Postprint: A Survey on Hyperledger Applications in IoT from a Reconstructed Graph Perspective

Authors: Leng Zeqi, Wang Kunhao, Liang Wei, Zheng Yuefeng

Date: 2022-05-10T11:22:58Z

Abstract

In deploying blockchain-based IoT applications, technical obstacles have emerged, including lack of fine-grained privacy protection, low transaction processing efficiency, high latency, and insufficient flexibility and dynamism. To further advance the popularization and practical deployment of blockchain technology in IoT, Hyperledger—dedicated to enterprise-grade blockchain standards—has attracted widespread attention from the research community. However, current research lacks an objective survey of Hyperledger-based IoT. This study aims to review Hyperledger research in the IoT domain from a unique perspective. To demonstrate more intuitive differences and provide technical integration processes, this study proposes a reconstruction diagram analysis method. Reconstruction is the process of integrating core designs and original architecture diagrams from literature to reconstruct diagrams that can showcase the core ideas of the literature. This method aims to visualize the core ideas of literature. Finally, future research on Hyperledger in IoT is prospected and summarized from four directions: low-power consensus algorithms, intelligent transaction verification, on-chain and off-chain hybrid storage, and customized incentive mechanisms.

Full Text

Preamble

Vol. 39 No. 9
Application Research of Computers
ChinaXiv Cooperative Journal

Survey on Application of Hyperledger in IoT from the Perspective of Reconstructing Diagrams

Leng Zeqi, Wang Kunhao†, Liang Wei, Zheng Yuefeng
(College of Computer Science, Jilin Normal University, Siping 136000, China)

Abstract: The deployment of blockchain-based IoT applications faces technical obstacles including lack of fine-grained privacy protection, low transaction processing efficiency, high latency, and insufficient flexibility and dynamism. To further promote the adoption and practical implementation of blockchain technology in IoT, Hyperledger—dedicated to enterprise-grade blockchain standards—has attracted widespread attention from the research community. However, current literature lacks objective surveys of Hyperledger-based IoT systems. This study aims to review Hyperledger research in the IoT domain from a unique perspective. To demonstrate more intuitive differences and provide a streamlined process for technology convergence, we propose a reconstructing diagrams analysis method. Reconstruction is the process of merging the core design from literature with original architecture diagrams to create new diagrams that reveal the document' s core ideas. This approach visualizes the essential concepts of the literature. Finally, we prospectively summarize future Hyperledger research in IoT across four directions: low-power consensus algorithms, intelligent transaction verification, on-chain/off-chain hybrid storage, and custom incentive mechanisms.

Key words: hyperledger; IoT; blockchain

0 Introduction

With the rapid development of smart devices and high-speed networks, IoT has emerged as a low-power network with constrained resources, and its main standards have been widely accepted and popularized [**?**]. However, technical vulnerabilities and defects have hindered IoT development, primarily concentrated in data security issues and network congestion caused by centralized servers. Blockchain transcends traditional trust models by shifting network decisions from a few nodes to collective decisions by all participants, increasing transaction transparency and storage trustworthiness. Consequently, blockchain-based IoT research has been extensively explored, partially addressing secure data storage and integrity verification for IoT data. Nevertheless, blockchain' s limitations in privacy protection, load balancing, and network latency prevent it from meeting commercial application standards, particularly for IoT projects.

In recent years, Hyperledger has emerged as a potential solution to these challenges. Beyond general blockchain characteristics, Hyperledger provides new capabilities in four aspects: security, interoperability, consensus, and performance. In terms of security, Hyperledger designs fine-grained access control and private data management, offering privacy protection mechanisms and ledger isolation between enterprises, and providing infrastructure for enterprise-grade solutions. To protect consumer interests, Hyperledger supports autonomous access control,

enabling the design and implementation of consumer-centric applications. Its highly modular structure ensures that system-wide operations remain unaffected when a single module or component fails. This feature also enables faster integration with various systems. These pluggable components allow Hyperledger to satisfy diverse business logic within the same distributed network.

Regarding interoperability, Hyperledger has developed a peer-to-peer identity authentication system that provides infrastructure for consumers and enterprises to perform cross-chain, cross-layer, or cross-system operations using portable digital identities. In consensus, pluggable consensus mechanisms enable different businesses to reach agreement within the same distributed network. Currently supported consensus algorithms cover energy-saving, reputation, proof-of-work, proof-of-elapsed-time, authority, fault tolerance, and delegated proof-of-stake, significantly enhancing Hyperledger' s applicability. For performance, network decisions are made by a certain number of nodes rather than all nodes, substantially reducing computational costs while ensuring trust. Hyperledger networks can be dynamic, enabling connections for large numbers of portable devices. Hyperledger subdivides transaction-processing nodes into four roles, each with different functions, and allows developers to adjust node deployment according to network load. Additionally, decoupled ordering processes can mitigate network congestion and latency.

Hyperledger-based IoT research has grown annually, yet no comprehensive survey of Hyperledger in IoT exists. Moreover, most blockchain surveys are text-heavy with charts as supplementary material. While concise language showcases the latest application progress and trends, it fails to intuitively present the design 思路 of these studies, making it difficult for researchers to obtain sufficient technical integration guidance and core ideas from condensed text.

To better address these issues, this study proposes a novel analysis method: the reconstructing diagrams method. The main advantages of this approach are twofold: first, it displays research progress and core ideas in the most intuitive way, highlighting differences between studies; second, it adds more design details by visualizing the core designs from literature. The main contributions of this study are:

a) We propose a reconstructing diagrams analysis method. This research considers two scenarios: first, for literature without architecture diagrams, we extract core designs to construct reconstruction diagrams that maximally restore the author' s original design 思路; second, for literature with existing architecture diagrams, we reconstruct the original diagrams based on core designs to add more implementation details.

b) We showcase the latest application progress of Hyperledger in IoT. Since current Hyperledger research in IoT is fragmented, this study organizes 52 papers by application domain. These domains involve IoT data security, smart agriculture and fisheries, smart city monitoring, smart toys and IoT games, smart fitness, smart transportation, smart power grids, smart

building projects, and smart energy (energy-saving direction).

1 Overview of Hyperledger Technology

Hyperledger is dedicated to developing enterprise-grade blockchain standards. At the conceptual level, Hyperledger is a "greenhouse" ecosystem where all technologies are developed by the community, providing an open-source and secure collaborative environment for users, developers, and suppliers across various fields. Therefore, Hyperledger encourages interoperability among participants in similar domains, with each participant obtaining necessary information through communication. This effective collaboration significantly reduces redundant work, allowing participants to focus on incubating new ideas. To improve code quality, Hyperledger' s Technical Steering Committee (TSC) regularly reviews community code and projects, discarding unqualified ones.

Additionally, Hyperledger encourages specialization [**?**], enabling more people to concentrate on fewer tasks and improving participants' expertise. Developing participant specialization also helps unify intellectual property rights, so contributors to the Hyperledger community need not worry about hidden legal issues.

Hyperledger' s generic architecture comprises nine components: consensus layer, contract layer, communication layer, data storage module, encryption module, identity service module, policy service module, Application Programming Interfaces (APIs), and interoperability module [**?**]. These components form a highly modular structure where failure in any component does not affect overall operations.

1.1 Overview of Enabling Technologies

As one of the largest open-source projects, Hyperledger currently has 18 top-level projects (including one deprecated project). These projects provide key technologies for Hyperledger and enable its widespread application across various domains. Technically, Hyperledger involves cross-system identity authentication, access control, multi-channel (multi-chain) platforms, visual interfaces, mobile applications, benchmarking, cryptography libraries, Ethereum clients, and business logic development. In applications, Hyperledger has been applied to mainstream fields such as IoT, digital healthcare, supply chain traceability, finance, digital evidence, and artificial intelligence.

Hyperledger currently classifies top-level projects into four categories: distributed ledgers, domain-specific, libraries, and tools. Each contributed project requires regular maintenance by developers, meaning that beyond normal operations, developers must promptly address issues for new participants. The TSC regularly reviews project maintenance and decides whether projects advance to the next stage. When a project reaches the "no longer recommended" stage, it is abandoned by the community after six months, though project information and partial code remain available.

Generally, all Hyperledger projects must go through six stages: Proposal, Incubation, Graduated (Active), Dormant, Deprecated, and End of Life. Project status is dynamic and determined through multiple reviews by project maintainers and the TSC. Currently, top-level projects have only two statuses: Graduated and Incubation. Graduated projects are the most active, with the largest membership and most code contributions. Due to continuous updates, active projects provide mature technologies and infrastructure for Hyperledger. Based on official information from https://www.hyperledger.org/, this paper analyzes the core architecture and innovative designs of currently Graduated projects.

1.1.1 Overview of Hyperledger Fabric Fabric is the cornerstone of Hyperledger, and its innovative design enables widespread application across various domains. Fabric was the first to introduce permission mechanisms, enabling confidential transactions and ledger isolation across industries. Fabric' s architecture consists of four component types: Membership services, Certificate Authorities (CA), Nodes, and Peers. Membership services provide digital certificates for blockchain nodes. CA issues identity certificates to all nodes in the network, which complete transactions using private and public keys. Nodes consist of permitted network participants, while Peers are roles in the blockchain network that perform different tasks.

1.1.2 Overview of Hyperledger Sawtooth Sawtooth' s innovative design lies in its strong dynamism and robustness. Each Sawtooth node comprises a fixed component (validator) and optional components (Transaction Processor, REST API, and Client). In Sawtooth networks, initial nodes broadcast packets to discover nearby nodes, which can join the network according to rules and broadcast their one-hop neighbors. Any node with a response can join the network.

Sawtooth' s architecture has five core components: peer-to-peer network, distributed log, state machine/smart contract logic layer, distributed state storage, and consensus algorithm. The peer-to-peer network allows nodes to communicate via TCP, including blocks and peer information. Sawtooth networks broadcast transactions through the Gossip protocol. The distributed log includes ordered transaction lists, with nodes ordering transactions according to consensus algorithms. Sawtooth extends smart contract functionality by treating them as state machines or transaction processors. The smart contract logic layer includes core smart contracts (e.g., Settings, identity, validator registry) and transaction families (e.g., IntegerKey, BlockInfo, HyperDirectory, Marketplace).

Sawtooth uses Radix Merkle Tree storage structure, which combines Radix Tree and Merkle Hash Tree functions to store serialized contract states. The consensus component provides a consensus interface that allows various consensus algorithms.

1.1.3 Overview of Hyperledger Iroha Iroha also provides a distributed framework, with distinctive features in permission management, fault tolerance, and performance efficiency. Unlike other platforms, Iroha requires authorization not only for node joining but also for data reading and writing. Iroha allows rich built-in commands to simplify asset management, eliminating the need for preset assets. Its fault-tolerant consensus algorithm, Crash, enables low latency.

The Iroha architecture includes 11 components: Torii, MST Processor, Peer Communication Service (PCS), Ordering Gate, Ordering service, Verified Proposal Creator (VPC), block creator, Block Consensus (YAC), Synchronizer, Ametsuchi Blockstore, and World State View (WSV). Torii receives and preprocesses transactions, MST Processor forwards transactions and receives peer signatures, PCS primarily passes transactions to Ordering Gate. Ordering Gate validates stateless transactions with other peers, while the Ordering service in each peer creates transaction proposals and validates whether stateless transactions pass initial verification. After receiving proposals, Ordering Gate broadcasts transactions to VPC in the simulator. VPC performs state validation on transactions, and block creator forms new blocks sent to YAC for consensus. YAC forwards final messages to multiple peers. Synchronizer downloads blocks from block storage and adds missing blocks to peers. WSV displays the latest block information.

1.1.4 Overview of Hyperledger Indy Indy' s innovative design is its decentralized identity authentication system, whose core feature is self-sovereign identity. Once established, identity cannot be revoked, selected, or associated by any institution or person without the identity owner' s permission. Thus, Indy can provide users with portable identity proofs without third-party centralized authentication. The Indy network has only two node types: validator nodes (few in number) and observer nodes (many in number). Validator nodes process write requests and participate in consensus, while observer nodes handle read requests and may become validator nodes based on reputation levels.

1.1.5 Overview of Hyperledger Aries As the only active project that is not a distributed ledger platform, Aries provides secure communication methods for decentralized identity management and verifiable credentials. Aries has four core components: agents, DID communications, protocols, and key management. Agents provide trusted proxies for self-sovereign identity authentication. Users download or write agents according to their needs, such as IoT agents, cloud agents, protocols, scale, and privacy requirements. DID communications enable information exchange among multiple trusted agents based on decentralized protocols, following a message-based (notification), asynchronous (request-response), and simplex paradigm. Key management provides a distributed key management system using three key types: master keys, key encryption keys, and data keys. This distributed system protects identity owners from central failures of third-party institutions, enabling network connections and key exchanges without organizational dependence.

Aries facilitates decentralized identity authentication implementation, and peer-to-peer certificate authentication will eradicate the surveillance economy. This authentication method is highly portable and applicable, allowing users to store work proofs or other identities in wallets and decide which information can be publicly queried.

1.1.6 Overview of Hyperledger Besu Besu is an enterprise-grade Ethereum platform with seven core modules: Ethereum Virtual Machine (EVM), P2P network, Storage, Permissioning, Privacy, User-facing API, and Monitoring. For privacy, Besu ensures private interactions through Tessera nodes. For enterprise orientation, Permissioning enables node and account permissions, allowing only specific nodes and accounts to access the network. Storage maintains blockchain and world state, including account states, account storage, and code storage. Besu provides monitoring interfaces for users to monitor nodes and networks.

Besu supports two node types: Full nodes and Archive nodes. Full nodes store only current block states to ensure the latest state, while Archive nodes store all historical states from the genesis block. Besu provides three APIs: HTTP/WebSockets-based JSON-RPC, WebRocket-based RPC publish/subscribe, and HTTP-based GraphQL. Besu is compatible with the Ethereum mainnet and supports both public and private networks, enabling enterprise-grade Ethereum platform construction.

2 Introduction to IoT

IoT comprises two parts of varying difficulty. One segment is the Internet of Things (IoT), a significant improvement where the dominant interaction type is client-server [**?**]. IoT provides increasingly intelligent services to meet rich semantic requests. The other segment is the Industrial Internet of Things (IIoT), designed for complex task collaboration, data-based decision-making, and remote machinery access [**?**].

IoT Concept Introduction

IoT is a new technological paradigm—a global network of machines and devices capable of interacting with each other. At the application level, IoT can complete various lightweight tasks according to consumer preset requirements, such as automatic cleaning, intelligent recognition, and traffic light coordination. The value of IoT for enterprises lies in connected devices' ability to communicate with each other and integrate with vendor-managed inventory systems, customer support systems, business intelligence applications, and business analytics [**?**].

IIoT Concept Introduction

The Industrial Internet of Things softwareizes and models industrial knowledge and experience to improve manufacturing efficiency and quality. At the appli-

cation level, IIoT differs from IoT primarily in its design for heavy-duty tasks such as intelligent manufacturing, environmental monitoring, intelligent transportation, and enemy reconnaissance.

2.3 Integration Points Between Hyperledger and IoT/IIoT

According to GSMA statistics, global IoT device connections reached 14.7 billion in 2021. IoT has been widely applied across numerous fields. While blockchain technology has been extensively studied, practical implementation remains challenging, and IoT urgently needs new technologies to address its challenges. This paper summarizes the fundamental advantages of Hyperledger-IoT integration:

a) Distributed storage and collaboration ensure tamper resistance for massive data and decisions.

b) Fine-grained permission control enhances privacy protection between enterprises and consumers.

c) Fine-grained state-based endorsement policies strengthen enterprise transaction security.

d) Efficient consensus mechanisms effectively reduce network latency for device or heavy machinery collaboration, enabling faster node state agreement and millisecond-level response times for IIoT.

e) Peer-to-peer identity authentication ensures high identity portability, greatly facilitating identification for portable IoT devices.

f) Highly modular frameworks and support for diverse chaincode languages enable rapid integration with any IoT or IIoT system.

g) Dynamic networks provide strong flexibility and robustness, meeting basic IoT business requirements.

3 Hyperledger Applications in IoT Research

This section subdivides IoT research into nine application domains: IoT security, smart fisheries and agriculture, smart toys and IoT games, smart fitness, smart city monitoring, smart power grids, smart transportation, smart building projects, and smart energy (energy-saving direction).

3.1 IoT Security Domain

Current research focuses more on data privacy, confidentiality, and integrity security than other requirements. Since massive IoT data is primarily processed by centralized cloud services, privacy and confidentiality are difficult to guarantee.

Wang [?] proposed a Hyperledger Fabric (v1.1.0)-based IoT data integrity verification scheme. As shown in Fig. 1, IoT data is divided into multiple fragments, with smart contracts (chaincode) preset to automatically verify and process device metadata and store records. Cloud service providers only return verification results to users, reducing overhead and computational costs, but lack design for handling complex data types. To address transaction security between different cloud providers, Yang [?] proposed a Hyperledger Fabric (v1.0)-based federated cloud system. This system designs a trusted-level mechanism determined by user credit values, replacing centralized management and enabling secure transactions between cloud providers through chaincode signing, ensuring trust to some extent and improving cloud resource utilization.

In cloud services storing datasets, risks exist of malicious tampering with data owners' dataset models and single-point failures. Dib [?] proposed a Hyperledger Fabric (v1.1)-based dataset utilization system. Cloud services store only encrypted data models from data owners, and consumers pay for shared datasets through Hyperledger. This enhances transparency in dataset utilization and dataset security but lacks supervision strategies for high-trust-level users. To address data sharing among different participants, Yu Jingang [?] proposed a Hyperledger Fabric (v1.4.0)-based IoT data sharing model. The model designs a new gateway for data collection, certificate storage, identity verification, and data format cleaning and conversion. It identifies key components of Hyperledger-based IoT data sharing models and confirms that Hyperledger can improve IoT data sharing efficiency.

In supply chain systems, data security is the primary concern. Cao [?] proposed a steel industry traceability system (Sawtooth). As shown in Fig. 2, smart contracts store data from each link, and regulatory departments obtain entire circulation data from blocks. Consumers scan RFID codes to obtain final traceability information. Zhang Sen [?] proposed a cold chain logistics data security scheme. As shown in Fig. 3, it uses Hyperledger Fabric to ensure real-time logistics data on-chain, combined with Diffie-Hellman key exchange to generate shared keys for user privacy protection.

Automatic handling of compromised devices can timely prevent dangerous behavior. Rodriguez [?] proposed a Hyperledger Fabric-based IoT device monitoring scheme. Source and target devices verify transaction reliability through Hyperledger endorsement nodes, with chaincode automatically isolating dangerous devices, ensuring device data security. To address latency and efficiency issues, Kim [?] proposed a lightweight solution combining deep learning and Hyperledger Fabric. As shown in Fig. 4, the system uses K-Means clustering on network node behavior, geographic coordinates, and other information to generate multiple clusters. The system creates corresponding chain validators (composed of four screened nodes) to verify communication legitimacy and store transaction records, improving data security to some extent.

IoT device configuration data is a crucial component of IoT data; once tampered with, it directly affects intended task directions. Helebrandt [?] proposed a Hy-

perledger Composer-based IoT device configuration file system. As shown in Fig. 5, it designs on-chain and off-chain (for large configuration files) storage solutions, encrypting configuration modification messages and loading management IDs, device IDs, and timestamps into new blocks. However, it lacks supervision of more configuration information such as power, CPU utilization, and disk space. Multi-level proxy methods help ensure IoT data transmission security. Mbarekp [**?**] proposed a Hyperledger Fabric (v1.1.0)-based multi-level proxy IoT data protection system. As shown in Fig. 6, three-level proxy inspection verifies block validity, ensuring data security.

Since Hyperledger key management is mostly issued and managed by government nodes, security issues such as key tampering and forgery remain. Ribeiro [**?**] proposed a distributed key management scheme (Fabric v1.4.0). Devices and connection servers sign smart contracts to establish temporary session keys, protecting device privacy and addressing device key security issues to some extent.

Some research focuses on authentication, authorization, and accounting security requirements in IoT. Hang [**?**] proposed a Hyperledger Fabric (v1.2)-based IoT communication platform. As shown in Fig. 7, the system uses smart contracts to enable secure device access, storing data in Hyperledger to improve transaction security. Its lightweight architecture provides feasibility for large-scale IoT device communication. To improve smart contract reliability, Liu [**?**] proposed a data access control system (Fabric v1.4.3). Multiple users jointly formulate access control policies, with Hyperledger storing records and data URLs, reducing on-chain storage pressure.

To address centralized root management in top-level domain authorization, Zhang [**?**] proposed a Hyperledger Fabric (v1.4)-based distributed root management scheme. As shown in Fig. 8, domain authorization transactions are sent to multiple authorization nodes, with only those responding within a time threshold deemed valid. Smart contracts automatically process and count authorization messages. To improve identity verification efficiency, Chi [**?**] proposed a data authentication scheme (Fabric). As shown in Fig. 9, user identity information is divided into tag data and real data. The K-medoids algorithm [**?**] partitions the network into multiple communities, and Cosine similarity algorithm [**?**] measures similarity between node tag data and community data. Users retrieve relevant information based on tags, improving efficiency in identity-related data retrieval and sharing. Zhang Jianghui [**?**] proposed a Hyperledger Fabric (v1.4.4)-based access control policy model. As shown in Fig. 10, it uses smart contracts for fine-grained access control permission management, demonstrating good defense against excessive authorization and privilege escalation.

In Hyperledger, centralized CA authorization and authentication may cause tampering and forgery risks. To address CA centralization, Siris [**?**] proposed two decentralized authorization strategies based on Hyperledger Fabric. As shown in Fig. 11, multiple organizational authorizations replace unified CA node authorization, with authorization nodes for transactions at a given moment screened based on response time. This ensures distributed authorization

security while improving efficiency, though the first strategy requires higher computational costs. To address CA centralized authentication issues, Kakei [**?**] proposed a distributed CA authentication policy (Fabric). As shown in Fig. 12, Texas CA nodes are divided into meta-CAs and CAs, with cross-certification between meta-CAs and CAs determining CA node trustworthiness, improving CA node reliability to some extent.

To provide a universal Hyperledger-based authorization architecture, Pajooh [**?**] proposed a cellular system-based multi-layer blockchain model (Fabric). As shown in Fig. 13, the network is divided into three layers using Swarm Intelligence (SI) and Evolutionary Computation (EC) algorithms, connecting multiple base stations in Hyperledger to achieve distributed authorization and authentication for IoT devices. This model reduces network load but lacks actual test platform implementation.

Hyperledger-based IoT systems should meet service availability security requirements, and data encryption is an effective method to prevent attacks. Zhou [**?**] proposed a fully homomorphic computation-based IoT data protection scheme (Fabric). It uses homomorphic encryption algorithms to encrypt session messages and multiple servers to verify message tampering, effectively protecting IoT data from attacks with good performance. Hou [**?**] proposed an edge computing data protection scheme. As shown in Fig. 14, device messages are obtained through LoRa gateways, with uplink messages stored in Hyperledger, reducing the possibility of message attacks.

3.2 Smart Fisheries and Agriculture Domain

Information technology advances have promoted digital transformation in fisheries and agriculture. Conceptually, smart fisheries and smart agriculture are similar—both deeply integrate big data, blockchain, and AI to obtain real-time data collection, quantitative decision-making, intelligent control, precise investment, yield prediction, and other personalized services [**?**]. Smart fisheries focus on water quality monitoring for large-area analysis and regulation, while smart agriculture primarily demands intelligent decision-making through real-time monitoring and analysis to improve productivity and resource efficiency [**?**]. Currently, Hyperledger applications in smart fisheries and agriculture are limited, mainly addressing data tamper resistance and real-time data streams.

Accurate fishery regulation and tamper-proof data present certain difficulties. Hang [**?**] proposed a Hyperledger Fabric (v1.4.3)-based smart fish farming platform. As shown in Fig. 15, water level sensors predict actual water level data, Kalman filter algorithms eliminate errors, and the system calculates required water levels and durations for automatic regulation. This platform provides a more secure development 思路 for smart fisheries but lacks interaction with different fisheries.

In smart farm systems, real-time crop monitoring and monitoring data reliability are concerns. Lee [**?**] proposed a Hyperledger Sawtooth-based middleware

for food growth environment monitoring. As shown in Fig. 16, sensor-collected crop data is uploaded to the chain, with Hyperledger performing 10-cycle authentication on monitoring data. This proves that POET (Proof of Elapsed Time) consensus has faster processing efficiency and practical applicability. To address long traceability information query times, Yi Weiguo [**?**] proposed a Hyperledger Fabric (v2.0)-based enhanced fruit and vegetable product traceability credibility system. As shown in Fig. 17, it improves data preservation, pre-verification, and traceability performance through secondary on-chain data hashing and verification, reducing query time algorithm complexity.

3.3 Smart Toys and IoT Games Domain

Although both smart toys and IoT games belong to intelligent entertainment services, their implementation goals differ significantly. Smart toy users are primarily children, integrating IT technology for phone calls, children' s education, web browsing, location tracking, and other services. Global smart toy types include add-on mechanical toys, voice/image recognition toys, screenless toys, life toys, educational and building games, and health tracking/wearable toys [**?**]. However, smart toys face horizontal data exchange problems because heterogeneous APIs make cross-system data exchange difficult [**?**], resulting in large amounts of redundant data (unneeded by users) that cannot be effectively utilized. IoT games break through traditional image and video-based concepts, using IoT technology as the main driver for interactive games between real-world physical objects to obtain rewards. IoT games target dispersed audiences, primarily location-aware games. However, such games lack strong technical guarantees for task authenticity and user privacy protection. Hyperledger provides effective solutions to these problems.

In smart toy data sharing, horizontal data secure exchange presents challenges. Yang [**?**] proposed a Hyperledger Fabric (v1.0)-based toy data exchange model. As shown in Fig. 18, toy data undergoes desensitization processing, suppliers generate unique identifiers for toys, and Hyperledger inspects and stores toy data in CouchDB to ensure storage security.

In Hyperledger-based IoT game systems, issues include real-time game task updates, player privacy, and reliability of game task locations. Manzoor [**?**] proposed a location-aware mobile hunting game based on Hyperledger Fabric. Player-submitted hunting tasks are verified through smart contracts, publishing only reward information without revealing hunting details. Wallet functions ensure player rewards, with completed task information stored in Hyperledger, enhancing reward transparency and security for location-based games. However, IoT beacon detection latency is high, and hunting location safety cannot be guaranteed. Considering that some players cannot complete hunting tasks, Pittaras [**?**] developed a location-based mobile game interconnecting Ethereum and Hyperledger Fabric (v1.4) (since the original text did not describe Ethereum' s design, only Hyperledger-related design is shown in the figure). It developed advertising functions and used chaincode to count player ad views and automat-

ically distribute rewards.

3.4 Smart Fitness Domain

Smart fitness is a popular IoT scenario. It aims to obtain user training data through sensors and combine it with AI algorithms to provide intelligent training decisions, dietary supervision, behavior prediction, and other services. IoT-based smart fitness falls into three categories: fitness trackers (including wearable and non-wearable sensors), motion analysis, and fitness applications [**?**]. Currently, Hyperledger primarily addresses training model and decision security and enhances precise automation.

In Hyperledger-based fitness data systems, to provide more secure intelligent services, Jamil [**?**] proposed a Hyperledger Fabric (v1.2, Composer v1.13.0)-based fitness model. As shown in Fig. 19, machine learning implements a fitness data inference engine providing reasonable fitness and diet plans. The system compares inference knowledge thresholds with actual read data and updates inference information, improving fitness data security.

3.5 Smart City Monitoring Domain

Urban monitoring is crucial infrastructure in smart cities. IoT-based urban monitoring collects information through cameras to obtain real-time geospatial status and performs intelligent analysis and detection on this data.

In urban monitoring systems, the authenticity of user-provided monitoring information is a concern. Khan [**?**] proposed a Hyperledger Fabric (v1.4)-based monitoring information detection system. As shown in Fig. 20, endorsement nodes judge the importance of surveillance videos/images, and chaincode prioritizes detection of important information, extracting frames for comparison with original videos. This system ensures CCTV (Closed-Circuit Television Camera) data authenticity to some extent but has a single detection mechanism.

3.6 Smart Grid Domain

Smart grid is an advanced digital two-way power flow system with self-healing, adaptive, resilient, and sustainable capabilities that can predict uncertainties [**?**]. Smart grids require reliable, sustainable power supply [**?**], and secure two-way power transactions are crucial for ensuring sustainable supply. Security includes not only secure storage and transaction traceability but also reasonable privacy protection. Current Hyperledger research mainly focuses on solving power transactions, privacy protection, and energy load.

In Hyperledger-based smart grid systems, real-time scheduling strategies are important for power transactions. Zhao [**?**] established a Hyperledger Fabric (v1.1)-based microgrid market model. It uses multiple chaincodes for real-time power resource scheduling, storing transaction records on the Hyperledger blockchain. Transaction prices and volumes are determined based

on Bayesian-Nash equilibrium theory from incomplete information static games, effectively reducing power purchase costs but without guaranteeing systematic performance when handling large transaction volumes. Li [**?**] proposed a Hyperledger Fabric (v1.4.0)-based two-way power trading system. As shown in Fig. 21, it uses an iterative two-layer optimization-based charging/discharging strategy to formulate real-time scheduling for electric vehicles, with chaincode performing scheduling transactions and settlement. The hierarchical power dispatch structure improves system scalability.

Considering transaction stability, Li [**?**] proposed a power dispatch scheme (Fabric v1.4.0). As shown in Fig. 22, it uses an improved krill herd algorithm optimization model to formulate electric vehicle charging/discharging schedules, minimizing grid load variance and improving power transaction security and stability. In power transactions, reasonable bidding strategies aid power dispatch. Yu [**?**] proposed a Hyperledger Fabric-based power trading model. It uses an improved Bayesian bidding algorithm to provide users with optimal bidding strategies, including possible bid types, optimal bids, and opponent probability distributions. A three-layer structure (user layer, agent layer, and Hyperledger layer) ensures detailed transaction information is not obtained by agents or Hyperledger. To address supply chain imbalance caused by user over-scheduling, Lohachab [**?**] discussed a novel energy trading framework (Fabric v1.4.0, v1.4.1). It replaces centralized microgrid dispatch with Hyperledger real-time scheduling and designs reward and dispatch algorithms to encourage users to sell excess energy, maintain energy demand balance, and ensure each user's energy level stays between minimum and maximum requirements, improving energy utilization.

To ensure stability of energy transactions across different periods, Jamil [**?**] combined machine learning with Hyperledger Fabric (v1.2) to propose a smart power trading platform. As shown in Fig. 23, it collects customer information from physical networks, uses machine learning to analyze data features, and predicts short-term and long-term scheduling transactions, effectively ensuring network load but with single prediction indicators. To better alleviate network congestion during power system peak times, crowdsourcing tasks are effective solutions. Sciume [**?**] proposed an energy load response scheme (Fabric). It predicts next-day network load through data concentrators and crowdsources network load reduction tasks to users. Smart contracts evaluate each participant's actual load reduction capability based on baseline assessments and allocate corresponding reward tasks, effectively solving network congestion caused by peak power system loads. Regarding user privacy protection in smart power transactions, Wang [**?**] proposed an energy management system. It uses entity mapping protocol averaging combined with zero-knowledge proof authentication to separate user information and guarantee privacy.

3.7 Smart Transportation Domain

Smart transportation leverages AI potential to develop big data-driven smart traffic management solutions for effective decision-making [**?**], primarily refer-

ring to effectively avoiding or mitigating traffic congestion and accidents [**?**]. Making rapid and precise adjustments for high-mobility, high-dynamic traffic situations has become an urgent challenge. Currently, Hyperledger research in smart transportation covers multiple aspects, including automatic authentication, intersection control and monitoring, ETC (Electronic Toll Collection), air-land integrated authentication, and IoV data security.

In Hyperledger-based vehicle systems, Feng [**?**] proposed a Hyperledger Fabric (Fabric, Composer v0.20.7)-based automatic certified vehicle information system. As shown in Fig. 24, onboard units serve as unique vehicle identifiers, roadside units and onboard units perform real-time detection, and chaincode automatically authenticates vehicles. Vehicle identities are encrypted during authentication, improving privacy.

To address cross-domain identity authentication, Li [**?**] proposed a Hyperledger Fabric (v1.2, Ursa)-based vehicle location-aware system. As shown in Fig. 25, it uses the I-SIG system to obtain vehicle data, provides optimal signal schemes for intersections, uses Zero Knowledge Range Proofs (ZKPR) protocols to encrypt vehicle information, and verifies vehicle identity legitimacy through intelligent gateways, showing advantages in transaction delay, throughput, and success rates. Due to limited roadside unit monitoring ranges, some solutions combine aerial resources. Luo [**?**] proposed an air-land integrated vehicle cross-domain identity monitoring system (Indy). As shown in Fig. 26, it uses Universal Software Radio Peripheral (USRP) technology to provide vehicle identity features, uses drones for vehicle identity authentication, and employs adjacent drone cross-authentication to ensure drone identity legitimacy. Aerial nodes expand monitoring range but have high authentication latency.

To address intersection traffic safety, Buzachis [**?**] proposed a Hyperledger Fabric-based system for monitoring vehicles at intersections. Chaincode performs real-time trajectory simulation of vehicles, with endorsement nodes detecting simulation results. Tests of autonomous vehicles passing through 1-2 intersections prove system availability but lack design for multiple intersections. To address real-time assistance for vehicles in danger, Mbarek [**?**] proposed a multi-level endorsement vehicle communication system (Fabric). It uses a BF-DF-AF-IF (Belief function-Desire function-Analysis function-Intension function) model to refine vehicle needs into specific repair action requirements. It designs an endorsement level mechanism (automatically upgrading or downgrading endorsement levels based on transaction scores) where each transaction is endorsed by higher-level endorsement nodes, ensuring transaction reliability. This implements intelligent endorsement mechanisms and enhances endorsement efficiency but has incomplete scoring mechanisms.

For accident information authenticity in IoV, Xiao [**?**] proposed an IoV fake news detection model (Fabric). As shown in Fig. 27, it uses Bayesian algorithms to detect the probability of IoV message authenticity and stores it in Hyperledger, achieving load balancing and proving feasibility in prior probability, transaction processing speed, and accuracy. To timely obtain road condi-

tions and avoid traffic accidents, some research focuses on secure transactions in smart transportation. Gao [**?**] proposed a Hyperledger Fabric (v0.6)-based V2G (Vehicle-to-grid) payment model. It ensures privacy by allowing payers to create multiple accounts in the same transaction. Chiu [**?**] proposed a Hyperledger Fabric (v2.2)-based ETC system. Vehicles and ETC gates perform cross-authentication, with ETC gates detecting vehicle identity legitimacy and storing transaction records in Hyperledger, showing stability and high performance, though PBFT consensus is not suitable for large networks.

In toll systems, to address electronic identity issues, Viera [**?**] proposed a 5G-based C-V2X (Vehicle to Everything) road tolling system (Fabric). As shown in Fig. 29, it uses Indy' s portable identity technology, with smartphones sending identity information instead of roadside units. Phones process toll requests and store transaction records. This proposal first demonstrates the feasibility of combining 5G and Hyperledger in V2X systems. Lee [**?**] proposed an auction mechanism and fog computing-based traffic system (Fabric). As shown in Fig. 30, it uses fog computing to allocate public transportation resources and designs an auction mechanism to select the highest-bidding IoV users. This achieves reasonable public transportation resource allocation but uses a single winner selection method. Additionally, adjacent RSU nodes are assumed secure by default, reducing endorsement result credibility.

3.8 Smart Building Projects Domain

In this paper, smart building projects refer to the deep integration of building projects with cutting-edge IT technology to achieve real-time building modeling updates, transaction security, reduced delivery costs, and effective collaboration [**?**, **?**]. Current research mainly focuses on solving multi-party information exchange in construction projects.

To address building project information exchange issues, Suliyanti [**?**] proposed a Hyperledger Fabric (Fabric, Composer)-based system for multiple interested parties to exchange building information. As shown in Fig. 31, the system develops a building project bidding system and stores the entire building completion cycle in Hyperledger. It explores complete Building Information Modeling (BIM) information recording and exchange but is overly owner-centric, lacking proper supervision of owner selection. To address financial distribution in building projects, Elghaish [**?**] proposed a Hyperledger Fabric-based building information model system. As shown in Fig. 32, it uses smart contracts to check construction team financial distribution, allocating corresponding finances to each participant based on total profit, cost savings, and net amount of repaid costs. This scheme proves the feasibility of applying Hyperledger to Integrated Project Delivery (IPD) systems.

To address privacy issues across different building project ledgers, Yang [**?**] discussed a multi-channel design scheme (Fabric). As shown in Fig. 33, it uses smart contracts to enable communication between architects and suppliers, en-

gineers, clients, building surveyors, and urban planners, storing each link' s information in different channels. This research identifies unique advantages of Hyperledger-based building project systems in scalability, traceability, and auditability, and challenges in transaction processing efficiency, business changes, identity, costs, and smart contract security. To address incomplete building project information, Sheng [**?**] proposed a Hyperledger Fabric (v1.4)-based building project information management system. The system uses Hyperledger endorsement nodes to check building information authenticity, Orderer for transaction ordering, and Web queries for complete building project information, partially solving incompleteness and traceability issues.

3.9 Smart Energy Domain

Smart energy trading aims to enable autonomous energy regulation and effective energy utilization through consumers and enterprises selling surplus energy or purchasing needed energy. In this section, energy may refer to electricity or carbon emissions. Smart energy trading improves energy utilization and reduces manual errors and management costs. Hyperledger primarily addresses secure transactions and transaction integrity verification in smart energy trading.

To address secure scheduling of energy emissions, Yuan [**?**] proposed a Hyperledger Fabric (v1.1)-based energy emissions trading system. Nodes allocate emissions through specific channels, using smart contracts to store and review energy emissions transactions. To ensure legitimacy of energy emissions trading identities, Hu [**?**] proposed a distributed energy trading model (Fabric). Endorsement nodes verify enterprise identities and applied emissions, storing transaction information on-chain. To improve verification efficiency of energy emissions transactions, Che [**?**] proposed an on-chain and off-chain co-validation scheme for energy transactions (Fabric v1.1). As shown in Fig. 34, matching units package and verify a certain number of transactions, which are then reverified and stored by on-chain peers. To improve energy scheduling efficiency, Silva [**?**] proposed an electric vehicle energy bidding system using Hyperledger (Fabric, Composer). It designs electricity bidding and connects to local parking lot controllers for electricity dispatch. Using chaincode to complete electricity transactions offers good advantages in transaction integrity and transparency, but buyers are nearly centralized, with obvious supervision deficiencies.

4 Future Research Directions

As Hyperledger technology applications and research progress, IoT-Hyperledger integration has attracted widespread attention. Hyperledger addresses flexibility, robustness, and privacy limitations of other blockchain technologies, but Hyperledger-based IoT systems still have insufficiently researched and unresolved issues, mainly concentrated in performance and incentive mechanisms. This paper proposes four future directions:

a) **Low-power consensus algorithms.** Consensus algorithms are key de-

terminants of Hyperledger-based IoT system performance. Most IoT devices cannot fully meet the computational and energy requirements for processing large-scale consensus. Therefore, low-power consensus algorithms suitable for most IoT devices are an urgently important problem.

b) **Intelligent transaction verification.** Hyperledger' s "Endorse+Kafka+Commit" modes do not fully solve transaction verification performance issues. Existing transaction verification performance still cannot meet the demands of massive IoT device information exchange. Overly long response times from some verification nodes affect efficiency. Therefore, using intelligent clustering algorithms to screen currently active nodes for verification roles may solve this problem [**?**].

c) **On-chain/off-chain hybrid storage.** Hyperledger blocks are stored in nodes, which are typically IoT devices. Some devices have very low storage capacity and cannot store multiple blockchains. Integrating Hyperledger with distributed databases (such as IPFS) for on-chain/off-chain storage may alleviate device storage pressure.

d) **Custom incentive mechanisms.** Hyperledger does not advocate any cryptocurrency as rewards, but distributed task undertaking still requires incentive mechanisms as the main driving force. This study believes such incentive mechanisms can be customized, with developers focusing on consumer interest areas. For example, if consumers favor certain games or website membership services, they can choose these as task rewards. This incentive mechanism will improve collaboration efficiency and motivate users to better participate in collaboration.

5 Conclusion

Blockchain-based IoT systems have obvious deficiencies in scalability, flexibility, robustness, and privacy. To address these issues, Hyperledger is considered an ideal technology and has attracted widespread attention. This study summarizes Hyperledger research in IoT, demonstrating its feasibility and effectiveness in IoT applications. It aims to present more intuitive differences and design 思路 from a reconstructing diagrams perspective, providing researchers with rapid technology integration guidelines. Hyperledger technology can already satisfy multiple business scenarios, but exploration in the IoT domain remains in its preliminary stages. Additionally, the reconstructing diagrams survey method demonstrates unique advantages in visualizing business logic, technology convergence, and readability.

References

[1] Khan M A, Salah K. IoT security: Review, blockchain solutions, and open challenges [J]. Future Generation Computer Systems, 2018, 82: 395-411.

[2] Blummer T, Sean M, Cachin C. An introduction to hyperledger [J]. Hyperledger Organization: San Francisco, CA, USA, 2018. https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf

[3] Leng Zeqi, Tan Zhenjiang, Wang Kunhao. Application of Hyperledger in the Hospital Information Systems: A Survey [J]. IEEE Access, 2021, 9: 1-15.

[4] Keramidas G, Voros N, Hübner M. Components and Services for IoT Platforms [M]. Cham: Springer International Publishing, 2016.

[5] Olson K, Bowman M, Mitchell J, et al. Sawtooth: an introduction [J]. The Linux Foundation, Jan, 2018: 26. https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf

[6] Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises [J]. Business Horizons, 2015, 58(4): 431-440.

[7] Wang Haiyan, Zhang Jiawei. Blockchain based data integrity verification for large-scale IoT data [J]. IEEE Access, 2019, 7: 164996-165006.

[8] Yang Hui, Yuan Jiaqi, Yao Haipeng, et al. Blockchain-based hierarchical trust networking for JointCloud [J]. IEEE Internet of Things Journal, 2019, 7(3): 1667-1677.

[9] Dib O, Huyart C, Toumi K. A novel data exploitation framework based on blockchain [J]. Pervasive and Mobile Computing, 2020, 61: 101104.

[10] Yu Jingang, Zhang Hong, Li Shu, Mao Lishuang, Ji Pengxiang. Data Sharing Model for Internet of Things Based on Blockchain [J]. Journal of Chinese Computer Systems, 2019, 40(11): 2324-2329.

[11] Cao Yan, Jia Feng, Manogaran G. Efficient traceability systems of steel products using blockchain-based industrial Internet of Things [J]. IEEE Transactions on Industrial Informatics, 2019, 16(9): 6004-6012.

[12] Zhang Sen, Ye Jian, Li Guogang. Research and Implementation of Blockchain Technology Scheme for Cold Chain Logistics [J]. Computer Engineering and Applications, 2020, 56(03): 19-27.

[13] Seshadri S S, Rodriguez D, Subedi M, et al. IoTcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems [J]. IEEE Internet of Things Journal, 2020, 8(5): 3346-3359.

[14] Kim J H, Lee S, Hong S. Autonomous Operation Control of IoT Blockchain Networks [J]. Electronics, 2021, 10(2): 204.

[15] Košťál K, Helebrandt P, Belluš M, et al. Management and monitoring of IoT devices using blockchain [J]. Sensors, 2019, 19(4): 856.

[16] Mbarek B, Jabeur N, Pitner T. Mbs: Multilevel blockchain system for IoT [J]. Personal and Ubiquitous Computing, 2019: 1-8.

[17] Ribeiro V, Holanda R, Ramos A, et al. Enhancing key management in LoRaWAN with permissioned blockchain [J]. Sensors, 2020, 20(11): 3156.

[18] Hang Lei, Kim D H. Design and implementation of an integrated IoT blockchain platform for sensing data integrity [J]. Sensors, 2019, 19(10): 2345.

[19] Liu Han, Han Dezhi, Li Dun. Fabric-IoT: A blockchain-based access control system in IoT [J]. IEEE Access, 2020, 8: 18207-18218.

[20] Zhang Yu, Liu Wenfeng, Xia Zhongda, et al. Blockchain-Based DNS Root Zone Management Decentralization for Internet of Things [J]. Wireless Communications and Mobile Computing, 2021, 2021: 1-15.

[21] Chi Jiancheng, Li Yu, Huang Jing, et al. A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things [J]. Journal of Network and Computer Applications, 2020, 167: 102710.

[22] Yu Donghua, Liu Guojun, Guo Maozu, et al. An improved K-medoids algorithm based on step increasing and optimizing medoids [J]. Expert Systems with Applications, 2018, 92: 464-473.

[23] Fauzi M A, Utomo D C, Setiawan B D, et al. Automatic essay scoring system using n-gram and cosine similarity for gamification based e-learning [C]. Proceedings of the International Conference on Advances in Image Processing, 2017: 151-155.

[24] Zhang Jianghui, Cui Bo, Li Ru, Shi Jinshan. Access Control System of Internet of Things Based on Smart Contract [J]. Computer Engineering, 2021, 47(04): 21-31.

[25] Siris V A, Dimopoulos D, Fotiou N, et al. Decentralized authorization in constrained IoT environments exploiting interledger mechanisms [J]. Computer Communications, 2020, 152: 243-251.

[26] Kakei S, Shiraishi Y, Mohri M, et al. Cross-certification towards distributed authentication infrastructure: A case of hyperledger fabric [J]. IEEE Access, 2020, 8: 135742-135757.

[27] Honar Pajooh H, Rashid M, Alam F, et al. Multi-layer blockchain-based security architecture for internet of things [J]. Sensors, 2021, 21(3): 772.

[28] Zhou Lijing, Wang Licheng, Ai Tianyi, et al. BeeKeeper 2.0: confidential blockchain-enabled IoT system with fully homomorphic computation [J]. Sensors, 2018, 18(11): 3785.

[29] Hou Lu, Zheng Kan, Liu Zhiming, et al. Design and prototype implementation of a blockchain-enabled LoRa system with edge computing [J]. IEEE Internet of Things Journal, 2020, 8(4): 2419-2430.

[30] Yang Xinting, Zhang Song, Liu Jintao, et al. Deep learning for smart fish farming: applications, opportunities and challenges [J]. Reviews in Aquaculture, 2021, 13(1): 66-90.

[31] Feng Yunhe, Niu Haoran, Wang Fanqi, et al. SocialCattle: IoT-based Mastitis Detection and Control through Social Cattle Behavior Sensing in Smart Farms [J]. IEEE Internet of Things Journal, 2021.

[32] Hang Lei, Ullah I, Kim D H. A secure fish farm platform based on blockchain for agriculture data integrity [J]. Computers and Electronics in Agriculture, 2020, 170: 105251.

[33] Lee S, Lee J, Hong S, et al. Lightweight end-to-end blockchain for IoT applications [J]. KSII Transactions on Internet and Information Systems (TIIS), 2020, 14(8): 3224-3242.

[34] Yi Weiguo, He Jianguo, Liu Guishan, Kang Ningbo. Development and Implementation of Blockchain to Enhance Traceability and Reliability of Fruit and Vegetable Quality [J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(02): 309-315+345.

[35] Kara N, Cagiltay K. Smart toys for preschool children: A design and development research [J]. Electronic Commerce Research and Applications, 2020, 39: 100909.

[36] Yang Jian, Lu Zhihui, Wu Jie. Smart-toy-edge-computing-oriented data exchange based on blockchain [J]. Journal of Systems Architecture, 2018, 87: 36-48.

[37] Manzoor A, Samarin M, Mason D, et al. Scavenger Hunt: Utilization of Blockchain and IoT for a location-based Game [J]. IEEE Access, 2020, 8: 204863-204879.

[38] Pittaras I, Fotiou N, Siris V A, et al. Beacons and blockchains in the mobile gaming ecosystem: A feasibility analysis [J]. Sensors, 2021, 21(3): 862.

[39] Farrokhi A, Farahbakhsh R, Rezazadeh J, et al. Application of Internet of Things and artificial intelligence for smart fitness: A survey [J]. Computer Networks, 2021: 107859.

[40] Jamil F, Iqbal N, Ahmad S, et al. Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid [J]. IEEE Access, 2021, 9: 39193-39217.

[41] Khan P W, Byun Y C, Park N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities [J]. Electronics, 2020, 9(3): 484.

[42] Dileep G. A survey on smart grid technologies and applications [J]. Renewable Energy, 2020, 146: 2589-2625.

[43] Li Fangxin, Qiao Wei, Sun Hongbin, et al. Smart transmission grid: Vision and framework [J]. IEEE Transactions on Smart Grid, 2010, 1(2): 168-177.

[44] Zhao Wenting, Lv Jun, Yao Xilong, et al. Consortium Blockchain-Based microgrid market transaction research [J]. Energies, 2019, 12(20): 3812.

[45] Li Y, Hu B. An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain [J]. IEEE Transactions on Smart Grid, 2019, 11(3): 2627-2637.

[46] Li Yuancheng, Hu Baiji. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles [J]. IEEE Transactions on Industrial Informatics, 2020, 17(3): 1968-1977.

[47] Yu Yunjun, Guo Yanghui, Min Wwendong, et al. Trusted transactions in micro-grid based on blockchain [J]. Energies, 2019, 12(10): 1952.

[48] Lohachab A, Garg S, Kang B H, et al. Performance evaluation of Hyperledger Fabric-enabled framework for pervasive peer-to-peer energy trading in smart Cyber–Physical Systems [J]. Future Generation Computer Systems, 2021, 118: 392-416.

[49] Jamil F, Kahng H K, Kim S, et al. Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms [J]. Sensors, 2021, 21(5): 1640.

[50] Sciumè G, Palacios-Garcia E J, Gallo P, et al. Demand response service certification and customer baseline evaluation using blockchain technology [J]. IEEE Access, 2020, 8: 139313-139331.

[51] Wang Lognze, Jiao Shucen, Xie Yu, et al. A Permissioned Blockchain-Based Energy Management System for Renewable Energy Microgrids [J]. Sustainability, 2021, 13(3): 1317.

[52] Nallaperuma D, Nawaratne R, Bandaragoda T, et al. Online incremental machine learning platform for big data-driven smart traffic management [J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(12): 4679-4690.

[53] Djahel S, Doolan R, Muntean G M, et al. A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches [J]. IEEE Communications Surveys & Tutorials, 2014, 17(1): 125-151.

[54] Feng Qi, He Debiao, Zeadally S, et al. BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks [J]. IEEE Transactions on Industrial Informatics, 2019, 16(6): 4146-4155.

[55] Li Wanxin, Guo Hao, Nejad M, et al. Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach [J]. IEEE Access, 2020, 8: 181733-181743.

[56] Luo Gege, Shi Mingxian, Zhao Caidan, et al. Hash-Chain-Based Cross-Regional Safety Authentication for Space-Air-Ground Integrated VANETs [J]. Applied Sciences, 2020, 10(12): 4206.

[57] Buzachis A, Celesti A, Galletta A, et al. A multi-agent autonomous intersection management (MA-AIM) system for smart cities leveraging edge-of-things and Blockchain [J]. Information Sciences, 2020, 522: 15-35.

[58] Mbarek B, Jabeur N, Pitner T, et al. Empowering communications in vehicular networks with an intelligent blockchain-based solution [J]. Sustainability, 2020, 12(19): 7917.

[59] Xiao Yonggang, Liu Yanbing, Li Tun. Edge computing and blockchain for quick fake news detection in IoV [J]. Sensors, 2020, 20(16): 4360.

[60] Chen Wuhui, Chen Yufei, Chen Xu, et al. Toward secure data sharing for the IoV: a quality-driven incentive mechanism with on-chain and off-chain guarantees [J]. IEEE Internet of Things Journal, 2019, 7(3): 1625-1638.

[61] Gao Feng, Zhu Liehuang, Shen Meng, et al. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks [J]. IEEE Network, 2018, 32(6): 184-192.

[62] Chiu Weiyang, Meng Weizhi. EdgeTC-a PBFT blockchain-based ETC scheme for smart cities [J]. Peer-to-Peer Networking and Applications, 2021: 1-13.

[63] Bartolomeu P C, Vieira E, Ferreira J. Pay as You Go: A Generic Crypto Tolling Architecture [J]. IEEE Access, 2020, 8: 196212-196222.

[64] Lee Y, Jeong S, Masood A, et al. Trustful Resource Management for Service Allocation in Fog-Enabled Intelligent Transportation Systems [J]. IEEE Access, 2020, 8: 147313-147322.

[65] Lee D, Lee S H, Masoud N, et al. Integrated digital twin and blockchain framework to support accountable information sharing in construction projects [J]. Automation in Construction, 2021, 127: 103688.

[66] Haaskjold H, Andersen B, Langlo J A. Dissecting the project anatomy: Understanding the cost of managing construction projects [J]. Production Planning & Control, 2021: 1-22.

[67] Suliyanti W N, Sari R F. Blockchain-Based Implementation of Building Information Modeling Information Using Hyperledger Composer [J]. Sustainability, 2021, 13(1): 321.

[68] Elghaish F, Abrishami S, Hosseini M R. Integrated project delivery with blockchain: An automated financial system [J]. Automation in Construction, 2020, 114: 103182.

[69] Yang R, Wakefield R, Lyu S, et al. Public and private blockchain in construction business process and information integration [J]. Automation in Construction, 2020, 118: 103276.

[70] Sheng Da, Ding Lieyun, Zhong Botao, et al. Construction quality information management with blockchains [J]. Automation in Construction, 2020, 120:

103373.

[71] Yuan Pu, Xiong Xiong, Lei Lei, et al. Design and implementation on hyperledger-based emission trading system [J]. IEEE Access, 2018, 7: 1-10.

[72] Hu Zhou, Du Yuhao, Rao Congjun, et al. Delegated Proof of Reputation Consensus Mechanism for Blockchain-Enabled Distributed Carbon Emission Trading System [J]. IEEE Access, 2020, 8: 214932-214944.

[73] Che Zheng, Wang Yu, Zhao Juanjuan, et al. A distributed energy trading authentication mechanism based on a consortium blockchain [J]. Energies, 2019, 12(15): 2878.

[74] Silva F C, A Ahmed M, Martínez J M, et al. Design and implementation of a blockchain-based energy trading platform for electric vehicles in smart campus parking lots [J]. Energies, 2019, 12(24): 4814.

Note: Figure translations are in progress. See original paper for figures.