristics of traceability, tamper resistance, and distributed trust, blockchain technology emerges as a promising solution for these issues. This paper introduces a Blockchain-Based Data Sharing System fortified by Decentralized Identifiers tailored for the Industrial Internet of Things (IIoT). The system incorporates a self-management mechanism for subject identification, standardizes data description on the chain while enabling off-chain data exchange, and employs attribute encryption for data access control. Additionally, a practical scenario involving car repair factoring business is presented, demonstrating the application of this system within the Xinghuo Blockchain Infrastructure & Facility.**

Keywords—blockchain; digital identifier; data sharing; industry chain collaboration

I. INTRODUCTION

The advent of the Industrial Internet, stemming from advancements in information and communication technology, has revolutionized manufacturing and service systems, spanning the entire value and industry chains. This transformation offers a pathway towards the digital, interconnected, and intelligent evolution of industries. Recently, the Industrial Internet of Things (IIoT) has gained traction among influential industrial nations aiming for intelligent manufacturing supremacy in the global competition. Initiatives like the United States' Advanced Manufacturing Partnership Program, Germany's Industry 4.0, and China's Made in China 2025 have underscored the appeal of the IIoT in achieving this goal.

Characterized by a closed-loop system rooted in "data-driven" intelligent optimization, the Industrial Internet orchestrates the collection, transmission, processing, analysis, decision-making, and feedback control of real-time industrial data. By merging this data with industrial expertise, a novel optimization paradigm emerges, perpetually enhancing operational efficiency in the physical realm and fostering increased value creation. Nonetheless, obstacles and challenges impede the further progression of the manufacturing industry. Despite the intrinsic "data-driven" nature of the Industrial Internet, businesses exhibit hesitancy in sharing data, particularly sensitive information, due to the absence of a secure mechanism for sharing among multiple agents. Although numerous centralized platforms offer data sharing services, the prevalence of "information islands" among these platforms persists, as illustrated in Fig1.

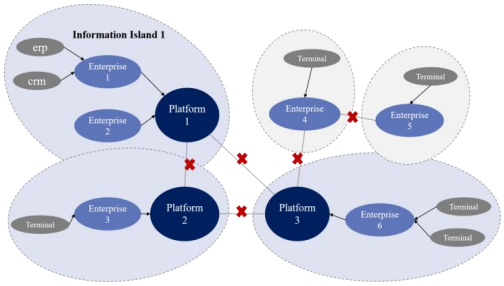

Fig. 1. The "information island" phenomenon

At present, with the emergence of blockchain technology and its widespread application in the field of data sharing, the idea of combining blockchain technology with the industrial chain collaboration has received considerable attention. By using the functions of the anti-tampering and decentralized consensus mechanism in the blockchain, we can establish a stable trust system between participants and solve the challenges of data sharing. There have been some studies on the application of blockchain technology in the data sharing. How to achieve secure and efficient data trades has been gaining increasing attention from academia and industry. For example, industrial circles focus on data discovery mechanisms based on the transparent characteristic of blockchain. Academic circles pay attention to fair data trading mechanisms in multi-part based on the blockchain. At the same time, the introduction of blockchain innovation into the industrial internet will encounter many problems. We summarized three main issues as follows.

- **Lack of identity management mechanisms:** Involvement of multiple roles within the industrial chain complicates identity cooperation, hindering data control and risking data leakage through third-party identity management systems.
- **Absence of a unified data discovery and description model:** Wide-ranging data sharing complicates data retrieval and understanding due to the absence of a standardized query entry and data description model.
- **Deficiency in dynamic sharing mechanisms for long chains:** Traditional attribute encryption solves the one-to-many access control problem but struggles in scenarios with undefined data requesters, especially within complex industrial production chains.

To address these challenges, this article proposes a Blockchain-based Data Sharing System with a Decentralized Identifier for the Industrial Internet of Things. Our contributions include a self-management mechanism for subject identification, a unified data description mechanism, and an off-chain data exchange with robust data access control based on attribute re-encryption.

The remainder of this article is organized as follows: Section 2 reviews the background and related work. Section 3 presents the design principles and implementation of the proposed Data Sharing System with a Decentralized Identifier for the Industrial Internet of Things. Section 4 details the system's workflow. Subsequently, Section 5 covers performance evaluation and discussions. Finally, Section 6 concludes the article and outlines future directions.

II. Background and related word

In this section, we provide an overview of existing industrial data sharing methods within current blockchain systems. We analyze works related to decentralized identifiers and the integration of blockchain within the Industrial Internet of Things (IIoT).

A. Related Work of Data Sharing Based on Blockchain

Recently, with the emergence of blockchain technology, a variety of blockchain-enabled data sharing systems are developed. Due to the structural features of blockchain, along with the advantages of non-tampering, non-repudiation, and traceability, the blockchain-enabled data sharing are mainly focused on the following sectors:

- **Framework Design for Blockchain-Supported Data Sharing:** Zhang Yachuan[1] propose a implementation of blockchian-based data sharing model for internet of things. A blockchain-based user identity security corroboration method and data paid sharing scheme were presented by Liu Yangquan [2] et al. to realize the protection of users' personal information, data rights and interests. A digital asset corroboration transaction model based on blockchain technology was put up by Ting Zhang et al. [3]. The model splits the entire life cycle of a digital asset into four steps: registration, authentication, transaction, and payment. This approach addresses the issue of challenging digital asset copyright corroboration, authorization, and transaction. To facilitate the development of blockchain data structures and to enable complete process transparency and auditability of data sharing processes based on smart contracts, Wenbilong et al. [4] presented a data resource description model. In order to achieve the unified expression of data resources on the chain, Xie Renqiang et al. [5] proposed a blockchain-based digital resource authorization and transaction scheme, introduced the data access and storage model of "metadata + cloud storage," and designed a data on-chain metadata information table based on the Dublin core element set PREMIS preservation metadata idea. Meng Hongwei [6] et al. proposed a blockchain-based data sharing and exchange method, introducing digital signature and data usage process on-chain deposition mechanism to solve the problems of unknown data ownership, poor data quality, data liquidity checking and unknown data supervision responsibility.
- **Point Technology Design for Blockchain-Based Data Sharing:** In order to address the issue of the unreliability of conventional corroboration techniques, Wang Hailong [7] et al. proposed a big data corroboration scheme based on blockchain and digital watermarking technology. This scheme introduces an audit center and a watermarking center to corroborate the right at the source of data. A blockchain-based system for data asset corroboration was proposed by Cai Chang [8] et al., which explains who owns the property rights to the data through data pass-through. Richardo [9] et al. proposed a blockchain-based data accountability and traceability mechanism, which uses blockchain to record the data usage flow process and achieve traceability and auditability of data transaction records. Zhu Ziqiang [10] et al. proposed an anonymous and traceable blockchain data transaction scheme to achieve anonymity of user transactions and traceability of transaction records by group signing data asset transactions and uploading the transaction records to the chain. Liang Xiubo[11] review the data security management and privacy protection of blockchain. Li Dongxing[12] propose an authentication method for the network entities based on blockchain.

While previous research has made significant strides in various facets of blockchain-enabled data sharing, most efforts focus on specific aspects, lacking comprehensive solutions capable of supporting large-scale data sharing in the context of the Industrial Internet of Things. This paper aims to present a comprehensive, scalable, and secure data-sharing scheme to address the identified challenges.

B. Decentralized Identity

The concept of "digital identity" refers to the representation of network entities in a digital format, which allows for the association of pertinent data with entity objects as well as system verification and authorization. The overall development of digital identity can be divided into three phases: centralized identity, federalized identity and decentralized identity. Data leakage and identity dependence on third-party platforms are risks associated with the first two identity management strategies.

Decentralized identifier (DID) is a self-sovereign identity management scheme developed by the W3C community. DID is created using blockchain technology and the DID protocol, which primarily consists of the two components DID and verifiable credential (VC). The DID, which is connected to the user attribute document connected to the user identity, is essentially a global URL. Users can choose which attributes to reveal when authenticating their identities. The term "VC" refers to a claim regarding identity data that a user has checked out. The verifier can verify the user's identity through the claim. In the DID system, users have absolute control over their own identity, which avoids the risk of identity abuse caused by third-party storage.

The trusted relationship is the network of relationships in the circulation process of the certificate, which is composed of the issuer, the holder and the verifier. The issuer is the source of the credential, which gives the credential its real meaning. The credential holder is the owner of the credential and can have multiple credentials to prove his identity. The verifier is the object which verifies the certificate.

C. *Xinghuo Blockchain Infrastructure & Facility*

Xinghuo Blockchain Infrastructure & Facility (Xinghuo BIF) is an important example of blockchain infrastructure. Xinghuo BIF is a permissioned public blockchain, meaning any company can access blockchain services based on Xinghuo BIF. Authorized parties can build and operate the Xinghuo BIF nodes. Through double-layer architecture design and sharding technology, Xinghuo BIF strikes an effective balance between the performance and large-scale scenarios of blockchain, thus improving the effectiveness of blockchain applications.

The main chain of Xinghuo BIF is composed of supernodes. It provides public services for backbone nodes and is responsible for the management of chain group nodes, public data scheduling, and digital assets anchoring. Super nodes are responsible for the stable operation of the main chain, perform main chain consensus, and have various functions such as public data sharing management, cross-chain gateways, qualification review, chain group management, and so on.

The sub-chain of Xinghuo BIF consists of backbone nodes, which independently design and operate business according to different business scenarios. The backbone nodes are responsible for the connection between the sub-chain and the main chain. It has functions such as anchoring the main chain, supervising the sub-chain, and deploying smart contracts. The sub-chain is connected with the mainchain through backbone nodes to perform cross-chain interactions.

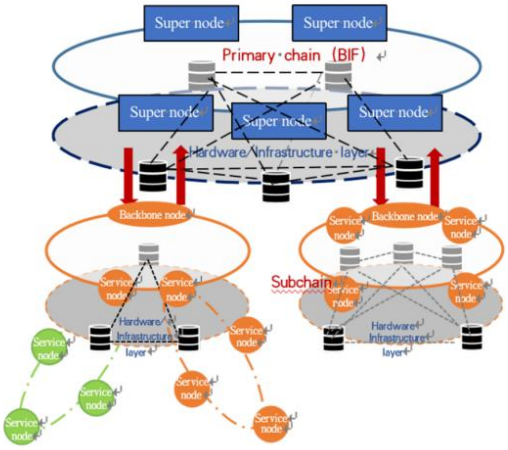

Fig. 2. The architecture of Xinghuo Blockchain Infrastructure & Facility

Xinghuo BIF adopts an open construction model to provide Decentralized Identifiers DID basic service, facilitating interconnectivity among different blockchains, regions and sectors, and building a smart and trusted Internet of Value in the era of the digital economy. The primary designing principle of Xinghuo BIF is to fully support the latest DID standards (BID), stress test the coexistence of multiple chains, transfer from permissioned public blockchain to public chains.

In the subsequent sections, we delve deeper into the proposed comprehensive data-sharing scheme, leveraging decentralized identifiers and blockchain technology to address challenges prevalent in the Industrial Internet of Things landscape.

III. System Design and Implementation

In this section, the design principle of the system is present first, followed by the implementation of Data Sharing System with Decentralized Identifier.

A. *Design Principles*

The construction of the Data Sharing System adheres to specific guiding principles, ensuring its efficacy:

- **Compatibility**: The system have the capability of interconnecting with internal/corporate and/or external information systems by using middleware and standard protocols.
- **Interoperability**: The system have the capability of interconnecting between business systems by establishing a general data model for cross-business system collaboration.
- **Security**: Ensuring data preservation and reliability through robust authentication and authorization mechanisms is crucial.
- **Traceability:** The system should maintain non-repudiation in network security by recording ownership changes and data operations across the entire business process lifecycle on the blockchain.
- **Scalability:** The system should expand processing, interconnecting, and storage capabilities without necessitating architecture changes.

B. *System overview*

In this article, we establish a Data Sharing System with Decentralized Identifier for the Industrial Internet of Things that is based on blockchain. The architecture is made up of data source service, digital identity service, data uploading service, and data sharing service, as depicted in Fig4.

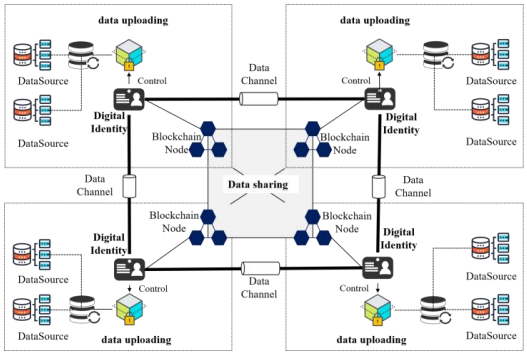

Fig. 3. Architecture of data sharing based on Decentralized Identifier

- Data Source Service

The data source service is an important source of data exchange and sharing, including enterprise data and third-party data. The majority of enterprise data sources are from internal information systems, such as product lifecycle management systems (PLM), product data management systems (PDM), enterprise resource planning systems (ERP), manufacturing execution systems (MES), dealer management systems (DMS), and supervisory control and data acquisition (SCADA). The term "third-party data" primarily refers to information gathered by outside agencies or the government, such as data on water, power, gas, and other public platforms, as well as data on quality inspections.

- Digital Identity Service

The primary functions of the digital identity service are identity management, ownership and access rights management to prevent data leakage. A trusted digital identity is necessary for data sharing because it requires digital identity-based authentication for resource access authorization. For data owners, digital identity is the basis of data rights confirmation and data authorization. For data users, it is necessary to have a digital identity in order to apply for data usage rights. For auditing organizations, arbitration and accountability based on the identities of data sharing participants are required. Currently, data owners lack control over their digital identities, which are primarily controlled and owned by third-party central organizations, and third-party data centers are prone to breach user privacy or sell data owners' data privately. As a result, this paper proposed a method to let the data participants manage and regulate their own identity, so as to realize the confirmation, management and authorization of data. [13][14]

- Data Uploading Service

The data model based on blockchain gathers the data from each company and transforms it into a standard format in accordance with a predetermined data meta model before storing it locally or a distributed storage network. Finally, it publishes the unified description of the data to the blockchain and exchanges the data in accordance with the data sharing policy. A common data meta model needs to be established for the data across the entire product life cycle because various companies may have different descriptions of the same type of data, or even the same data may be defined differently in different systems of the same organization. In order to share data, resources must be represented using a single description model. [15-20]

- Data Sharing Service

The blockchain, which ensures the auditability and traceability of the data sharing process and promotes industry chain collaboration, is the key element of the data sharing layer. Data is a valuable resource in the information era, and every business must handle it well and share it with others in a trustworthy manner to maximize its potential value and foster the development of new industrial models as well as industrial transformation and upgradation. However, data can be easily stolen and tampered with during the sharing process, and it is difficult to identify and trace the person responsible for data leakage. By providing proof and a traceable record of property rights, blockchain technology can ensure data ownership. This paper offers an auditable data sharing mechanism based on blockchain technology, which maintains data sharing and operational behavior information in the form of transactions on the chain, provides data trustworthy verification and traceability, and ensures safe and reliable data sharing among numerous subjects. [21]

C. Key Technology

This section offers a data sharing solution based on the digital identifier. The data sharing has three subjects: the data owner, the data requester, and the data storage agent. The data owners have the ability of managing BID, issuing verifiable credential to the Data BID and encrypting data and preset sharing permissions. The data requester can send a data sharing request to the data owner and a query request to the chain using the specific data identifier. The data storage agent is responsible for providing storage space.

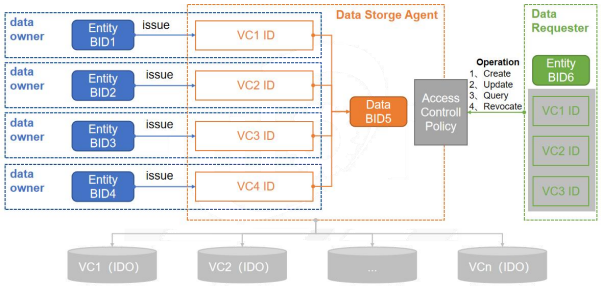

Fig. 4. The model of Data Sharing System with Decentralized Identifier

The solution's essence lies in the seamless interaction among identifiers, verifiable credentials, and sharing policies (as depicted in Fig. 5). Each participant requires a distinct digital identifier and document to partake in industrial chain activities. Similarly, every piece of data necessitates a globally unique data identifier and a corresponding digital document storing the data's verifiable credentials. Particularly in scenarios such as product traceability, data is generated across parts, manufacturing, and logistics links. However, storing this data in diverse systems using disparate identifiers and data models poses challenges in data aggregation. Furthermore, balancing data sharing and privacy protection risks reducing data leakage. The solution addresses this by ensuring trusted transmission off-chain and performing data discovery and verification on-chain.

- Data model of BID document

The key to release the value of data is self-managed identity. Data owners are unable to reveal and exchange data as needed while using the conventional data sharing mechanism since identity and data are controlled by third-party platforms. In order to solve the issue of challenging data identification and secure sharing, this paper presents a set of autonomous management identity mechanisms based on blockchain technology. These mechanisms enable users to govern the ownership, management, and use of data.

In a blockchain-based digital identity, the authentication process is independent of a centralized identity provider, because public key information and personally identifiable user identifiers are anchored on the blockchain for user identity verification. Each BID has a corresponding BID document that serves as a repository for metadata to the BID subject. The BID document metamodel is displayed below, following to the principle of minimal exposure of user information.

1) BID Specification

The BID used in this paper is a 3-segment encoding that follows the W3C DID technical standard, as follows: did, bid method and specification. The BID is created using the public key of the BID controller, meaning it is associated to a series of public/private key pairs, and the controller of the private key verifies its identity as the controller of the BID by matching up these pairs.

did:bid:byo1:zf2LL97siENHnaHYpEHpTHW1MA5RBbPM1v

did method specification

2) BID Documentation

This solution is based on BID, but dividing the identifier as identity identifier and data identifier. The documents of

identity BID and data BID are composed of a bid identifier, a public key, authentication, a signature, and business service information. The difference between the entity bid and the data bid is that the service list in the entity bid includes the credential revocation information of the data owner, and the service list in the data bid includes data list shared data.

Digital objects will have different data for data identification in various links of the industrial chain. Data fragmentation is a serious issue because data is stored in various units. In this paper, a common maintenance method for multi-agent data based on data BID is proposed. This method adds data VC to the document by requesting write permission from the data BID owner, storing the data in various links within the same data bid document, and updating the document.

TABLE I. ENTITY AND DATA BID DOCUMENT

BID Type		DESCRIPTION	NOTE
@context		The rules follow the DID specification and are used to realize the interoperability of different DID documents	Require
Version		Document version	Require
ID		BID	Require
Control		The BID of public keys can control this BID document.	Require
PublicKey		Public keys including four fields: ID, type, controller and Publickeyhex.	Require
Authentication		The BID of public keys can control and manage this BID document.	Require
Entity Service	Credential Revocation List(CRL)	Maintain a maximum prime number to verify whether the VC is revoked	Require
Data Service	Data List(DL)	Data indexed by data BID, including multiple data VC.	Require

- Data model of VC

Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This article provide a mechanism to express data in the industrial internet of things field according to the Verifiable Credentials(VC) specification.

A credential is a set of one or more claims made by the same entity. A verifiable credential is a set of tamper-evident claims and metadata that cryptographically prove who issued it. The credential metadata describe properties of the credential, include an identifier, credential type, issuer, issuance. The claim is a statement about an entity. In this article, the VC is used for describe the data, including Data BID, Has Value of IDO, key word, and storage policy. Digital objects will have different data for data identification in various links of the industrial, so there will have lots of data VC to describe the data BID. In order to to be compatible with existing systems , this article adopts the existing digital object model (IDO), which describes the data model from both object and relationship perspectives, and establishes dynamic data classification to describe the whole life cycle behavior of the object. The object data can be divided into attribute data and business data, where the attribute data describes the property characteristics of the object, and the event data describes the business process data of the object.

TABLE II. DATA VC FOR INDUSTRIAL INTERNET OF THINGS

Data VC Type	DESCRIPTION	NOTE
Credential Metadata	Id	Specify the identifier for credential	Require
	Type	The credential types, which declare what data to expect in the credential	Require
	Issuer	The entity that issued the credential	Require
	IssuanceDate	When the credential was issued	Require
	Prime	Used to verify whether the verifiable credential is revoked	Require
Claims	Data BID	Identifier for the only subject of the credential	Require
	HashValue(IDO)	The data hash of the data based on IDO	Require
	Key word	Describe the data	Require
	Storage Policy	Sharing strategy based on proxy re-encryption technology, such as Re encrypt ciphertext, or address of IPFS	Require
proof	Type	The cryptographic signature suite that was used to generate the signature	Require
	Created time	The date the signature was created	Require
	ProofPurpose	Purpose of this proof	Require
	VerificationMethod	The identifier of the public key that can verify the signature	Require
	SignatureValue	The digital signature value	Require

- Proxy Re-Encryption and On/Off Chain Storage Mechanism

This section suggests a secure data sharing system based on proxy re-encryption for on-chain and off-chain collaboration. Many sensitive data points will be produced in industrial scenarios, and some design drawing data points are too large to be stored on the chain. Ciphertext can be stored and shared in two parts to ease the storage burden and address the issue of ineffective data sharing between systems: (a) Symmetrically encrypted data is distributedly stored in IPFS. (b) For important data like a path and key words are available on the blockchain for storing and sharing. At the same time, it is challenging to achieve effective expansion because the blockchain sharing in the current technology is restricted to the users of the predetermined data. However, it is likely to encounter the need to modify access policies in real life. As a result, this paper combines attribute encryption technology and proxy re-encryption technology. It generates a new key and completes the re-encryption process while realizing one-to-many data sharing. Then it overcomes the shortcomings of an attribute encryption access policy that cannot be changed, cannot be dynamically shared, and has low efficiency, so as to achieve efficient and dynamic data sharing.

1) System initialization

$\text{setup}(k, U) \rightarrow (GP, MSK, PK)$, Input security parameter k, attribution collection U, and generate public parameters GP, Master key MSK, public key PK.

2) Key generation

$\text{KeyGen}(MSK, PK, S_{DO}, S_{DR}) \rightarrow ((SK_{DO}, PK_{DO}), (SK_{DR}, PK_{DR})$, input public parameter GP, Master Key MSK, public key PK, Data Owner (DO) attribute collection $S_{DO} \subseteq U$ and Data Requester（DR）attribute collection $S_{DR} \subseteq U$, generate public Private Key Pair (SK_{DO}, PK_{DO}) of DO and public Private Key Pair (SK_{DR}, PK_{DR}) of DR.

3) Re-encryption key generation

$\text{ReKey}(SK_{DO}, S_{DO}, PK_{DR}, GP, (M', \rho')) \rightarrow rk_{DO \rightarrow DR}$, input the SK_{DO} of data owner and attribute collection S_{DO}, public

parameter GP, the PK_{DR} of data requester, and (M', ρ'), generate Re encryption key $rk_{DO \to DR}$, M' is a $l \times m$ matrix, Row labeling function ρ' switch M' as attribute and $\rho': \{1,2,\ldots,l\} \to S_{DR}$.

4) Encryption

$Encrpt(m, (M, \rho), GP, PK_{DO}) \to CT_{DO}$, input PK_{DO}, public parameters GP, shared structure (M, ρ) and plain-text m, generate cipher-text CT_{DO}. CT_{DO} can switch to CT_{DR}, and could be decrypt by the data requester satisfied the shared structure (M, ρ).

5) R- encryption

$ReEncrpt(PK, GP, CT_{DO}, GP, rk_{DO \to DR}) \to CT_{DU}$, input public key PK, CT_{DO} and Proxy Re encryption Key $rk_{DO \to DR}$, output Re encrypt cipher-text CT_{DR}.

6) Cipher-text decryption

$Decrypt(PK, CT_{DO}, SK_{DO}) \to m$, input public key PK, cipher-text CT_{DO} and SK_{DO}, output m.

7) Re-encryption and decryption

$ReDecrypt(CT_{DU}, SK_{Du}) \to m$, Using the private key SK_{DR}, decrypt the re-encrypted cipher-text CT_{DR} to the plain-text m.

- Operation Protocol

The BID method and VC method define fundamental operations for BID and VC in the blockchain to enhance data interoperability. The BID method governs BID creation, management, and parsing for BID documents. This empowers autonomous BID management. Meanwhile, the VC method regulates VC creation, query, and revocation, ensuring VC compatibility across diverse systems. The VC revocation mechanism verifies VC availability through a prime number table, enhancing the revocation process.

TABLE III. BID METHOD

BID Method	Operator	Data Payload
create BID	BID owner	id, operation:"create", did document
update BID	BID owner	id, operation:"update"
query BID	BID owner, BID Requester	Id, operation:"query"
delete BID	BID owner	id, operation:"delete", proof

Create: A detailed description of the process for creating BID and the BID documents that go along with W3C DID specification. The BID of this scheme is generated directly through a key pair, and the mechanism allows direct verification of the binding relationship between the controller and the identifier.

Read: Specification of how to retrieve the association to a BID document by BID. Three types of methods are usually included: storing the BID document on the blockchain directly; constructing the BID document based on the attributes in the blockchain record through a BID parser dynamically; storing a pointer to the BID document on the blockchain while the corresponding BID document is stored in other decentralized storage networks.

Update: A description of how to modify a BID document's content, usually involving changes to the BID controller key pair and associated topic characteristics. Since the verification of BID document update permissions can only be performed in the blockchain, the BID method specification must define exactly how to authenticate and authorize all update operations.

Revocation: Regulates how BID can be revoked and no longer used. Since data stored on the blockchain is tamper-proof, they can never be "deleted" in a traditional database, but they can be deactivated in a cryptographic way. For instance, deactivating and not updating a BID document's public key can be indicated by erasing its contents.

TABLE IV. VC METHOD

VC Method	Operator	Data payload
create VC	Data Owner	id, operation:"create"
query VC	Data Owner, Data Requester	id, operation:"query"
revoke VC	Data owner	id, operation:"revoke"

Create: The entity BID create a VC of data and store it on the data BID document.

Query： Receiving the VC id and verify it on the chain by vocation and public key of the data VC issuer.

Revocation: Regulates how VC can be revoked and no longer used. A Verifiable credential (VC) revocation mechanism adopted in this article, which can verify the availability of VC. The issuer maintains a prime number table locally, and the VC correspond to a prime number in the table. Verify whether the VC is valid by prime value. The calculation formula is as follows:

$$Accumulator = \prod_{n \in U} u.prime,$$

Where, U is the set of holder, and prime is the code in the VC, which is a prime number. The final calculation result is stored in the service field of the BID document of the issuer. When issuing or revoking a VC, the service field in the BID document needs to be updated.

$$Accumulator \,\%u.prime = 0$$

Use the above formula to accelerate the verification of whether the VC is revoked.

These methodologies, protocols, and mechanisms constitute the foundational elements driving the proposed Data Sharing System with Decentralized Identifier, reinforcing data security, interoperability, and efficient sharing in complex industrial ecosystems.

IV. INTERACTION PROCESS

This section delineates the interaction process among key subjects, including the identifier register process, data catalogue publish process, and data sharing process. The process involves five primary roles:

- **Data Requester**: Requests data from the data owner.
- **Data Owner**: Controls data and predefines data sharing policies.
- **Blockchain**: Facilitates discovery services and records data ownership relationships.
- **IPFS**: Provides storage space.
- **Identity Provider**: Offers identity attribute data.

A. BID Register Process

The data requester and data owner initiate BID generation to validate data ownership before sharing data. The step-by-step process is as follows:

1) Data requester and data owner generate a local public-private key pair and upload the BID document with the public key to the blockchain;

2) The blockchain return a BID identifier to participants;

3) The data requester submits the BID identifier and an application to the identity provider for KYC certification;

4) The digital identity authentication authority signs the identity certificate with its private key. After verification, the identity certificate's hash is uploaded onto the chain.

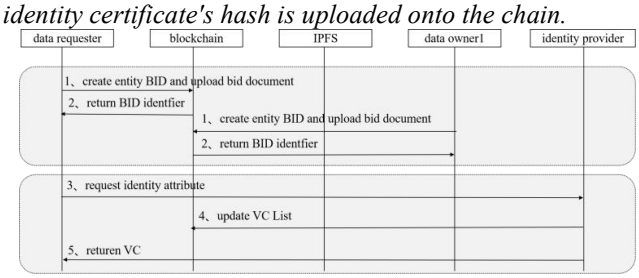

Fig. 5. Identity register process

B. Data Catalogue Publish Process

The data owner creates a data catalogue to share metadata and consolidate data. The step-by-step process is as follows:

1) The data owner generates a BID document for the data, allowing multiple agents to collaboratively maintain a data directory by setting a controller to update data credentials.

2) The blockchain records the BID document and reaches consensus among nodes.

3) The bid dynamically generates data at different stages. The data owner queries to update the BID document.

4) The blockchain verifies the data owner's identity rights to update the document and issues a session cookie to the data owner2;

5) The data owner2 adds the hash of new data vc to the blockchain;

6) The IDO data is stored off-chain.

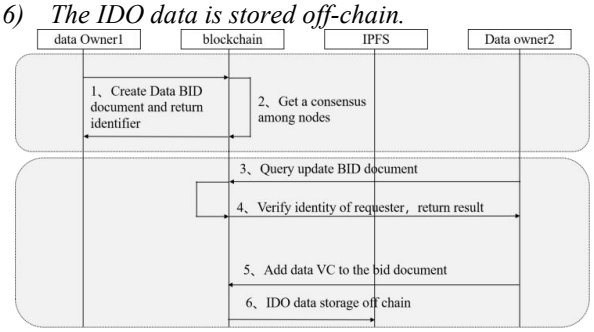

Fig. 6. data catalogue publish process

C. Data Sharing Process

Both the data requester and data owner must generate a BID to authenticate data ownership before sharing. The specific process includes:

1) The data requester searches for data on the blockchain and retrieves data access policies;

2) Th data requester applies for data access permission by ID, public key and attribute to the data owner;

3) The data owner generate Proxy Re-encryption Key $rk_{DO \to DR}$*;*

4) The IPFS re-encrypt cipher-text CT_{DR} *to the data requester;*

5) The data requester decrypts cipher-text CT_{DR} by the private key of data requester.

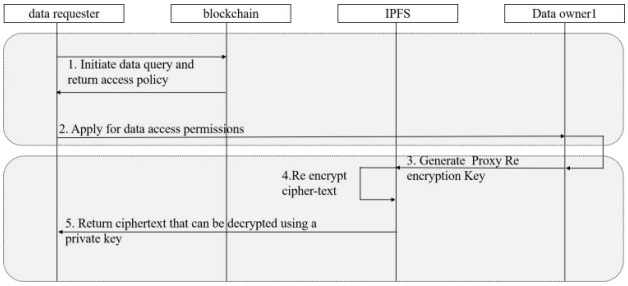

Fig. 7. data sharing process

These processes constitute the interaction framework among involved entities, ensuring robust validation, transparent data management, and secure sharing within the ecosystem.

V. Performance Evaluation

A. Implementation

Utilizing the Xinghuo Blockchain Infrastructure & Facility, this study establishes an industry chain collaboration platform and conducts experimental validation within the auto repair service scenario. In the context of vehicle maintenance, the scenario involves service stations checking vehicles for warranty eligibility. If a vehicle meets the warranty criteria, the service station performs free repairs and forwards a claim request to the Original Equipment Manufacturer (OEM). Subsequently, the OEM investigates the issue based on quality analysis and raises a claim with the parts manufacturer. However, due to fragmented information across various databases, the service station faces challenges in verifying whether the damaged parts fall under the warranty scope. By aggregating data from diverse databases to compile a comprehensive claim list, service stations can enhance the accuracy of damaged parts verification, reduce OEM claim costs, and offer high-value services to OEMs, suppliers, and end customers.

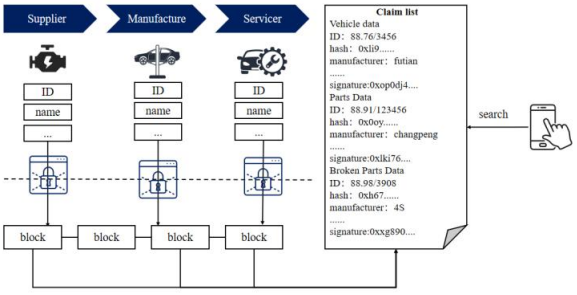

Fig. 8. auto repair service scenario

B. Identity Registration

Collaborative participants in auto repair services, including parts suppliers, auto manufacturers, and maintenance stations, initially register their identity accounts via Xinghuo Wallet. This process generates a user-managed public-private key pair used for subsequent identity and data management activities, such as digital signature, data validation, and data sharing authorization. The account registration interface is illustrated in the following figure.

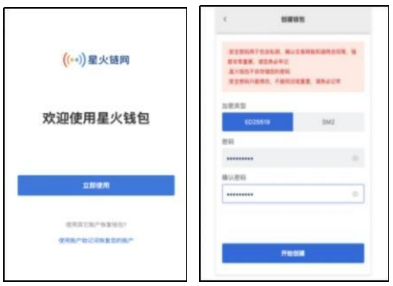

Fig. 9. BID digital identity registration

C. *Data sharing*

Participants involved in auto repair services, such as parts suppliers, auto manufacturers, and maintenance stations, undertake the following steps for data sharing and supporting subsequent auto repair service scenarios:

- Data Standardization

Original data from various sources is converted to a unified format based on the IDO template via the data sharing platform's integrated business metadata dictionaries for the industry chain.

- Data up to the chain

Described data is stored on the chain as catalogues, and business data is stored in IPFS.

- Data sharing and car maintenance model construction

The auto manufacturer spearheads the construction of the auto repair claim application, inviting participation from auto parts suppliers and repairers. Based on shared data, the OEM develops an auto repair service claim application. The maintenance station verifies relationships between auto parts and vehicles, ensures data authenticity during repairs, and associates new parts information with vehicle data to prevent reused parts for claims.

Fig. 10. Claims Form

The auto repair service platform has undergone testing and verification in a prominent domestic car manufacturer, resulting in an estimated reduction of 50 million in after-sales claims misjudgment and service errors.

D. *Experimental Analysis*

To further validate the BID-IDO-based collaborative data sharing platform's performance within industrial chains, the paper conducts tests on throughput and average latency for different transaction volumes in the Xinghuo blockchain network. These analyses exhibit the platform's ability to handle considerable transaction volumes while maintaining stable performance and efficiency.

Throughput Analysis: Figure 12 illustrates the throughput for query and upload transactions. The peak throughput of the blockchain network stabilizes at 100 transactions/s for uploaded transactions. Query throughput consistently rises with the sending rate, indicating robust support for high sending rates.

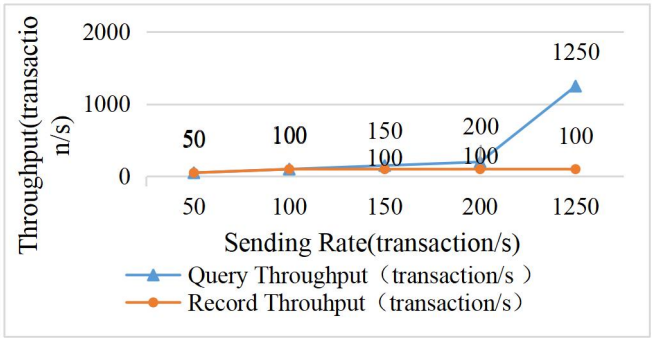

Fig. 11. Throughput of Data Upload and Query

Average Delay Analysis: Figure 13 showcases the average delay for data uploading and querying concerning different transaction volumes. The average delay for both query and upload increases proportionally with transaction volumes but remains stable up to 10240 transactions. This scheme demonstrates high system throughput and efficient data transactions.

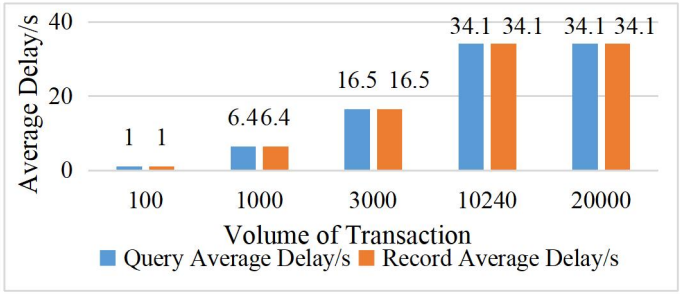

Fig. 12. Average Delay of Data Upload and Query

VI. CONCLUSIONS

The cornerstone of achieving synergy within industrial chains hinges on trusted data sharing among multiple entities. Presently, challenges persist regarding inconsistent data descriptions, difficulties in ascertaining data rights, and a lack of trust among subjects engaged in data-sharing transactions. To address these issues, this paper proposes a blockchain-based data-sharing mechanism tailored for industrial chain collaboration.

To validate the suggested BID-IDO-based collaborative data sharing mechanism's viability and effectiveness, a real-world case study was conducted in the auto factoring service scenario, leveraging the blockchain infrastructure of "Xinghuo". The study focused on testing data uploading and query throughput, affirming the practicality of the proposed mechanism.

This paper primarily designs and validates the overarching architecture of industry chain collaboration from a global perspective. Future research endeavors will delve into practical integration mechanisms between the proposed scheme and existing enterprise information systems. Additionally, emphasis will be placed on developing data privacy protection mechanisms and dynamic data pricing mechanisms to further incentivize enterprises to engage in data sharing. These avenues of exploration aim to foster a more robust and comprehensive framework for collaborative data sharing within industrial chains.

REFERENCES

[1] Zhang Yachuan. Research and implementation of blockchain-based data sharing model and key mechanisms for Internet of Things [D]. Beijing Institute of Technology, 2021. doi:10.26935/d.cnki.gbjgu.2021.000118.

[2] Liu Yangquan. Research on user identity confirmation and data reimbursement sharing application based on national secret algorithm and blockchain[D]. South China University of Technology, 2021. DOI:10.27151/d.cnki.ghnlu.2021.003118.

[3] Zhang Ting. Research on digital asset confirmation transaction model based on blockchain technology[J]. Journal of Fujian Engineering College,2019,17(01):65-71.

[4] Wen Bilong,Chen Youliang. Research on enterprise data sharing model based on blockchain[J]. Computer Technology and Development,2021,31(01):175-181.

[5] Xie R. Q., Zhang W. D.. Research on blockchain-based digital resource authorization and trading scheme[J]. Enterprise Economy,2022,41(01):65-73.DOI:10.13529/j.cnki.enterprise.economy.2022.01.007.

[6] Meng Hongwei,Tang Cong,Li Jun,Zhu Haogang,Song Wenliu. Research on blockchain-based data sharing and exchange method[J]. Journal of Hebei Academy of Sciences,2021,38(01):17-23.DOI:10.16191/j.cnki.hbkx.2021.01.003.

[7] WANG Hailong,TIAN Youliang,YIN Xin. A blockchain-based scheme for big data corroboration[J]. Computer Science,2018,45(02):15-19+24.

[8] Cai Chang,Zhao Yanyan,Li Mengjuan. Blockchain-enabled data asset identification and tax governance[J]. Taxation Research,2021(07):90-97.DOI:10.19376/j.cnki.cn11-1011/f.2021.07.014.

[9] Neisse, Ricardo & Steri, Gary & Nai Fovino, Igor.(2017). A Blockchain-based Approach for Data Accountability and Provenance Tracking.

[10] Zhu ZQ, Yao ZY, Zhu WEIH, Zhao HH, Pan CHF, and S Xue-Ming. Anonymous traceable blockchain data transaction scheme[J]. Journal of Applied Sciences,2022,40(04):653-665.Zhang Jin, Gu F, Gu Xinjian, Ji Yangjian, Li Linli, Zheng Fanying. A blockchain-based collaborative data sharing approach for multiple value chains [J/OL]. Computer Integrated Manufacturing Systems:1-24 [2022-09-16]. http://kns.cnki.net/kcms/detail/11.5946.TP.20220714.1913.004.html

[11] Liang, Xiubo, Wu, Junhan, Zhao, Yu, Yin, Keting. A review of blockchain data security management and privacy protection technology research[J]. Journal of Zhejiang University (Engineering Edition),2022,56(01):1-15.

[12] Li Dongxing. Research on blockchain-based authentication technology for network entities [D]. University of Defense Technology, 2018. doi:10.27052/d.cnki.gzjgu.2018.000672.

[13] Zhang Jin, Gu F, Gu Xinjian, Ji Yangjian, Li Linli, Zheng Fanying. A blockchain-based collaborative data sharing approach for multiple value chains [J/OL]. Computer Integrated Manufacturing Systems:1-24 [2022-09-16]. http://kns.cnki.net/kcms/detail/11.5946.TP.20220714.1913.004.html

[14] Wang Zhe. Design and implementation of blockchain-based digital identity management system[D]. Southeast University,2020.DOI:10.27014/d.cnki.gdnau.2020.002026.

[15] Zhou Tong. Research and Application of Trusted Data Generalization Method based on Blockchain Technology[D]. University of Science and Technology of China,2019.

[16] Sheng, Nianzu, Li, Fang, Li, Xiaofeng, Zhao, He, Zhou, Tong. A blockchain smart contract-based approach to assetization of IoT data[J]. Journal of Zhejiang University (Engineering Edition),2018,52(11):2150-2158.

[17] Sun L, Li XF, Zhao H, Yu B, Zhou T, Li CIR. An NFT-based physical on-chain assetization approach [J/OL]. Journal of Zhejiang University (Engineering Edition):1-13 [2022-09-16]. http://kns.cnki.net/kcms/detail/33.1245.T.20220905.1009.002.html

[18] Zhao M,Dong DZ. A data asset management mechanism based on blockchain technology[J]. Big Data,2021,7(04):49-60.

[19] Li Chenglong. Design and implementation of blockchain-based digital asset management system for IoT edge-side [D]. Beijing University of Posts and Telecommunications, 2020. doi:10.26969/d.cnki.gbydu.2020.001874.

[20] Ke Xiang. Research on blockchain-based data pricing mechanism and transaction system[D]. Beijing University of Posts and Telecommunications, 2021. doi:10.26969/d.cnki.gbydu.2021.001525.

[21] Qi A-Min, Pan Jia. The establishment of data right, data sovereignty and the basic principles of big data protection[J]. Journal of Soochow University (Philosophy and Social Science Edition),2015,36(01):64-*70+191.DOI:10.19563/j.cnki.sdzs.2015.01.013.*