Blockchain in the Digital Twin Context: A Comprehensive Survey

DUN LI*, Shanghai Maritime University, China
DEZHI HAN, Shanghai Maritime University, China
NOEL CRESPI, Samovar, Telecom SudParis, Institut Polytechnique de Paris, France
ROBERTO MINERVA, Samovar, Telecom SudParis, Institut Polytechnique de Paris, France
SYED MOHSAN RAZA, Samovar, Telecom SudParis, Institut Polytechnique de Paris, France
REZA FARAHBAKHSH, Samovar, Telecom SudParis, Institut Polytechnique de Paris, France
WEI LIANG, Hunan University of Science and Technology, China
ZIBIN ZHENG, Sun Yat-sen University, China

Digital twin (DT) technology integrates Internet of Things (IoT), communication networks, and sensor systems through high-fidelity modeling and multi-dimensional simulation, enabling dynamic mapping and real-time optimization of physical objects. However, DT development still faces several challenges, including cross-platform interoperability limitations, excessive latency in real-time scenarios, security vulnerabilities in distributed deployments, and the complexity of accurately modeling multi-modal systems. Blockchain (BC) enhances the security and functional scope of DTs across diverse applications. This survey begins by introducing the core principles of BC and DT, and then investigates the rationale and benefits behind their integration. From a data-centric perspective, we explore how Blockchain-empowered Digital Twins (BCDTs) enhance data storage, secure exchange, privacy protection, and system interoperability. The survey further explores the architecture of BCDT systems, covering network topology, functional modules, platform design, and representative prototypes, offering insights into real-world applications. In addition, we survey how BCDT supports the convergence of key Industry 4.0 technologies, including the Internet of Things, vehicle networks, unmanned aerial systems, artificial intelligence, federated learning, 5G mobile networks, and software-defined networking. Industrial-grade quality BCDT-supported applications are highlighted, providing a solid foundation for further research. Finally, we analyze the challenges faced by BCDT and offer some optimistic suggestions for further research in the field of BCDT.

CCS Concepts: • **Networks** → **Network security**; • **Information systems** → **Blockchain**; • **Computer systems organization** → *Embedded and Cyber-physical system*; • **Computing methodologies** → *Modeling and simulation*; • **Applied computing** → *Digital twins*; • **Software and its engineering** → *Software reliability*.

Additional Key Words and Phrases: Blockchain; Digital twin; Smart contract; Industry 4.0; Industrial applications.

---

*Corresponding author: Dun Li (lidunshmtu@outlook.com)

Authors' addresses: Dun Li, Shanghai Maritime University, Shanghai, China, lidunshmtu@outlook.com; Dezhi Han, Shanghai Maritime University, Shanghai, China, dzhan@shmtu.edu.cn; Noel Crespi, Samovar, Telecom SudParis, Institut Polytechnique de Paris, Palaiseau, France, noel.crespi@mines-telecom.fr; Roberto Minerva, Samovar, Telecom SudParis, Institut Polytechnique de Paris, Palaiseau, France, roberto.minerva@telecom-sudparis.eu; Syed Mohsan Raza, Samovar, Telecom SudParis, Institut Polytechnique de Paris, Palaiseau, France, syed-mohsan_raza@telecom-sudparis.eu; Reza Farahbakhsh, Samovar, Telecom SudParis, Institut Polytechnique de Paris, Palaiseau, France, reza.farahbakhsh@telecom-sudparis.eu; Wei Liang, Hunan University of Science and Technology, Xiangtan, China, wliang@hnust.edu.cn; Zibin Zheng, Sun Yat-sen University, Guangzhou, China, zhzibin@mail.sysu.edu.cn.

0360-0300/2025/3-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

ACM Reference Format:
Dun Li, Dezhi Han, Noel Crespi, Roberto Minerva, Syed Mohsan Raza, Reza Farahbakhsh, Wei Liang, and Zibin Zheng. 2025. Blockchain in the Digital Twin Context: A Comprehensive Survey. *ACM Comput. Surv.* , (March 2025), 34 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The Fourth Industrial Revolution (Industry 4.0) is redefining modern industrial practices by combining traditional manufacturing with advanced digital technologies, driving greater intelligence and automation [37, 98]. Industry 4.0 promises the next generation of production models that can support the increasing demand for customized, personalized, and service-oriented products at lower costs and higher quality [3]. Fundamentally, this revolution is triggered by a convergence of cutting-edge concepts and technologies, including cloud computing, mobile computing, Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR) [165], Cyber-Physical System (CPS), robotics, the Internet of Things (IoT), big data, Digital Twin (DT), Blockchain (BC), and additive manufacturing. As manufacturing becomes increasingly digitized, the industry is shifting from scale-based to scope-based economies [91, 146]. To close the gap between data and assets, the fusion of physical and digital systems is vital—enabling more sustainable, intelligent, and resilient industrial ecosystems [201].

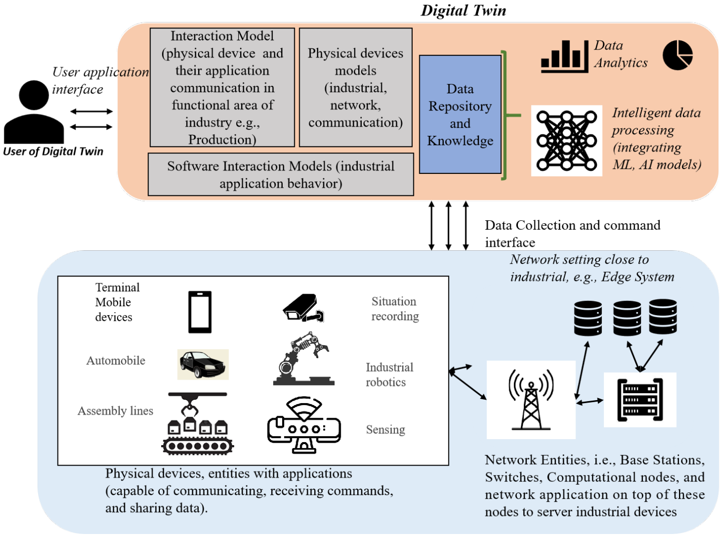

Fig. 1. A simple illustration of DT in Industry 4.0

In this context, the concept of the DT, which refers to the creation of a Digital Object (DO) that precisely reflects a Physical Object (PO), has gained growing attention across academic and industrial domains [178]. Fig. 1 presents an abstract relationship of the industrial system and DT. DT collects data from machines, sensors, networks, and computing units either directly or through existing applications, achieving bidirectional synchronization with physical systems through real-time data processing, modeling, and simulation. By incorporating both real-time and historical data, a DT enables predictive analytics and proactive resource coordination, supporting informed decision-making [102, 118]. High-fidelity simulation further allows operators to assess alternative strategies prior to physical implementation. However, realizing real-time, secure integration with physical assets remains challenging, as DTs face six core technical issues.

- **Interoperability**: DTs lack standardized representations for individual and collaborative components in industrial systems. Variations in modeling methods, interfaces, and architectures hinder cross-system interoperability [2, 80]. As DTs operate in AI-driven and security-critical domains, interoperability must also ensure explainability and trusted automation [154].
- **Programmability**: Proactive DTs must dynamically collect and process data, requiring programmability beyond passive mirroring. APIs and configurable parameters enable behavior modification, data source discovery, and adaptation to evolving scenarios [40, 183].
- **Modeling Complexity**: Modeling POs, context, and scenarios at scale remains challenging, particularly across distributed nodes [71]. Effective DT models must integrate structural dynamics, behaviors, and system interactions, often under resource and latency constraints [199].
- **Responsiveness**: DTs must sense, analyze, coordinate, and act with temporal precision [131]. Real-time responsiveness relies on adaptive, autonomous, and context-aware mechanisms, increasingly vital in Industry 4.0 environments [17].
- **Data security**: As web-based DTs scale into complex ecosystems, the volume of collected data increases rapidly [6]. The rise of AI-driven DTs heightens concerns over data security and privacy [149], especially as user interactions risk exposing personal information without robust safeguards [111].
- **Authorization and access control**: Allocating access rights in DT systems is challenging due to multiple stakeholders and interconnected components [106]. Without well-defined policies, redundant responsibilities and inconsistent privileges may cause security vulnerabilities and operational inefficiencies [162].

Interestingly, the features of BC technology, such as data security, trustworthiness, traceability, programmability, and scalability, position it as a strong complement to the limitations of existing DT frameworks [41, 58, 59, 95, 139]. In more detail, the proposed Blockchain-based Digital Twin (BCDT) paradigm ensures the secure execution of large-scale DT applications across distributed environments or multiple administrative domains by incorporating BC signature verification. In addition, smart contracts are designed as tamper-resistant code deployed in BC, triggered by transactions or external events and executed deterministically across the network [90]. In the BCDT framework, core operations such as entity registration, twin instantiation, permission control, and update verification can be encoded into smart contracts, ensuring transparency and auditability between stakeholders. This paper aims to provide a comprehensive study of BCDT, highlighting its architectural patterns, application domains, and technical challenges.

1.1 Existing Surveys and Tutorials

Several surveys have examined the integration of BC and DT, focusing on applications in supply chain [100], smart manufacturing [168, 203], digital identity and sovereignty [176], product lifecycle [143], access control [129], IIoT fault diagnostics [167], and intelligent transportation systems [151]. Some studies further explore interdisciplinary extensions, such as applications in biology [45], additive manufacturing [56], and data governance frameworks. Meanwhile, foundational work on the development of the DT [15, 49, 86, 145] and BC architecture [16, 196, 212, 214] has supported this growing body of research. Although these efforts offer valuable insights, most focus on specific domains or functions, few provide a unified architectural abstraction or examine the integration of BCDT from a holistic perspective of the lifecycle. This survey addresses these gaps by introducing a layered framework that maps BC functionalities such as identity management, consensus mechanisms, provenance tracking, and smart contracts to key stages of the DT lifecycle, while also examining how BCDT synergizes with next-generation technologies to enable scalable, secure, and intelligent systems. Table 1 summarizes the focus and limitations of representative surveys and situates our work in relation to the existing literature.

Table 1. Comparison of representative BCDT-related surveys

Ref.	**Focus Area**	**Perspective**	**Scope Beyond Applications**	**Key Notes**
[100]	Supply Chain	Application-driven	No lifecycle or multi-tech view	Data sharing in BCDT logistics
[45]	Interdisciplinary (Biology)	Conceptual proposal	No	Domain extension encouragement
[176]	Digital Identity, SSI	Governance	No	BC for sovereignty and regulation
[143]	Product Lifecycle	Ownership	Partial lifecycle	Copyright and traceability
[129]	Access Control	Security-focused	No	Legal DT authentication
[203]	Manufacturing	Compliance	Partial	Traceability without architecture
[168]	Industrial Production	Synchronization	Partial	Fusion and anomaly detection
[167]	IIoT Fault Detection	Reliability	Partial	Recommends open-source support
[151]	Transport Systems	Domain-specific	No	Only covers ITS use cases
[184]	Generic BCDT	Framework-level	Partial, some integration	Blending with other techniques
[56]	Additive MFG	Social impact	No	Custom production scenarios
This Work	Multi-domain (IoT, FL, 6G)	Lifecycle-centric architecture	**Yes**	DT lifecycle + cross-tech integration

1.2 Our Contributions

This survey addresses that gap by examining BCDT-related studies from 2018 to 2025, covering data services, prototypes, technology convergence, industrial applications, challenges, and future directions. Regarding earlier works, our objectives are to (i) present a theoretical overview of DT and BC technology, (ii) provide a systematic examination of the possibility of integrating BC into DT, (iii)outline BCDT in the context of other significant technologies, and (iv) thoroughly investigate the specific applications of BCDT. Specifically, the main contributions of this study are summarized as follows.

- This survey gives an outline of the concept of BC and DT convergence as well as its architectural design and platform deployment.
- We propose a generic BCDT topology and investigate the main available prototypes of BCDT.
- In this survey, we present an organized review of the research aimed at enhancing overall performance by combining BCDT with other technologies.
- The BCDT implementations currently available for industrial applications are described in detail.

1.3 The Survey Organization

This survey is organized as shown in Fig. 2. We first introduce the background and fundamentals of DT and BC in Section 2. Section 3 then describes the role of BC for DT from a data perspective. The converging framework and installation platform of BCDT are then presented in Section 4. Section 5 then summarizes the integration and improvement of BCDT with other technologies. Section 6 next summarizes the feasible application of BCDT. The research challenges and future directions of BCDT are discussed in Section 7. Finally, Section 8 concludes the paper.

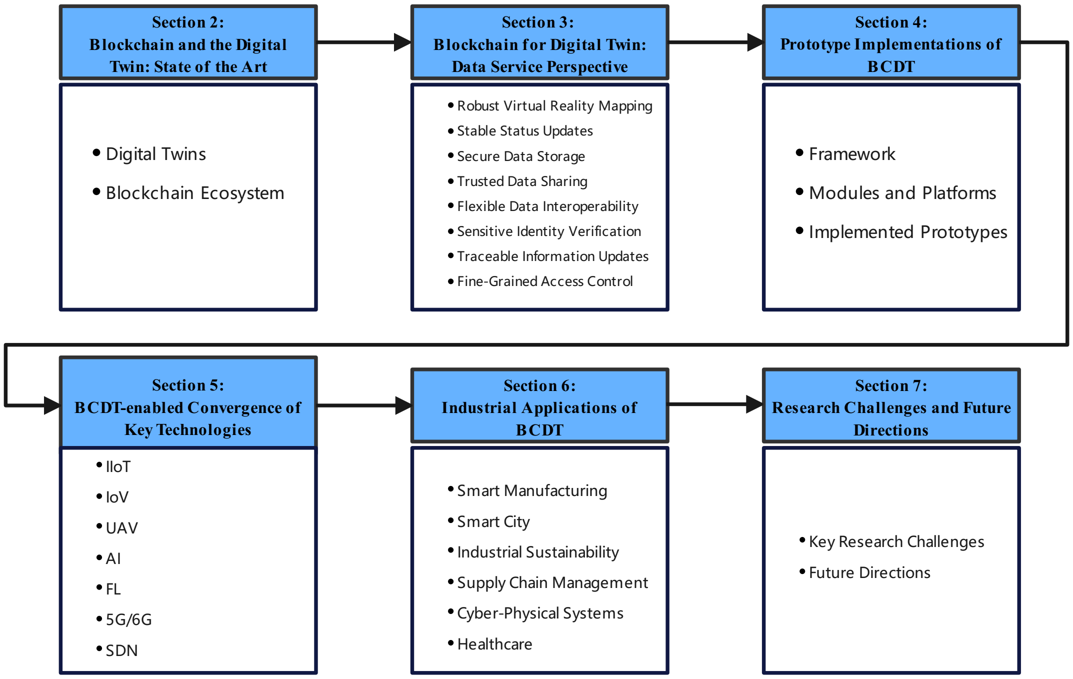

Fig. 2. Structure of the survey

2 BLOCKCHAIN AND THE DIGITAL TWIN: STATE OF THE ART

In this section, we briefly introduce DT integration in Subsection 2.1 and BC ecosystem in Subsection 2.2. Table 2 highlights a list of acronyms and the definitions used in this survey.

2.1 Digital Twin

2.1.1 Concept and Definition. DTs have been widely explored due to the increasing relevance in industrial and digital ecosystems. The evolution of DT, from its origin in the Apollo 13 mission [15] to its application in Industry 4.0 and smart manufacturing, is documented in several surveys [49, 86, 121, 153]. As software-based representations of POs, DTs mirror their real-world counterparts by encapsulating dynamic attributes and interactions. Through API integration, external applications can access real-time PO data for analysis and decision-making without altering the physical system, thus improving safety and modularity. Core DT features include contextual modeling, real-time reflection, and interface entanglement, enabling the representation of diverse operational states of the PO, supporting applications from anomaly detection to process optimization [117].

2.1.2 DT Origin. The concept of the DT was formally proposed by Professor Michael Grieves in the early 2000s within the framework of Product Lifecycle Management (PLM) [55]. However, its practical origin can be traced back to NASA's Apollo program, where engineers used physical replicas on Earth to simulate and monitor spacecraft conditions during missions [52]. NASA later popularized the term "Digital Twin" in its 2010 roadmap, defining it as a multiphysics, multiscale simulation model continuously synchronized with real-time operational

Table 2. The summary of acronyms & definitions

Acronym	**Definition**
BC	Blockchain
DT	Digital Twin
IoT	Internet of Things
IIoT	Industrial Internet of Things
BCDT	Blockchain-based Digital Twin Paradigm
Industry 4.0	The Fourth Industrial Revolution
IoV	Internet of Vehicles
UAV	Unmanned Aerial Vehicle
AI	Artificial Intelligence
FL	Federated Learning
5G	Fifth Generation Mobile Communications
6G	Sixth Generation Mobile Communications
SDN	Software-Defined Networking
VR	Virtual Reality
AR	Augmented Reality
MR	Mixed Reality
CPS	Cyber-Physical System
PO	Physical Object
DO	Digital Object
APIs	Application Programming Interfaces
HTTP	Hypertext Transfer Protocol
P2P	Peer-to-Peer
IPFS	InterPlanetary File System
PoW	Proof of Work
DAOs	Decentralized Autonomous Organizations
NFTs	Non-Fungible Tokens
ABAC	Attribute-based Access Control
RBAC	Role-based Access Control
RSUs	Roadside Units
ML	Machine Learning
DRL	Deep Reinforcement Learning
DL	Deep Learning
mPBFT	Modified Practical Byzantine Fault Tolerance
SMEs	Small and Medium-sized Enterprises
DApps	Decentralized Applications

data [160]. Tao et al. [178] further emphasized that DTs differ from traditional digital models by enabling real-time, bidirectional data exchange and persistent synchronization with their corresponding POs.

2.1.3 DT Modeling and Platforms. The architectural evolution of DT modeling frameworks demonstrates a paradigm shift toward cross-domain adaptability, with contemporary platforms embedding ontological specification frameworks to bridge physical-digital semantics [136]. Microsoft Azure Digital Twins [12] serves as a representative implementation of a cloud-native PaaS ecosystem structured around domain-specific knowledge graphs. Upon instantiation of the model, the Azure runtime environment enables bidirectional synchronization between DT instances and physical assets through integration of the IoT Hub, supporting real-time state mirroring through configurable data pipelines. In addition, Siemens MindSphere [159] focuses on the integration of IIoT, offering cloud-based DT services for the manufacturing, energy, and infrastructure sectors [138]. Bentley's iTwin platform [21] specializes in infrastructure-oriented DTs, enabling synchronized engineering data management for assets such as railways, bridges, and pipelines. NVIDIA Omniverse [130] empowers the creation of high-fidelity, real-time 3D DTs, combining AI-driven simulation with photorealistic visualization.

2.1.4 DT Characteristics and Requirements. DTs are characterized by fundamental properties that enable dynamic interaction with POs across various application contexts [119]. Contextualization ensures each DT captures only the relevant attributes of its PO. Reflection and replication enable timely synchronization and digital mirroring of physical states, while entanglement supports real-time bidirectional interaction between the virtual and physical domains. Persistency maintains functionality even when the PO is offline, and memorization preserves operational history for learning and prediction. Other key properties include composability for integrating subsystems, accountability for ensuring resilience under PO failures, and augmentation for extending functionalities beyond the original object. Ownership defines data usage rights, whereas servitization transforms DT functions into service-oriented offerings via APIs. Predictability leverages historical and contextual data—often through AI or ML models—to anticipate system behaviors [117, 178]. A software-based abstraction of these DT characteristics is shown in Fig. 3.

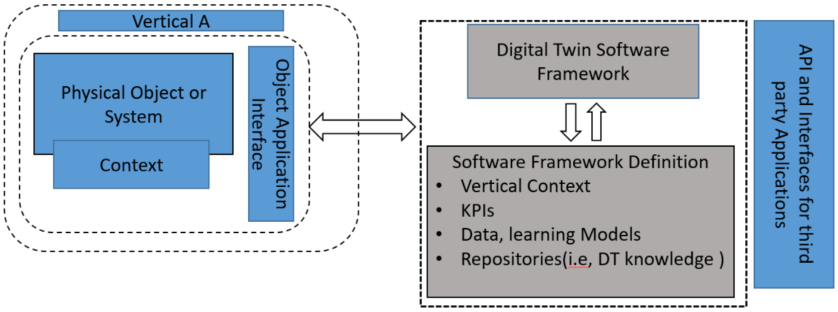

Fig. 3. DT as software framework

2.2 Blockchain Ecosystem

The concept of BC was introduced by Satoshi Nakamoto in 2008 [125]. BC is a distributed ledger technology built on a Peer-to-Peer (P2P) network that records transactions across multiple nodes without relying on a central authority. By combining asymmetric cryptography with distributed consensus, BC enables secure, tamper-resistant, and transparent data sharing.

2.2.1 Blockchain Structure. BC is a decentralized, append-only ledger that ensures verifiable and tamper-evident data storage across mutually untrusted nodes [174]. In distributed systems, any data modification must be approved through network-wide consensus, which effectively prevents unauthorized alterations. Each block contains a group of transactions, typically organized by arrival time or transaction fee, and is appended sequentially to the chain. Transaction integrity is maintained by computing cryptographic hash values that are aggregated into a Merkle root. Any change in the transaction set results in a different root, enabling immediate detection of inconsistencies. The first block in the chain, known as the genesis block, has no predecessor [161]. Each subsequent block includes metadata such as the timestamp, nonce, and hash of the previous block, ensuring continuity and traceability throughout the ledger. The blockchain grows from the genesis block as shown in Eq. 1.

$$Genesis \xrightarrow{ctgen} \{Block_1, Block_2, \cdots Block_n\} \tag{1}$$

The block body stores the majority of data, including verified transactions and optional smart contracts [126]. For example, in Bitcoin, a block can be up to 1 MB in size, while a typical transaction is around 250 bytes, allowing approximately 4,000 transactions per block. However, these values are platform-specific and not standardized across all BCs. In permissioned systems such as Hyperledger Fabric, block and transaction sizes are configurable according to system requirements.

2.2.2 *Blockchain Network.*

In BC networks, nodes function as autonomous and decentralized components, maintaining equality across the system. New nodes can join or existing ones can leave without disrupting network operations [96]. Each node continuously monitors the network for broadcasted messages and validates newly received transactions or blocks from neighboring nodes upon arrival. Digital signatures, work proofs, hash values, blocks, and smart contracts are all included in the communication [64]. To prevent the creation of erroneous data entries, the message is encrypted and posted to the BC only when information verification has gained consensus.

2.2.3 *Blockchain Encryption.*

BC systems operate within peer-to-peer (P2P) networks, where each node generates a public–private key pair for identity authentication and message signing [34]. The private key is securely held by the node, while the corresponding public key is shared to allow other nodes to verify digital signatures. Asymmetric cryptography is commonly employed in public and consortium BCs to ensure transaction integrity [88]. When initiating a transaction, a node signs the data with its private key and broadcasts it to the network, where it is validated by other participants.In contrast, permissioned BCs may adopt symmetric encryption or application-specific identity management mechanisms to meet the performance and security requirements of controlled environments [209].

2.2.4 *Consensus.*

In BC systems, consensus protocols ensure that all distributed nodes maintain a consistent view of the ledger without relying on any central authority, using fault-tolerant mechanisms to preserve data integrity [22]. Proof of Work (PoW), one of the earliest and most widely adopted mechanisms, requires participants to solve computational puzzles to validate transactions and generate new blocks. To maintain a stable average block interval of about ten minutes, the mining difficulty is periodically adjusted according to the network's overall computational power [193]. The new difficulty D is calculated as Eq. 2.

$$D = D_{prev} \cdot \frac{2016 \times 10 \text{ minutes}}{t_{actual}} \tag{2}$$

where t_{actual} denotes the actual time required to mine the previous 2,016 blocks, and D_{prev} represents the previous difficulty. The adjustment factor is constrained within a fourfold range to prevent abrupt fluctuations in network difficulty. If the previous 2,016 blocks are mined in less than two weeks (20,160 minutes), the reduced t_{actual} indicates higher network computing power, resulting in an increase in the PoW difficulty; conversely, if blocks are produced more slowly, the difficulty is reduced to maintain the target interval.

2.2.5 *Transaction and Ledger.*

Transactions represent the fundamental data units recorded in BC. In many public BC platforms, a user typically includes a transaction fee to incentivize miners or validators to include the transaction in a newly created block [89]. Miners are responsible for collecting and validating transactions, which are then packaged into blocks. Each block may contain zero or more transactions, depending on network activity and block size constraints. Any remaining balance not explicitly assigned within a transaction can be interpreted as a transaction fee, as shown in Eq. 3.

$$Inputs - outputs = Transaction_{fees} \tag{3}$$

The ledger consists of a state database that maintains the most recent state, and a BC that stores immutable chronologically ordered blocks. Each transaction creates or modifies a set of key-value pairs representing assets, which are then reflected in the ledger [44]. In some implementations, new blocks are appended periodically, even if empty, to preserve consensus and ensure system liveness. It is worth noting that not all BC systems impose transaction fees. For example, permissioned BCs such as Hyperledger Fabric do not require fees for transaction processing, as participants are pre-authorized and incentivization mechanisms differ from those in public chains. Since each previous transaction is reflected in the hash of the most recent block, all nodes are guaranteed to be in a consistent and stable state.

2.2.6 *Smart Contract.*

BC 1.0 began with cryptocurrency systems like Bitcoin [125], while BC 2.0 introduced smart contracts [25, 81], enabling decentralized computation platforms such as Ethereum and paving the way for Decentralized Autonomous Organizations (DAOs). Tools such as Remix support the development and deployment of Solidity-based contracts [213]. Smart contracts serve as the foundational mechanism for implementing Decentralized Applications (DApps) and custom business process logic [216]. Public networks like Ethereum integrate them with transaction fees (e.g., gas), while permissioned systems may omit native tokens for enterprise use. As Fig. 4 shows, the Ethereum Virtual Machine (EVM) executes the contract logic upon activation.

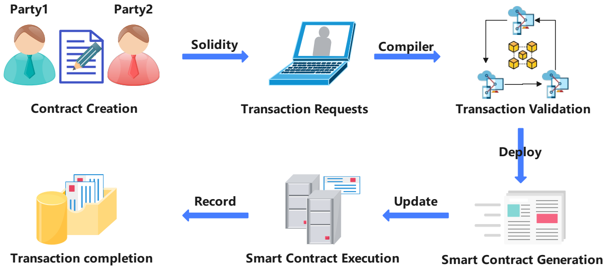

Fig. 4. Processing of smart contracts

2.2.7 *Non-fungible Tokens.*

Non-fungible Tokens (NFTs) are unique, traceable, and indivisible digital assets issued on BC platforms such as Ethereum, following the ERC721 standard and protocol [31]. The value of NFTs is primarily shaped by market perceptions of uniqueness, scarcity, and liquidity. NFTs enable the identification of unique, non-transferable digital certificates that ensure authenticity and ownership, with their immutable storage on the BC preventing any alterations or duplication. The adoption of NFT standards has seen rapid growth within the BC ecosystem, driven by their applications in digital art, gaming, and asset tokenization.

2.2.8 *InterPlanetary File System Storage.*

The InterPlanetary File System (IPFS) is a decentralized hypermedia protocol designed to provide distributed file storage and retrieval [20]. While not part of the BC, the IPFS is commonly employed as a complementary off-chain storage solution to address the limitations of on-chain data handling. Unlike traditional file storage methods, IPFS segments files into smaller blocks and distributes the blocks across multiple nodes in a decentralized network, enabling efficient restoration, data availability, and resilience [166]. IPFS assigns each uploaded file a unique hash for integrity verification, offering a secure, low-cost, and predictable alternative to traditional on-chain storage.

3 BLOCKCHAIN FOR DIGITAL TWIN: DATA SERVICE PERSPECTIVE

This section investigates advanced BC-based data services for DTs from a data services perspective, covering data access, storage, sharing, interoperability, data privacy protection, and access control as shown in Fig. 5.

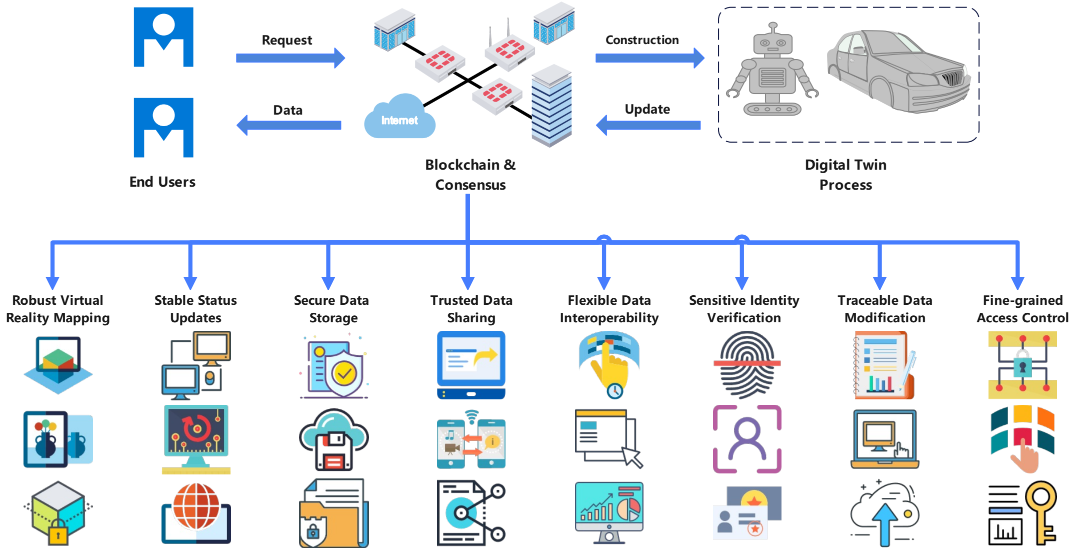

Fig. 5. BC data service for digital twins

3.1 Robust Virtual Reality Mapping

The core objective of DTs is to represent the internal mechanisms of physical entities through analysis and simulation, enabling data-driven decision-making and optimization [26]. BCDT supports accurate and dynamic representations of physical items by capturing real-time data on aspects such as appearance, performance, location, and anomalies [63]. Ideally, the mapping and synchronization state that the BCDT achieves should encompass the twin item's whole lifecycle, changing and updating along the way, from design through manufacture, use, and end-of-life.

3.2 Stable Status Updates

A robust IoT sensing system for continuous monitoring of POs requires accurate measurement, coordinated data interaction, and precise identification of object location and attributes. Reliable synchronization between the DT and PO enables consistent data mapping and interaction across physical and digital domains [137]. BC's distributed ledger facilitates transaction verification and traceable updates throughout the DT lifecycle [47], while majority-node consensus mechanisms help prevent unauthorized modifications and enhance system trust.

3.3 Secure Data Storage

Implementing the DT requires large-scale data storage. Each virtual entity has its own data file, which grows over time due to the simulation and prediction of real conditions. Virtual simulations, analytical tools and reality itself are all very vulnerable if basic data storage is disrupted. A centralized storage system, however, runs the risk of data loss, manipulation or leakage [83]. By adopting asymmetric cryptography, BC technology enables individuals to take charge of maintaining their data [8, 105].

3.4 Trusted Data Sharing

DT simulations often require cross-organizational data sharing for analysis. Centralized platforms pose privacy risks and suffer from data inconsistency, latency, and limited availability. Real-time sharing in DTs demands higher levels of security and transparency, which are difficult to achieve in traditional setups. BC's decentralized structure allows applications to exchange information freely across locations and technologies [190], while also enabling collaborative data preparation and reducing labeling costs for analysis [215].

3.5 Flexible Data Interoperability

Interoperability is essential for DTs, as data flows continuously between physical and virtual entities [42]. Digital applications should support efficient information exchange across diverse locations and technologies [120], yet current centralized platforms are often fragmented. BC offers potential to enhance interoperability by enabling data transformation, encryption, and exchange via both on-chain and off-chain mechanisms, though further research is still required.

3.6 Sensitive Identity Verification

Digital identity codes assigned to POs ensure accurate mapping to their corresponding DOs in the twin space [155, 200]. Synchronization ensures that changes to the DO are immediately reflected in the PO [148]. Global identifiers also enable fast access to the DT database, allowing efficient retrieval of index, location, and metadata.

3.7 Traceable Data Modification

Effective information management and exchange with DTs in Industry 4.0 require seamless access for all stakeholders involved throughout the lifecycle. However, the integrity of DT data remains vulnerable to errors at any individual node, potentially compromising the entire system. Third-party applications, which often lack robust security measures, can expose sensitive information, making them prime targets for malicious attacks within the DT environment. Integrating BC technology into DT frameworks offers a promising solution to enhance data traceability and ensure immutable record keeping [123].

3.8 Fine-Grained Access Control

The DT base model is a network element and topology model that matches a physical entity network based on environmental data, operational status, link topology, and other information to achieve an accurate representation of the physical network in real time [36, 189]. An industrial asset often reflects a sophisticated system, item, or procedure. Compounding complexity creates serious trust problems. Each organization should be granted exact authorization and access to the different DT data modules since the lifecycle parties participating in an industrial plant have varying ownership and access to data.

4 PROTOTYPE IMPLEMENTATIONS OF BCDT

This section describes the prototypical implementations of BCDT. Subsection 4.1 introduces the generic framework, Subsection 4.2 describes the installation platform, and Subsection 4.3 presents the prototype implementation.

4.1 Framework

The BCDT proposal was first seen in [39], but has not received much attention until recently. When managing massive DT services, security and sustainability concerns are addressed using the distributed and shareable paradigm of BC technology. The structure of BCDT has therefore been analyzed in many studies. Hemdan et al. [62] reviewed key aspects of BCDT design and implementation. Focusing on secure access control, Danilczyk et al. [38] proposed a decentralized, ownership-centric sharing architecture tailored to DT components and lifecycle requirements. Lv et al. [113] further examined BCDT architecture and introduced the Blocknet model. Combined with the analysis of the data functions of the BC in the BCDT, the topology of the BCDT is shown in Fig. 6. Most of the prototype implementations in subsequent studies are based on this structure.

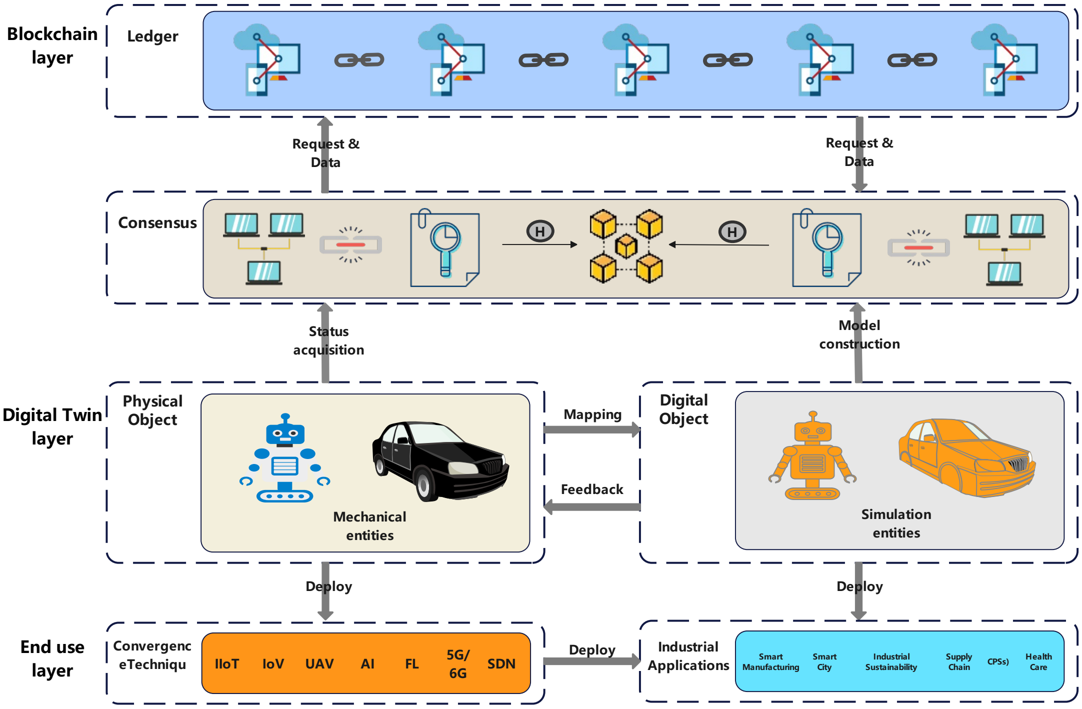

Fig. 6. The basic framework of BCDT

4.2 Modules and platforms

BC platforms are commonly categorized as public, consortium, and private (permissioned). Among them, consortium BCs have become the dominant choice for industrial BCDT deployments, offering a practical balance between decentralization and administrative governance. Turing completeness enables the automated execution of complex business logic, enhancing the efficiency of tasks such as data access control, identity authentication, and DT interaction within BCDT systems. Platforms like Hyperledger Fabric and Ethereum further support dynamic policy management through programmable smart contracts, aligning system performance and scalability with the demands of a controlled consensus framework.

4.2.1 Ethereum.

Ethereum[1] is a leading open-source BC platform featuring smart contract support and a vast decentralized network. It introduces Ether as both its native cryptocurrency and fuel for executing programs on the EVM, a decentralized runtime environment capable of running Turing-complete smart contracts. Designed to address scalability limitations of earlier BCs like Bitcoin, Ethereum supports a robust ecosystem of DApps developed using mature toolchains and security frameworks, backed by an active global developer community.

4.2.2 Swarm.

Swarm[2] is a decentralized storage and content distribution platform designed for the Ethereum Web 3.0 ecosystem. It enables interaction with smart contracts and supports Ethereum-based DApps by offering services such as content storage, distribution, and retrieval. Swarm utilizes the unused storage and bandwidth of participating nodes, forming a peer-to-peer infrastructure for scalable, fault-tolerant data management. Identity and access control are integrated through Ethereum accounts, while open ledger records ensure transparent, verifiable off-chain storage. Developers can access content and manage data using Swarm's set of APIs.

4.2.3 Erebos.

Erebos[3] is a JavaScript toolkit developed by the Mainframe team for building DApps on top of Swarm. Originally created as a proof of concept for the Onyx messaging application, it now serves as a core component of the Mainframe OS. Erebos uses Swarm to encrypt and store files off-chain through a BC account and provides a set of commands for interacting with the Swarm API. Beyond basic functionality like publishing static websites, it also supports more advanced use cases, such as managing interactive timelines.

4.2.4 Web3.js.

Web3.js[4] provides a JavaScript interface for interacting with the Ethereum. Since the Web3.js API was initially intended to be used primarily with local RPC nodes, synchronous Hypertext Transfer Protocol (HTTP) requests are made by default. Web3 version 1.0 provides multiple mechanisms for managing asynchronous operations, thereby improving its adaptability across heterogeneous projects complying with different standards. Typically, the last parameter of a function acts as a callback, whereas a promise is returned when multiple functions are invoked concurrently.

4.2.5 Hyperledger Fabric.

Hyperledger Fabric[5] is an open-source, enterprise-grade, permissioned blockchain framework supporting smart contracts—known as chaincode—written in Golang, Node.js, or Java. The framework eliminates reliance on cryptocurrency and mining, thereby reducing operational risks and costs. Besides, Fabric supports LevelDB and CouchDB as world state databases, enabling key-value storage or JSON-based queries. Its modular consensus design allows initiators to choose mechanisms suited to various organizational structures, from hierarchical to peer-to-peer. Fabric ensures strong data validity through multi-stage endorsement, permission checks, and transaction sequencing before appending blocks to the ledger.

4.3 Implemented prototypes

Several BCDT prototypes have been developed to explore architectural feasibility and deployment. The earliest open-source project by [60] introduced a smart contract-based method for DT creation, emphasizing traceability, accessibility, and immutability. To enhance security and quantum resilience, [76] proposed the spiral DT framework with a variant BC, Twinchain, which incorporates dynamic dimensions and enables instant transaction confirmation. To support decentralized DT data sharing, [11] embedded smart contracts into DT

---

[1] https://Ethereum.org/en/

[2] https://www.ethswarm.org/

[3] https://erebos.js.org/

[4] https://github.com/ChainSafe/Web3.js/blob/v1.7.5/docs/index.rst

[5] https://github.com/hyperledger/fabric#releases

containers—eliminating reliance on Oracles—by integrating tools such as *Chainlink*[6] and *Compellio Registry*[7] that enable smart contracts to access external data sources.

In industrial contexts, EtherTwin [140] presents a decentralized sharing model aligned with DT lifecycle access control. Similarly, [67] used Ethereum and the *Siemens* Building Twin[8] platform to build a full-stack prototype using real building data. [82] proposed a unified testing framework combining *Unity*[9], Ethereum via *NEthereum*[10], smart contracts in *Solidity*[11], and a *Web3-react* interface[12], enabling interactive and visualized DT simulations. In contrast, [94] used Hyperledger Fabric to implement a BC-based Synchronized Provable Data Possession (BSPDP) scheme that enhances DT state verification and integrity assurance. Lastly, a conceptual attempt to create personal DTs with cognitive BC support was presented in [9], though it remains in an early phase. The reviewed prototypes are summarized in Table 3.

Table 3. The available BCDT prototypes

Project	Platform	Tools/modules	Ref.	Github/Open Source
DT	Ethereum,Hyperledger Besu	IPFS, Golang, NodeJS, SmartCheck, Solidity Remix.	[60]	https://github.com/smartcontract694/DT/blob/master/code
Spiral DT	Twinchain	Smart digital signatures, PoW consensus, Genesis	[76]	-
Compellio Registry	Ethereum, Chainlink	Smalltalk, C++, Java, Gang of Four	[11]	https://compell.io/products/BC-registry
EtherTwin	Ethereum	JavaScript framework Vue.js, Web3.js, erebos	[140]	https://github.com/sigma67/ethertwin
PBST	Ethereum	Siemens, Solidity, JavaScript, NodeJS, Web3.js API	[67]	https://github.com/mahshidmotie/PerformanceBasedSmartContracts
BCDT-CPPS	Ethereum, Unity	web3-react, Nethereum, .NET, Solidity	[82]	-
BSPDP	Hyperledger Fabric	Software Development Kit (SDK)	[94]	-

5 BCDT-ENABLED CONVERGENCE OF KEY TECHNOLOGIES

The essential industrial decision-making process is heavily reliant on new technologies. BC can improve important DT technologies to address the major issues with various data repositories, enhancing the efficiency of social and commercial operations in industrial production and industry 4.0. Fig. 7 depicts the key enabling technologies of BCDT. Details of the entities involved in these technologies, the existing challenges, the advantages of deploying BCDT, and all the studies mentioned are presented in Table 4.

5.1 Industrial Internet of Things

With the emergence of 6G and advanced IoT technologies, IIoT systems are evolving into sustainable computing infrastructures. In Industry 4.0 environments, BCDT frameworks address the strain of massive sensitive data on limited IoT devices by improving communication efficiency, privacy, and scalability. Suhail et al. [167] propose a BC-based IIoT architecture to secure data acquisition and management, where lifecycle events are securely recorded and used for monitoring, diagnostics, and optimization. Zhang et al. [207] further introduce a smart manufacturing system that integrates edge-implemented DT with permissioned BC to ensure traceability and operational transparency.

Recognizing challenges in decentralized management and resource allocation, Wang et al. [188] design a BCDT-based architecture to support resilient data and energy flow in distributed settings. Building on this, HDTIoT [191] employs edge networks to securely bridge physical and digital domains through real-time computing. ManuChain [87] advances the concept for personalized manufacturing by enabling real-time IIoT event tracking

---

[6] https://coincentral.com/what-is-chainlink-a-beginners-guide-to-decentralized-oracles/

[7] https://compell.io/

[8] https://new.siemens.com/global/en/products/buildings/digital-building-lifecycle/building-twin.html

[9] https://unity.com/

[10] http://docs.nEthereum.com/en/latest/

[11] https://docs.soliditylang.org/

[12] https://betterprogramming.pub/BC-introduction-using-real-world-dapp-react-solidity-web3-js-546471419955

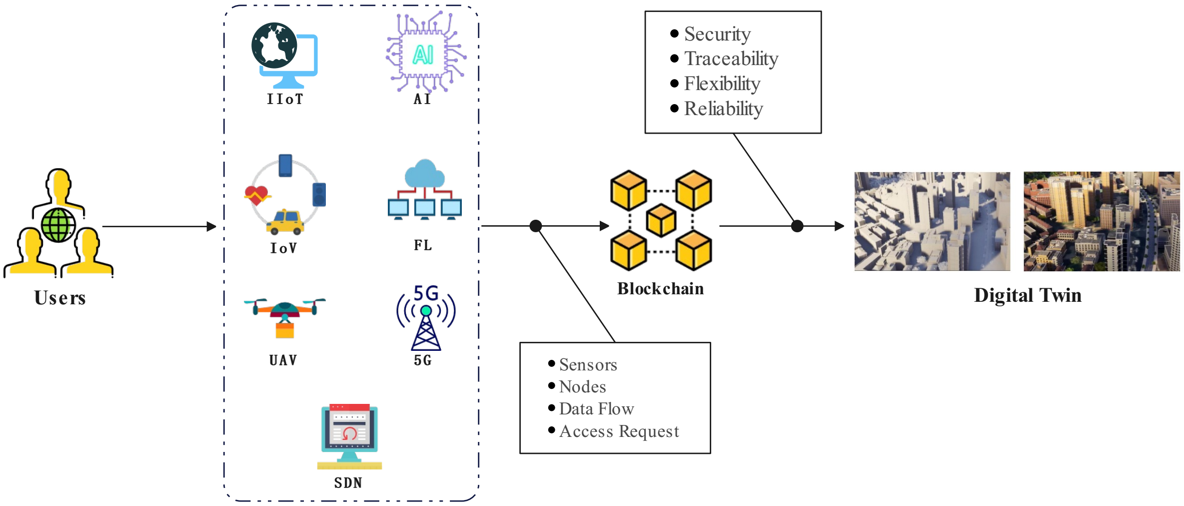

Fig. 7. BCDT-enabled convergence of key technologies

Table 4. The summary of BCDT-enabled Convergence of Key Technologies

Technologies	Entities	Existing Challenges	Advantages of Implementing BCDT	Related Studies
IIoT	• IIoT network nodes	• Large-scale data processing • Limited computing resources • Weak data privacy	• Improved communication efficiency • Enhanced data privacy • Lower computing costs	[57, 87, 167, 188, 191, 202, 207]
IoV	• Vehicles	• Inefficient data sharing mechanism • Insufficient safety of vehicle resources	• Safety • Traceability • Innovative incentive mechanism	[28, 175]
UAV	• UAV • Vehicles	• High dynamics • Unpredictability	• Energy-efficient design • Real-time dynamics	[35, 172, 194, 197, 198]
AI	• Sensors • Mobile users	• Unreliable data dissemination • Restrictions of the amendment • Collaborative nodes with weak security	• Reduced failure rates • Increased efficiency • Flexibility	[85, 103, 115, 169]
FL	• IoT devices • Edge nodes	• Fragile communication security • Poor data privacy protection • Limited computing resources	• Enhanced user security • Guaranteed data privacy • Trusted communication • Minor accuracy lost	[73, 101, 108, 142, 144]
5G & 6G	• Wireless networks • Edge nodes	• Unreliable communication channels • Heterogeneity and latency • Mobility	• System reliability • Secure communication • Data privacy	[13, 77, 109, 110, 206]
SDN	• SDN controller • End-user application • Application plane	• Attacker focus • Vulnerable communication channels	• Preventing attacks • Reliable communication • Avoiding single points of failure	[4, 7, 10, 18, 19, 65, 69, 70, 78, 79, 156, 185, 187, 204, 205]

and autonomous process execution via smart contracts. Yang et al. [202] employ BC rules to facilitate flexible access and visualization of IoT sensor data. Additionally, Hammoudeh et al. [57] highlight BCDT's value in securing national infrastructure and ensuring efficient, reliable operations.

5.2 Internet of Vehicles

IoV enables continuous connectivity and localized computing for advanced Vehicle-to-Everything applications, deploying smart infrastructure like Roadside Units (RSUs) and adaptive traffic signals for real-time data coordination. However, the dynamic and heterogeneous nature of IoV complicates resource allocation and secure data exchange. DTs support real-time representation of vehicle states such as position, speed, and fuel level for predictive control and situational awareness, but current communication frameworks often face limitations in data sharing efficiency, privacy, and trust management.

BCDT addresses these challenges by integrating BC into DT systems to enable secure resource exchange, decentralized authentication, and verifiable transactions among vehicle twins. For instance, [175] proposes a consortium BC-based framework to safeguard resource sharing between vehicle DTs. Similarly, [28] introduces Cyberchain, a permissioned BCDT authentication framework tailored for dynamic IoV environments, which reduces communication and storage overhead while preserving privacy. These efforts reflect a clear trend where DT models constitute the operational core, and BC serves as an enabling infrastructure to enhance trust, integrity, and system-level security in vehicular networks. The BCDT paradigm thus offers promising solutions for traceable interaction, privacy-aware coordination, and autonomous resource management in complex IoV scenarios.

5.3 Unmanned Aerial Vehicle

Unmanned Aerial Vehicle (UAV) features high flexibility, operational reliability, cost efficiency, minimal environmental requirements, and compact portability. However, in practice, UAV nodes move at high speeds, facing challenges such as high dynamics and unpredictability. To analyze airspace organization and safety performance in UAV systems based on DT, the study in [197] introduced the DT concept. Then, the work in [194] developed a dynamic DT model for air-assisted IoV, considering time-varying resource availability and the need for consistent resource scheduling and allocation.

The construction of dynamic DT channels for air-assisted IoVs is examined in [172] to capture system resource availability and time-varying demands. With UAV assistance, vehicles detected by the ground network can offload computational tasks to resource-rich units such as roadside units (RSUs). As a result, resource scheduling and allocation in aerial-assisted IoVs become more efficient and adaptive. Furthermore, [198] analyzes the architecture and functional roles of each layer within a DT framework designed for reliable communication in military UAV networks. In [35], a secure federated aerial learning framework inspired by BCDT is proposed, integrating a null-based BC mechanism for secure data transmission and an aerial BC with training models to validate the proposed scheme. In summary, BCDT enables high energy efficiency, improved vehicle satisfaction, and real-time responsiveness for UAV nodes and related applications.

5.4 Artificial Intelligence

Data is the backbone of DT systems, supporting algorithms that simulate and reflect physical asset behavior. BC reinforces digital trust by offering decentralized mechanisms for secure data validation and provenance tracking, addressing issues such as unverifiable data, rigid update procedures, and weak security in loosely coupled systems. By continuously gathering real-time and contextual information, DTs provide fertile ground for machine learning (ML) applications in predictive analytics, anomaly detection, and performance optimization. Integrating AI into BCDT architectures enhances intelligent decision-making, while BC ensures the integrity and traceability of outcomes.

For instance, the system proposed in [115] uses sensors to build real-time DTs and supports precise BC transactions, offering a scalable model for Industry 4.0. Liu et al. [103] demonstrate that BCDT-assisted task offloading to mobile-edge servers effectively reduces power consumption and latency, optimizing real-time interaction with physical assets. Suhail et al. [169] present a BC-AI fusion framework that enhances DT security in CPS, with use cases illustrating how intelligence-driven designs mitigate cyber threats. Similarly, Lee et al. [85] propose a reference architecture combining Deep Learning (DL), DT, and CPS to support the transition toward smart manufacturing under Industry 4.0.

5.5 Federated Learning

FL addresses privacy concerns by enabling users to train machine learning models locally, sharing only model parameters with a central server, offering a collaborative framework that preserves data privacy while supporting distributed model training. In traditional cloud-based DT architectures, data is typically aggregated on centralized servers for model training. However, such setups often raise concerns related to communication overhead, data exposure, and system scalability. By incorporating FL into BCDT systems, model training can be performed in a decentralized and privacy-preserving manner, enhancing both the security and efficiency of the DT lifecycle. For example, [101] investigates BC-based FL systems and highlights their applicability in DT scenarios. The survey by [144] suggests that integrating BCDT with federated learning (FL) enhances dependability and privacy, where BC ensures transparency and traceability, DT improves FL model efficiency in smart city contexts, and the distributed architecture enables effective data provisioning across multiple devices.

Then, Lu et al. [108] propose a two-tier digital network architecture that employs BCDT to enable secure and privacy-preserving communication across edge environments, where FL on the BC collaborates with IoT-enabled DTs to maintain model accuracy while reducing reliance on centralized data aggregation. Similarly, [73] indicates a novel DT-blade network architecture based on BC technology that bargains to build cooperative joint learning aimed at producing DTs at the network's edge while maintaining wireless resources and forming connections in local model update tangles. In particular, the FedTwin paradigm proposed in [142], focuses on improvements in automation, privacy, and security for DTs. and develops a federation proof consensus algorithm for efficient and secure synchronization of DTs while enabling personalization incentives.

5.6 5th and 6th Generation Mobile Communications Technology

The integration of BCDT plays a critical role in advancing communication technologies, particularly within next-generation wireless networks. Lu et al. [109] show that integrating DTs with wireless networks enables edge-centric processing that enhances reliability, security, and privacy, while the joint use of FL and BC improves communication efficiency and reduces latency. [206], [13], and [77] further explore how intelligent computing can be combined with 5G and 6G infrastructures to meet the performance and autonomy demands of future BCDT systems. The progression to 6G networks introduces challenges related to heterogeneity, mobility management, and ensuring consistent low-latency, high-throughput data handling.

As 6G networks evolve toward programmable and intelligence-driven architectures, the convergence of DT, BC, and AI is poised to become the foundation for intelligent automation, dynamic service orchestration, and secure digital operations. In dynamic device association scenarios, the BC-edge framework proposed by Fancy et al. [48] combines BC immutability with DT adaptability to enable self-verifiable service migration and strengthen edge node resilience against hijacking. With progress in Deep Reinforcement Learning (DRL) and asynchronous DT migration technologies, the BCDT architecture continues to advance through the integration of elastic data layers and cognitive decision engines—reshaping autonomy across the edge–cloud continuum and enabling multidimensional coordination in future intelligent networks [110].

5.7 Software Defined Networking

Software Defined Networking (SDN) modularizes the control, data, and application planes of the network, enabling centralized programmable control that facilitates dynamic resource allocation, scalable traffic management, and automated fault recovery. The layered abstraction is particularly impactful in complex environments such as 5G and beyond, where responsiveness and agility are crucial [4, 7, 70]. However, the logically centralized control plane introduces critical security vulnerabilities, especially in the communication channels between controllers and data-plane devices, which are prone to interception and tampering.

Permissioned BC architectures allow authenticated consensus among network entities, strengthening the security posture of SDN controllers while maintaining low-latency coordination [10, 205]. From a BCDT perspective, convergence offers a compelling foundation for orchestrating DTs of network functions and virtual assets. Using BC for transparent state synchronization and access validation and SDN for programmable resource control, BCDT systems can support self-adaptive service chaining, context-sensitive routing, and real-time policy reconfiguration in high-stakes environments such as IoT, vehicular networks, and industrial automation [156].

6 INDUSTRIAL APPLICATIONS OF BCDT

This section focuses on the industrial applications of BCDT, which are categorized into nine domains as summarized in Table 5. For each category, we highlight the specific benefits and advancements enabled by representative studies.

Table 5. The summary of Industrial Applications of BCDT

Application	Fields	Users/Deployment entities	Existing Challenges	Benefits of deploying BCDT	Related Studies
Smart Manufacturing	Big data management	• SMEs • Business stakeholder	• Inadequate digital capability • Limited budget and investment • Insufficient trust & collaboration	• Data encryption • Secure data Sharing • Effectiveness	[66, 104, 157]
	Collaboration and platform	• Shared platforms • Stakeholders	• Inadequate interactions • Mistrust challenges • Static information encapsulation	• High fidelity analysis • High confidence	[122, 179]
	Customised manufacturing	• SMEs	• Complex collaboration • Heterogeneity	• Facilitating knowledge exchange • Interoperability • Continuous updates	[56, 74, 92, 93]
	Precision manufacturing	• Component manufacturers	• Extreme production standards • High manufacturing loads	• Reliability • Transparency	[61, 114]
Smart City	Smart transportation	• Vehicles • Public transportation • Energy systems	• High dynamics • Complex interactions • Large-scale traffic data	• Stability • Reliability • Intelligence	[46, 97, 151]
	Vehicular Edge Networks	• RSUs • Vehicles	• High dynamics • Complexity • Variability	• Optimising cache utility • Large-scale processing capability	[208]
	Smart grid	• Sensors	• Complexity of calibration • Insecure environment • Vulnerability to cyber-attacks	• Trustworthiness • Lightweight • Anti-attack	[23, 32, 38, 106]
	Infrastructure & Construction	• Engineering industries	• Fragile trust • Inefficiency • Data silos	• Trust and security • Decentralization • Efficiency • Traceability and transparency	[27, 84, 164, 180, 181]
Industrial sustainability	Machine failure detection	• Production facilities	• Difficulty of manual prediction • Vulnerability to cyber-attacks	• Trust, transparency and security • Early Warning • Lightweight	[158]
	Equipment Maintenance	• Maintenance personnel	• Non-global • Non-service-oriented • Unrecoverable	• Simulation immediacy, • Transparency of information, • Low maintenance cost,	[54]
	Asset life cycle management	• Industry professionals	• Heterogeneous data structures • Non-standardised packaging • Different processes	• Applicability • Interoperability • Integratability	[30]
Supply Chain Management	Data Management	• Supply Chain Commodity	• Centralized management • Weak traceability • Single point of failure	• Traceability • Verifiability • Decentralized authority	[24, 50, 99]
	Risk management	• Supply Chain Commodity • Industrial hemp	• Complexity • Variability • No information tracking	• Transparency • Security • Efficiency	[68, 192]
CPS	Production security	• Automotive assembly lines	• Complexity of cyber-attacks • State synchronization issues	• Robust security • Trusted sources • Situational awareness	[82, 170, 171]
	System security	• Partners • Stakeholders • Parallel Sector	• Redundancy • Inefficiency	• Security • Accountability • Integrity	[75] [85]
Healthcare	Patient care	• Medical Systems	• Malicious use of data • Inferior data security • Fragile data privacy	• Data normalization • Model standardisation • System integration	[5]
	Pandemic Response	• Medical Systems	• Centralized management • Single point of failure	• Data integrity • Real-time data analysis. • Predictability • Reliable data sharing.	[107, 150]

6.1 Smart Manufacturing

Smart manufacturing, driven by big data and DTs, has become central to Industry 4.0 and the global industrial shift [141]. To remain competitive, manufacturers must improve precision while reducing costs. BCDT enables efficient resource use, speeds up production digitalization, and enhances sustainable modeling services.

6.1.1 Data Management. In industrial manufacturing, inconsistencies among software systems often hinder effective information flow. BCDT enhances collaboration across communication, sensing, and energy domains. To address trust issues in smart manufacturing, [157] proposes a BC-based system for secure sharing and storage of large DT datasets throughout a device's lifecycle. Similarly, [66] introduces a BC-driven data management strategy with smart contracts to automate processes and improve efficiency across the product lifecycle. To support SMEs facing financial and technical barriers, [104] presents Imsestudi, a secure BCDT platform tailored for service-oriented DT applications.

6.1.2 Collaboration and Platform. Production efficiency can be improved through models and platforms that enhance industrial collaboration. [179] explores BCDT-enhanced manufacturing service management on industrial internet platforms, proposing a corresponding collaboration mechanism based on current development trends and challenges. In [122], the benefits, challenges, and risks of applying BC to sustainable DT manufacturing are assessed, highlighting high-fidelity analysis and strong confidence levels as key advantages of BCDT platforms.

6.1.3 Customized Manufacturing. The BCDT module offers a reliable DT service to visualize and optimize customized production processes, helping manufacturers streamline operations. With the advancement of Industry 4.0, personalized and social manufacturing has emerged, enabling enterprises to co-create customized products and services through cross-organizational integration [74]. To support this, Refs.[92, 93] propose a resource-sharing model that protects DT copyrights and enhances interoperability within distributed networks. Similarly, [56] combines BC, additive manufacturing, and DTs to address data heterogeneity, promoting customer-centric and sustainable production models.

6.1.4 Precision manufacturing. High-tech sectors like aerospace and automotive demand precise simulation and inspection across the production lifecycle. BCDT enables virtualized POs, real-time monitoring, dynamic scheduling, and energy optimization, driving industrial transformation and efficient workshop control. In aerospace, BCDT offers a secure and integrated infrastructure for managing data across additive manufacturing stages [114]. Similarly, in the automotive domain, BCDT supports traceable data management across the entire vehicle lifecycle, from system engineering to after-sales service [61].

6.2 Smart City

The growth of urban data provides a vital foundation for smart city development, enabling standardized big data systems to enhance governance precision and administrative efficiency. BCDT supports smart city development by enabling refined governance, efficient urban planning, and accelerated operations, particularly in areas like transportation, energy grids, and infrastructure.

6.2.1 Smart transportation. Smart transportation systems play a vital role in future smart cities, offering improved intelligence, efficiency, and safety. However, the diversity and complexity of device deployment create challenges in managing system dynamics. BCDT supports realistic simulations, enhancing autonomous driving algorithms and crisis response. For instance, [46] explores BCDT-based road infrastructure development, while [97] proposes an on-demand DT architecture for evolving transport needs. [151] presents a collaborative ledger-based DT model, emphasizing distributed consensus and real-time analytics.

6.2.2 *Vehicular Edge Networks.*

The growth of intelligent vehicles and advanced applications drives demand for efficient content delivery. BCDT-based collaborative caching addresses this need by optimizing cache and communication resources amid limited storage, coverage, and dynamic network conditions. In [208], BCDT technology maps physical systems into virtual space, enabling cache controllers in socially aware networks to understand vehicle relationships and optimize content allocation.

6.2.3 *Smart Grid.*

The energy system of the smart city of the future will follow a diverse path towards a zero-carbon economy, of which the smart grid is a key component. However, the complexity of calibration, insecure environment and vulnerability to cyber-attacks are notable challenges for smart grids. Studies like [23, 32] demonstrate that BCDT can enable intelligent energy operations, improving efficiency while reducing industrial consumption. To ensure secure data transmission in Industry 4.0 smart grids, [38] introduces a BC-based method that links sensor data using checksums, reinforcing insecure protocols like Modbus [173] and DNP3 [33]. In addition, [106] explores how DTs can predict failures, detect real-time security risks, and dynamically adjust access controls—highlighting the long-term potential of BC and ML in autonomous, self-learning smart grids.

6.2.4 *Infrastructure and Construction.*

Infrastructure is essential to urban development, but construction projects often involve multiple stakeholders, leading to fragmented trust and isolated data systems. To address these challenges, Song et al. [164] proposed a BC-based data management model to ensure system stability and data integrity in smart city development. Teisserenc et al. [180, 181] introduced a conceptual framework for integrating BCDT in construction to enhance trust, efficiency, and information transparency. Lee et al. [84] validated a BCDT architecture that enables real-time tracking of prefabricated components, with positional data recorded on the BC to ensure traceability. Celik et al. [27] demonstrated that BCDT can improve the accuracy and reliability of cost and scheduling estimates, accelerating DT adoption in the construction sector.

6.3 Industrial Sustainability

Industry 4.0 emphasizes the need for sustainable industrial practices to meet growing production demands. Equipment-oriented BCDT applications focus on real-time monitoring of equipment, plant-oriented BCDT focuses on full-process production control, while industry-oriented BCDT can provide full product lifecycle traceability. Therefore, researchers propose to implement machine fault detection and equipment maintenance through BCDT, and better implement asset life cycle management.

6.3.1 *Machine Failure Detection.*

The manual prediction of tool condition wear on CNC machines has become more difficult as a result of the fast growth and expansion of industrial technologies in Industry 4.0. Thus, [158] proposes a BCDT-based architecture that leverages smart contracts to enhance prediction accuracy while ensuring authentication, traceability, and transparency. Data interaction between the DO and PO supports multi-dimensional equipment energy analysis and enables timely detection and handling of unexpected failures, reducing production losses.

6.3.2 *Equipment Maintenance.*

Through real-time data collection and equipment manufacturing equipment collection, BCDT allows the construction of data model-driven bi-directional real mapping and real-time interaction between physical and virtual bodies on the shop floor and equipment monitoring. It mainly consists of a virtual DT service before production, a real-time DT service during production and a DT service after production to ensure real-time correspondence between preparation and things. The BCDT-based design of the data chain for components manufacturing, equipment transfer and then the entire life cycle is presented in [54].

6.3.3 *Asset Life Cycle Management.*

The complexity of shop-floor and plant operations demands advanced management mechanisms. Traditional network lifecycle management lacks integration, hindering fault prediction and optimization. BCDT facilitates digital asset lifecycle management by enhancing usability, accessibility, and implementation guidance. For example, [30] highlights the idea's enormous potential to entirely fix current digitizing processes while presenting it as a tactical tool and multifaceted field assistance application. Network and device lifecycle data is tightly combined through DT and properly maintained by the BC module for refined management of the entire network and device process.

6.4 Supply Chain Management

The challenges of supply chain management focus on the large amount of data and the wide range of participants. BCDT enables full lifecycle participation in production, logistics, and services, spanning equipment, workshops, enterprises, and industrial chains. The decentralized and immutable nature of BCDT enhances data traceability, enabling more refined and transparent interactions among supply chain stakeholders, which improves coordination, accountability, and efficiency.

6.4.1 Data Management. BCDT and supply chain management are fully compatible, especially in smart manufacturing, smart maintenance, shop floor, warehouse and logistics deployments. The use of BC-based data transfer provides greater security and efficiency. Firstly, the survey of [99] offers a thorough analysis of the literature on the use of BCDT in supply chain management. [50] then suggests using a BCDT-based solution to restructure supply chain management systems. This will make it easier for supply chain management to be intelligent and digitized so that it can handle a sizable number of services in intricate cross-sector systems. Also, [24] proposes a paradigm for enhancing physical supply chain management through the integration of DT modules in diverse contexts with BC at all levels. The data saved in the BCDT is easier to trace and maintain functionally, securely and granular for the interaction of various supply chain management parties.

6.4.2 Risk Management. The design of resilient supply chains often introduces increased risk of information, increased exposure to external uncertainties, and challenges related to fluctuation in time and demand. Industrial production supply chains must contend with extreme complexity, unpredictability, limited manufacturing insights, and insufficient data monitoring. Wang et al. [192] propose a simulation-driven DT model with a BC-based interface to support distributed CPS, improving risk management and secure information sharing in the industrial hemp supply chain. Similarly, Ivanov and Dolgui [68] suggest that integrating Industry 4.0 technologies with additive manufacturing establishes a more resilient risk management framework powered by BCDT, enhancing the capacity of the supply chain for dynamic resource reallocation during recovery phases to improve adaptability and stability.

6.5 Cyber-Physical System

The complexity of cyber-attacks in CPS necessitates mechanisms that can evaluate operational behavior and infrastructure security without disrupting real-time processes. In this context, BCDT offers valuable capabilities by securely monitoring, modeling, predicting, and optimizing the state of CPS.

6.5.1 Production security. In [170, 171], a trustworthy DT framework based on BCs is envisioned to safeguard CPS. As a CPS use case, the automotive industry is utilized to demonstrate the framework's capabilities. Then, the BCDT-based concept for cyber-physical manufacturing systems is developed and illustrated in [82]. The recommended demonstration shows how cyber-physical manufacturing has improved process and data integrity as well as transparency.

6.5.2 System security. According to [75], BCDT supports Industry 4.0 applications by utilizing a decentralized BC architecture that enhances data integrity and accountability, particularly in complex multi-stakeholder environments. The reference model in [85] integrates DL with DTs, providing a roadmap for the development of intelligent manufacturing systems that are transparent, collaborative, resilient, and efficient.

6.6 Healthcare

DTs enable digital replicas of the human body, offering new capabilities in health monitoring and diagnostics. Integrating BC ensures secure, tamper-proof storage of sensitive medical data. BCDT addresses key challenges in lightweight digital healthcare, including privacy protection and secure communication.

6.6.1 Patient Care. Mirror mapping techniques facilitate the development of DT in the human body, capturing detailed physiological and anatomical information in a standardized digital format. DTs allow for continuous monitoring and precise tracking of health metrics, improving preventive care and personalized treatment strategies. Akash et al. [5] introduce a BCDT-based data model that systematically organizes patient-related information in a structured and accessible format, optimizing healthcare data management and real-time health assessments.

6.6.2 Pandemic Alerting & Response. The authors of [150] propose a DApp that leverages BC and DT technologies to address the COVID-19 outbreak and future pandemics. Building on this, [107] identifies and elaborates on the critical interrelationships among hospitals, information systems, and resource flow management. During the pandemic, the integration of dynamic DT and BC proved highly effective in patient management and in optimizing healthcare resource allocation. A summary of BCDT applications in the healthcare domain is presented in Fig. 8.

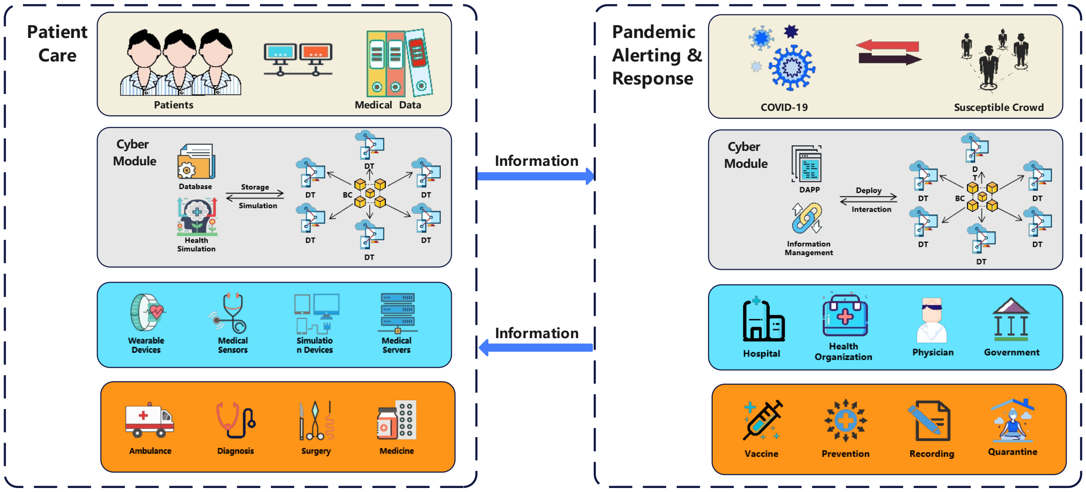

Fig. 8. Applications of BCDT in healthcare

7 CHALLENGES AND FUTURE RESEARCH DIRECTIONS

This section presents the key research challenges and future directions related to the BCDT paradigm.

7.1 Research Challenges

BCDT systems face a wide range of technical challenges due to the complexity involved in modeling, securing, and managing digital representations of physical systems throughout the entire lifecycle. In the following, we highlight several critical and interrelated issues that require further investigation to realize the potential of BCDT in industrial applications.

7.1.1 Multi-Modal Modeling. The integration of diverse data sources, including sensor signals, control logic, simulation outputs, and human intent, is fundamental for DTs. Establishing a unified and consistent modeling framework is essential for accurately reflecting the state and behavior of POs in real-time. Achieving consistent modeling across modalities in dynamic industrial environments requires real-time synchronization, contextual awareness, and adherence to physical laws. For example, modeling an aircraft DT may combine deep learning–based predictions with physics-driven aerodynamic and electromagnetic models, alongside symbolic reasoning for operational logic [182]. However, building scalable and trustworthy modeling pipelines remains a challenge. García-Valls et al. [51] emphasize coordination issues in collaborative DT refinement, even with BC support. Similarly, Bamakan and Far [14] note that while BC improves trust and traceability in distributed modeling, it can introduce latency and structural rigidity, limiting the scalability and adaptability of multi-modal DT systems.

7.1.2 Trusted Data and Input Validation. The reliability of DT behavior depends on the quality of input data. In BCDT systems aggregating heterogeneous sources, maintaining consistency, semantic alignment, and schema compliance remains challenging [129, 143]. Tang et al. [177] note that even with BC support, federated BCDT architectures struggle with enforcing trustworthy updates and detecting unreliable nodes in resource-limited or delay-sensitive environments. Mohammed et al. [120] further point out that BC enhances traceability but cannot fully address alignment and interoperability issues in IIoT scenarios. Although BC offers immutability and smart contract–based validation, its integration introduces latency, lacks semantic reasoning, and suffers from throughput limits—especially for real-time assurance in multitier BCDT deployments. Ensuring lightweight, scalable, and interpretable validation near the edge remains an open research challenge requiring advances in BC infrastructure, smart contract design, and data governance.

7.1.3 Security and Availability of Digital Entities. Ensuring security and availability of DT instances is critical for BCDT systems, particularly in open and collaborative industrial environments. Virtualizing POs within secure DTs reduces attack surfaces, while BC supports decentralized access control and auditability through smart contracts [195, 212]. BC mechanisms enhance cybersecurity in DT contexts [112], mitigating threats like data tampering and DDoS attacks via enforced policy constraints [128]. Zhang et al. developed a BCDT synchronization platform for production logistics that maintains trusted coordination and consistency under dynamic conditions [211]. Yet, BC consensus introduces latency and computational overhead that may impair DT responsiveness, and smart contracts lack adaptability under unstable or degraded network conditions. Moreover, BC's transparency may expose sensitive operational or personal data, especially in cross-organizational DT scenarios with varying privacy requirements. As BCDT systems scale, ensuring availability, timely synchronization, and consistency under adversarial or unstable conditions remains a pressing challenge.

7.1.4 Governance and Multi-party Control. Cross-organizational deployments of BCDT systems introduce fragmented ownership, inconsistent governance policies, and coordination conflicts, which complicate lifecycle management of digital assets [182]. While smart contracts and BC-based digital tokens such as NFTs can formalize access rights and operational roles, enforcing coherent governance across heterogeneous participants remains a core challenge [176]. In practice, variations in legal frameworks, trust boundaries, and domain-specific rules hinder consistent execution and auditing. Recent work has introduced orchestration-based governance using smart contracts to coordinate multi-party workflows, but technical complexity and lack of standard interfaces limit scalability [43]. Efforts to simplify policy enforcement through low-code tools have shown promise, though ensuring cross-domain compatibility and accountability continues to present challenges [29].

7.1.5 Scalability and Resource Efficiency. Meeting performance demands in BCDT systems is particularly challenging in resource-constrained IIoT environments. Improvements in scalability through alternative consensus protocols, federated learning, and sharding come at the cost of increased architectural complexity and coordination overhead [72]. Adaptive strategies such as reinforcement learning-based scheduling [1] and hybrid cloud–edge deployments [124] offer improvements, yet challenges in latency, synchronization, and energy efficiency remain. On-chain delays in block propagation and transaction confirmation continue to hinder responsiveness in time-sensitive scenarios. Moreover, frequent updates and smart contract interactions on public BCs (e.g., Ethereum) incur high transaction fees [53]. While layer-2 rollups [152], batching [133], and migration to fee-less permissioned chains offer relief, they often trade off decentralization, transparency, or flexibility.

7.1.6 Dynamism and Fault-Tolerant Continuity. BCDT systems operate in dynamic industrial settings characterized by frequent failures, human errors, data inconsistencies, and fluctuating workloads. Maintaining real-time synchronization between DTs and POs under such conditions remains a major challenge, as DTs must reflect external changes while preserving continuity even when the PO is offline. Fault-tolerant architectures are essential to support uninterrupted operations. Maintaining consistency across distributed environments during volatile states remains a significant obstacle [210]. Shard-based Byzantine fault-tolerant methods with reputation mechanisms have been explored to secure DT updates in zero-trust settings, though large-scale deployment remains challenging [132]. Incentive-aligned BC models using evolutionary games foster stakeholder collaboration but add coordination and trust complexity [215].

7.2 Future Directions

The future of BCDT lies in enabling secure, auditable, and standards-aligned data utilization. BC can serve as a trust anchor for end users and stakeholders, but further efforts are needed to optimize its logic and performance to improve the applicability of BCDT. Some possible research directions will be briefly discussed as follows.

7.2.1 Standardization. The DT paradigm currently lacks unified standards, limiting scalability and interoperability. Enabling cross-vendor compatibility in distributed environments requires standardized data repositories, interfaces, and modeling components [186]. However, most BCDT implementations rely on application-specific models, leading to semantic inconsistencies and limited cross-domain integration [147]. Future efforts should focus on lightweight, modular standards that bridge physical–digital heterogeneity, enable dynamic updates, and support efficient operation across edge and BC layers.

7.2.2 Servitization and Augmentation of the Digital Twin. Future BCDT systems are expected to deliver DTs as configurable, service-oriented components rather than static representations. Servitization enables on-demand access to DT capabilities, where smart contracts define usage rights, automate compliance, and enforce function-level control across diverse service tiers [139]. However, enabling secure enhancement introduces challenges in authentication, authorization, and runtime adaptability. Attribute-based encryption integrated with the BC has been proposed to enforce fine-grained access in decentralized environments, although performance bottlenecks persist [36]. Thus, future research should develop programmable service orchestration frameworks that balance flexibility, security, and accountability—particularly for DTs deployed in multi-stakeholder industrial ecosystems.

7.2.3 Simulation Recording and Audit. Simulation capabilities are fundamental to DTs, enabling the prediction of PO behavior under varied operational scenarios. However, ensuring that simulation processes and outcomes are verifiable, traceable, and auditable remains a challenge—especially in safety-critical applications where decisions depend on simulation integrity. Recent efforts propose risk-aware auditing frameworks to classify vulnerabilities in simulation pipelines and verify the trustworthiness of digital evidence [134]. BCDTs offer a promising foundation by using smart contracts to enforce simulation workflows, validate assumptions, and provide transparent accountability among stakeholders [116]. Nonetheless, future work must focus on designing lightweight, scalable audit mechanisms tailored to decentralized, multi-party DT environments.

7.2.4 *Intellectualisation.*

With the increasing autonomy and interconnectivity of DTs, the deployment across organizational, social, and even individual domains brings new governance and coordination challenges. In complex environments, multiple replicas of the same PO may exist—each operated by distinct agents or stakeholders—which can lead to conflicts in updating the PO's state or executing actions on its behalf. Recent proposals such as Twin3 leverage BC-backed identity systems to embed rich, multidimensional traits into personal DTs, facilitating more trustworthy interactions in decentralized ecosystems through Proof-of-Authenticity (PoA) mechanisms [200]. Moreover, in large-scale virtual environments—such as the emerging concept of Virtual Cities—DTs are evolving from static monitoring tools into intelligent agents capable of autonomous reasoning and adaptive behavior [127]. Future research should investigate robust coordination protocols and ethical frameworks to regulate replication, decision-making authority, and ownership transfer among DT agents [182].

7.2.5 *BCDT-Enabled Smart Sensors.*

Although BC enhances the security and traceability of DT systems, their overall reliability depends heavily on the quality of sensor data. Traditional sensors often fail to meet the precision, consistency, and adaptability required in modern industrial applications. Recent developments in smart sensors that combine digital acquisition, edge analytics, and communication capabilities have improved the responsiveness and autonomy of BCDT systems [135]. Future research should focus on improving sensor accuracy, resolution, and robustness while ensuring compatibility with BC infrastructures. Embedding lightweight consensus mechanisms within sensing modules can further enable secure and real-time data validation at the edge, reinforcing trust in decentralized and time-sensitive BCDT environments.

7.2.6 *Cross-chain Protocols for BCDT.*

Heterogeneity in data models, consensus protocols, and contract logic across BC platforms limits BCDT interoperability and scalability in multi-party industrial contexts. Ding et al. [43] proposed ManuChain4.0, a layered framework enabling smart contract negotiation and real-time data exchange across BC and IOTA Tangle networks. Future research should enhance orchestration frameworks with standardized interfaces, lightweight adapters, and decentralized gateways to enable efficient, consistent communication.

7.2.7 *Lightning Network.*

Timely responsiveness is critical in BCDT applications, particularly those involving dynamic service delivery and user-triggered operations. Traditional BC systems often introduce latency and transaction costs that limit their suitability for real-time interactions. To address these limitations, the lightning network—a layer-2 protocol—enables rapid, low-cost off-chain transactions through peer-to-peer payment channels, improving the responsiveness of time-sensitive services. In the context of BCDT, lightning network mechanisms can support microtransaction-based access to DT functions such as real-time data queries, computation, and visualization [163].

8 CONCLUSION

In the context of Industry 4.0, BCDT provides a new paradigm for solving the key challenges of DT systems in data credibility, cross-domain interoperability,and decentralized governance. This survey systematically sorts out the theoretical framework, technical architecture and application practice of BCDT from a lifecycle perspective. The deep collaboration of BCDT with IIoT, federated learning, 5G/6G and other technologies can significantly enhance the reliability of DTs in scenarios such as industrial manufacturing and smart cities. Typical implementation solutions based on Ethereum and Hyperledger have verified its feasibility in real-time data traceability and privacy protection. However, the current development still faces twelve key challenges: the technical level needs to break through the bottleneck of multimodal modeling and computing power constraints, and the application level urgently needs to establish an explainability framework and cross-chain interoperability standards. Looking to the future, the mature application of BCDT needs to focus on three major directions: (1) lightweight BCDT integrated architecture design, (2) construction of a quantitative evaluation system for security and performance, and (3) innovation of decentralized DT governance mechanisms. As technical standards are gradually improved, BCDT is expected to become the core enabling technology for trusted digital transformation in key areas, providing new theoretical support and practical paths for the evolution of intelligent infrastructure.

FUNDING

This research is supported by the Natural Science Foundation of Shanghai under Grant 25ZR1401156 and 25ZR1402184, and the National Natural Science Foundation of China under Grant 61672338.

DECLARATION OF INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Innocent Boakye Ababio, Jan Bieniek, Mohamed Rahouti, Thaier Hayajneh, Mohammed Aledhari, Dinesh C Verma, and Abdellah Chehri. 2025. A Blockchain-Assisted Federated Learning Framework for Secure and Self-Optimizing Digital Twins in Industrial IoT. *Future Internet* 17, 1 (2025), 13.

[2] Sarthak Acharya, Arif Ali Khan, and Tero Päivärinta. 2024. Interoperability levels and challenges of digital twins in cyber-physical systems. *Journal of Industrial Information Integration* (2024), 100714.

[3] Shohin Aheleroff, Xun Xu, Ray Y Zhong, and Yuqian Lu. 2021. Digital twin as a service (DTaaS) in industry 4.0: an architecture reference model. *Advanced Engineering Informatics* 47 (2021), 101225.

[4] Ehsan Ahvar, Shohreh Ahvar, Syed Mohsan Raza, Jose Manuel Sanchez Vilchez, and Gyu Myoung Lee. 2021. Next generation of SDN in cloud-fog for 5G and beyond-enabled applications: Opportunities and challenges. *Network* 1, 1 (2021), 28–49.

[5] Sadman Sakib Akash and Md Sadek Ferdous. 2022. A Blockchain Based System for Healthcare Digital Twin. *IEEE Access* (2022).

[6] Sadeq Almeaibed, Saba Al-Rubaye, Antonios Tsourdos, and Nicolas P Avdelidis. 2021. Digital twin analysis to promote safety and security in autonomous vehicles. *IEEE Communications Standards Magazine* 5, 1 (2021), 40–46.

[7] Rashid Amin, Martin Reisslein, and Nadir Shah. 2018. Hybrid SDN networks: A survey of existing approaches. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3259–3306.

[8] Sandro Amofa, Qi Xia, Hu Xia, Isaac Amankona Obiri, Bonsu Adjei-Arthur, Jingcong Yang, and Jianbin Gao. 2024. Blockchain-secure patient Digital Twin in healthcare using smart contracts. *PloS one* 19, 2 (2024), e0286120.

[9] Amir Reza Asadi. 2021. Cognitive Ledger Project: Towards Building Personal Digital Twins Through Cognitive Blockchain. In *2021 2nd International Informatics and Software Engineering Conference (IISEC)*. IEEE, 1–5.

[10] Gagangeet Singh Aujla, Maninderpal Singh, Arnab Bose, Neeraj Kumar, Guangjie Han, and Rajkumar Buyya. 2020. Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications. *IEEE Network* 34, 2 (2020), 83–91.

[11] Denis Avrilionis and Thomas Hardjono. 2021. Towards Blockchain-enabled Open Architectures for Scalable Digital Asset Platforms. *arXiv preprint arXiv:2110.12553* (2021).

[12] baanders. January 18, 2023. What is Azure Digital Twins. https://learn.microsoft.com/en-us/azure/digital-twins/overview.

[13] Jere Backman, Seppo Yrjölä, Kristiina Valtanen, and Olli Mämmelä. 2017. Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. In *2017 Internet of Things Business Models, Users, and Networks*. IEEE, 1–8.

[14] Seyed Mojtaba Hosseini Bamakan and Saeed Banaeian Far. 2024. Distributed and trustworthy digital twin platform based on blockchain and Web3 technologies. *Cyber Security and Applications* (2024), 100064.

[15] Barbara Rita Barricelli, Elena Casiraghi, and Daniela Fogli. 2019. A survey on digital twin: Definitions, characteristics, applications, and design implications. *IEEE access* 7 (2019), 167653–167671.

[16] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Pupo Correia. 2022. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Computing Surveys (CSUR)* 54 (2022), 1 – 41.

[17] Paolo Bellavista, Nicola Bicocchi, Mattia Fogli, Carlo Giannelli, Marco Mamei, and Marco Picone. 2023. Requirements and design patterns for adaptive, autonomous, and context-aware digital twins in industry 4.0 digital factories. *Computers in Industry* 149 (2023), 103918.

[18] Paolo Bellavista, Carlo Giannelli, Marco Mamei, Matteo Mendula, and Marco Picone. 2021. Application-driven network-aware digital twin management in industrial edge environments. *IEEE Transactions on Industrial Informatics* 17, 11 (2021), 7791–7801.

[19] Paolo Bellavista, Carlo Giannelli, Marco Mamei, Matteo Mendula, and Marco Picone. 2022. Digital twin oriented architecture for secure and QoS aware intelligent communications in industrial environments. *Pervasive and Mobile Computing* 85 (2022), 101646.

[20] Juan Benet. 2014. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561* (2014).

[21] Bentley Systems. 2025. iTwin Platform Official Website. https://www.itwinjs.org/. Accessed: 2025-05-05.

[22] Umesh Bodkhe, Dhyey Mehta, Sudeep Tanwar, Pronaya Bhattacharya, Pradeep Kumar Singh, and Wei-Chiang Hong. 2020. A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access* 8 (2020), 54371–54401.

[23] Piotr F Borowski. 2021. Digitization, digital twins, blockchain, and industry 4.0 as elements of management process in enterprises in the energy sector. *Energies* 14, 7 (2021), 1885.

[24] Vincenzo Botta, Laura Fusco, Attilio Mondelli, and Ivan Visconti. 2021. Secure Blockchain-Based Supply Chain Management with Verifiable Digital Twins. *arXiv preprint arXiv:2109.03870* (2021).

[25] Vitalik Buterin et al. 2014. A next-generation smart contract and decentralized application platform. *white paper* 3, 37 (2014), 2–1.

[26] Yinfeng Cao, Jiannong Cao, Zeyang Cui, Dongbin Bai, Mingjin Zhang, and Long Wen. 2024. Polytwin: Edge blockchain-empowered trustworthy digital twin network for metaverse. In *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)*. IEEE, 81–88.

[27] Yasin Celik, Ioan Petri, and Yacine Rezgui. 2021. Leveraging BIM and blockchain for digital twins. In *2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. IEEE, 1–10.

[28] Haoye Chai, Supeng Leng, Jianhua He, Ke Zhang, and Baoyi Cheng. 2021. CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-preserving Authentication in Internet of Vehicles. *IEEE Transactions on Vehicular Technology* (2021).

[29] Pushpita Chatterjee, Debashis Das, Danda B Rawat, Uttam Ghosh, Sourav Banerjee, and Mohammed S Al-Numay. 2024. Digital Twins and Blockchain Fusion for Security in Metaverse-Driven Consumer Supply Chains. *IEEE Transactions on Consumer Electronics* (2024).

[30] Qiuan Chen, Zhenwei Zhu, Shubin Si, and Zhiqiang Cai. 2020. Intelligent maintenance of complex equipment based on blockchain and digital twin technologies. In *2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE, 908–912.

[31] Usman W Chohan. 2021. Non-fungible tokens: Blockchains, scarcity, and value. *Critical Blockchain Research Initiative (CBRI) Working Papers* (2021).

[32] Tudor Cioara, Ionut Anghel, Marcel Antal, Ioan Salomie, Claudia Antal, and Arcas Gabriel Ioan. 2021. An overview of digital twins application domains in smart energy grid. *arXiv preprint arXiv:2104.07904* (2021).

[33] Gordon Clarke, Deon Reynders, and Edwin Wright. 2004. *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes.

[34] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. 2019. Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal* 6, 5 (2019), 8076–8094.

[35] Minghui Dai, Tianshun Wang, Yang Li, Yuan Wu, Liping Qian, and Zhou Su. 2022. Digital Twin Envisioned Secure Air-Ground Integrated Networks: A Blockchain-Based Approach. *IEEE Internet of Things Magazine* 5, 1 (2022), 96–103.

[36] Yueyue Dai, Jian Wu, Shuqi Mao, Xiaoyang Rao, Bruce Gu, Youyang Qu, and Yunlong Lu. 2024. Blockchain empowered access control for digital twin system with attribute-based encryption. *Future Generation Computer Systems* 160 (2024), 564–576.

[37] Lucas Santos Dalenogare, Guilherme Brittes Benitez, Néstor Fabián Ayala, and Alejandro Germán Frank. 2018. The expected contribution of Industry 4.0 technologies for industrial performance. *International Journal of production economics* 204 (2018), 383–394.

[38] William Danilczyk, Yan Lindsay Sun, and Haibo He. 2021. Blockchain Checksum for Establishing Secure Communications for Digital Twin Technology. In *2021 North American Power Symposium (NAPS)*. IEEE, 1–6.

[39] Shoumen Palit Austin Datta. 2016. Emergence of digital twins. *arXiv preprint arXiv:1610.06467* (2016).

[40] Utku Demir, Suyash Pradhan, Richard Kumahia, Debashri Roy, Kaushik Chowdhury, et al. 2023. Digital twins for maintaining QoS in programmable vehicular networks. *IEEE Network* 37, 4 (2023), 208–214.

[41] Marietheres Dietz, Benedikt Putz, and Günther Pernul. 2019. A distributed ledger approach to digital twin secure data sharing. In *Data and Applications Security and Privacy XXXIII: 33rd Annual IFIP WG 11.3 Conference, DBSec 2019, Charleston, SC, USA, July 15–17, 2019, Proceedings 33*. Springer, 281–300.

[42] Md Shezad Dihan, Anwar Islam Akash, Zinat Tasneem, Prangon Das, Sajal Kumar Das, Md Robiul Islam, Md Manirul Islam, Faisal R Badal, Md Firoj Ali, Md Hafiz Ahamed, et al. 2024. Digital twin: Data exploration, architecture, implementation and future. *Heliyon* 10, 5 (2024).

[43] Kai Ding, Liuqun Fan, and Chengxiao He. 2024. Orchestration constraints BlockChained smart contract and integrated digital twins manufacturing systems: ManuChain4. 0-based application paradigm and case study. *Journal of Manufacturing Systems* 74 (2024), 606–632.

[44] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang. 2018. Untangling blockchain: A data processing view of blockchain systems. *IEEE transactions on knowledge and data engineering* 30, 7 (2018), 1366–1385.

[45] Jens Ducrée. 2021. Digital Twin: An Oracle for Efficient Crowdsourcing of Research & Technology Development through Blockchain.

[46] Oussama El Marai, Tarik Taleb, and JaeSeung Song. 2020. Roads infrastructure digital twin: A step toward smarter cities realization. *IEEE Network* 35, 2 (2020), 136–143.

[47] Feruz Elmay, Maha Kadadha, Rabeb Mizouni, Shakti Singh, Hadi Otrok, and Azzam Mourad. 2024. Digital twins and dynamic NFTs for blockchain-based crowdsourced last-mile delivery. *Information Processing & Management* 61, 4 (2024), 103756.

[48] C Fancy, M Anand, and TM Sheeba. 2024. Blockchain for Edge Association in Digital Twin Empowered 6G Networks. *Artificial Intelligence-Enabled Blockchain Technology and Digital Twin for Smart Hospitals* (2024), 123–151.

[49] Aidan Fuller, Zhong Fan, Charles Day, and Chris Barlow. 2020. Digital twin: Enabling technologies, challenges and open research. *IEEE access* 8 (2020), 108952–108971.

[50] Keke Gai, Yue Zhang, Meikang Qiu, and Bhavani Thuraisingham. 2022. Blockchain-Enabled Service Optimizations in Supply Chain Digital Twin. *IEEE Transactions on Services Computing* (2022).

[51] Marisol García-Valls and Alejandro M Chirivella-Ciruelos. 2024. CoTwin: Collaborative improvement of digital twins enabled by blockchain. *Future Generation Computer Systems* 157 (2024), 408–421.

[52] Edward Glaessgen and David Stargel. 2012. The digital twin paradigm for future NASA and US Air Force vehicles. In *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference 20th AIAA/ASME/AHS adaptive structures conference 14th AIAA*. 1818.

[53] Yongkang Gong, Haipeng Yao, Zehui Xiong, CL Philip Chen, and Dusit Niyato. 2024. Blockchain-aided digital twin offloading mechanism in space-air-ground networks. *IEEE Transactions on Mobile Computing* (2024).

[54] Christopher Santi Götz, Patrik Karlsson, and Ibrahim Yitmen. 2020. Exploring applicability, interoperability and integrability of Blockchain-based digital twins for asset life cycle management. *Smart and Sustainable Built Environment* (2020).

[55] Michael Grieves. 2017. Digital twin: manufacturing excellence through virtual factory replication. 2014. *White Paper* (2017).

[56] Daqiang Guo, Shiquan Ling, Hao Li, Di Ao, Tongda Zhang, Yiming Rong, and George Q Huang. 2020. A framework for personalized production based on digital twin, blockchain and additive manufacturing in the context of Industry 4.0. In *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)*. IEEE, 1181–1186.

[57] Mohammad Hammoudeh. 2020. Blockchain, Internet of Things and Digital Twins in Trustless Security of Critical National Infrastructure. In *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*. 1–1.

[58] Dezhi Han, Nannan Pan, and Kuan-Ching Li. 2020. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection. *IEEE Transactions on Dependable and Secure Computing* 19, 1 (2020), 316–327.

[59] Dezhi Han, Yujie Zhu, Dun Li, Wei Liang, Alireza Souri, and Kuan-Ching Li. 2021. A blockchain-based auditable access control system for private data in service-centric IoT environments. *IEEE Transactions on Industrial Informatics* 18, 5 (2021), 3530–3540.

[60] Haya R Hasan, Khaled Salah, Raja Jayaraman, Mohammed Omar, Ibrar Yaqoob, Saša Pesic, Todd Taylor, and Dragan Boscovic. 2020. A blockchain-based approach for the creation of digital twins. *IEEE Access* 8 (2020), 34113–34126.

[61] Dominik Heber, Marco Groll, et al. 2017. Towards a digital twin: How the blockchain can foster E/E-traceability in consideration of model-based systems engineering. In *DS 87-3 Proceedings of the 21st International Conference on Engineering Design (ICED 17) Vol 3: Product, Services and Systems Design, Vancouver, Canada, 21-25.08. 2017*. 321–330.

[62] Ezz El-Din Hemdan and Amged Sayed Abdelmageed Mahmoud. 2021. BlockTwins: a blockchain-based digital twins framework. In *Blockchain Applications in IoT Ecosystem*. Springer, 177–186.

[63] Wahyu Nur Hidayat, Oktafian Sultan Hakim, Sritrusta Sukaridhoto, Muhammad Agus Zainuddin, Agus Prayudi, Cahyo Arissabarno, Zacky Maulana Achmad, and Rizqi Putri Nourma Budiarti. 2024. Digital Twin System for Smart Buildings Integrated with Blockchain and Mixed Reality Technology. In *2024 IEEE International Symposium on Consumer Technology (ISCT)*. IEEE, 339–345.

[64] Ivan Homoliak, Sarad Venugopalan, Daniël Reijsbergen, Qingze Hum, Richard Schumi, and Pawel Szalachowski. 2020. The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Communications Surveys & Tutorials* 23, 1 (2020), 341–390.

[65] Ning Hu, Zhihong Tian, Yanbin Sun, Lihua Yin, Baokang Zhao, Xiaojiang Du, and Nadra Guizani. 2021. Building agile and resilient UAV networks based on SDN and blockchain. *IEEE Network* 35, 1 (2021), 57–63.

[66] Sihan Huang, Guoxin Wang, Yan Yan, and Xiongbing Fang. 2020. Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems* 54 (2020), 361–371.

[67] Jens J Hunhevicz, Mahshid Motie, and Daniel M Hall. 2022. Digital building twins and blockchain for performance-based (smart) contracts. *Automation in Construction* 133 (2022), 103981.

[68] Dmitry Ivanov, Alexandre Dolgui, Ajay Das, and Boris Sokolov. 2019. Digital supply chain twins: Managing the ripple effect, resilience, and disruption risks by data-driven optimization, simulation, and visibility. In *Handbook of ripple effects in the supply chain*. Springer, 309–332.

[69] Jithin Jagannath, Keyvan Ramezanpour, and Anu Jagannath. 2022. Digital Twin Virtualization with Machine Learning for IoT and Beyond 5G Networks: Research Directions for Security and Optimal Control. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning*. 81–86.

[70] Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, et al. 2013. B4: Experience with a globally-deployed software defined WAN. *ACM SIGCOMM Computer Communication Review* 43, 4 (2013), 3–14.

[71] Wenjie Jia, Wei Wang, and Zhenzu Zhang. 2022. From simple digital twin to complex digital twin Part I: A novel modeling method for multi-scale and multi-scenario digital twin. *Advanced Engineering Informatics* 53 (2022), 101706.

[72] Li Jiang, Yi Liu, Hui Tian, Lun Tang, and Shengli Xie. 2024. Resource-efficient federated learning and DAG blockchain with sharding in digital-twin-driven industrial IoT. *IEEE Internet of Things Journal* 11, 10 (2024), 17113–17127.

[73] Li Jiang, Hao Zheng, Hui Tian, Shengli Xie, and Yan Zhang. 2021. Cooperative federated learning and model update verification in blockchain empowered digital twin edge networks. *IEEE Internet of Things Journal* (2021).

[74] Pingyu Jiang, Jiewu Leng, and Kai Ding. 2016. Social manufacturing: a survey of the state-of-the-art and future challenges. In *2016 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. IEEE, 12–17.

[75] Alper Kanak, Niyazi Ugur, and Salih Ergun. 2019. A visionary model on blockchain-based accountability for secure and collaborative digital twin environments. In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*. IEEE, 3512–3517.

[76] Abid Khan, Furqan Shahid, Carsten Maple, Awais Ahmad, and Gwanggil Jeon. 2020. Toward smart manufacturing using spiral digital twin framework and twinchain. *IEEE Transactions on Industrial Informatics* 18, 2 (2020), 1359–1366.

[77] Latif U Khan, Walid Saad, Dusit Niyato, Zhu Han, and Choong Seon Hong. 2022. Digital-twin-enabled 6G: Vision, architectural trends, and future directions. *IEEE Communications Magazine* 60, 1 (2022), 74–80.

[78] Latif Ullah Khan, Walid Saad, Dusit Tao Niyato, Zhu Han, and Choong Seon Hong. 2022. Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions. *IEEE Communications Magazine* 60 (2022), 74–80.

[79] Mehdi Kherbache, Moufida Maimour, and Eric Rondeau. 2021. When Digital Twin Meets Network Softwarization in the Industrial IoT: Real-Time Requirements Case Study. *Sensors* 21, 24 (2021), 8194.

[80] Robert Klar, Niklas Arvidsson, and Vangelis Angelakis. 2023. Digital Twins' Maturity: The Need for Interoperability. *IEEE Systems Journal* 18, 1 (2023), 713–724.

[81] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. 2016. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)*. IEEE, 839–858.

[82] Larissa Krämer, Nick Große, Patrick Stuckmann-Blumenstein, Rico Ahlbäumer, Michael Henke, and Michael ten Hompel. 2022. Designing A Blockchain-Based Digital Twin For Cyber-Physical Production Systems. In *Proceedings of the Conference on Production Systems and Logistics: CPSL 2022*. Hannover: publish-Ing., 141–150.

[83] Randhir Kumar, Ahamed Aljuhani, Danish Javeed, Prabhat Kumar, Shareeful Islam, and AKM Najmul Islam. 2024. Digital twins-enabled zero touch network: A smart contract and explainable AI integrated cybersecurity framework. *Future generation computer systems* 156 (2024), 191–205.

[84] Dongmin Lee, Sang Hyun Lee, Neda Masoud, MS Krishnan, and Victor C Li. 2021. Integrated digital twin and blockchain framework to support accountable information sharing in construction projects. *Automation in construction* 127 (2021), 103688.

[85] Jay Lee, Moslem Azamfar, Jaskaran Singh, and Shahin Siahpour. 2020. Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing. *IET Collaborative Intelligent Manufacturing* 2, 1 (2020), 34–36.

[86] Jay Lee, Moslem Azamfar, Jaskaran Singh, and Shahin Siahpour. 2020. Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing.

[87] Jiewu Leng, Douxi Yan, Qiang Liu, Kailin Xu, J Leon Zhao, Rui Shi, Lijun Wei, Ding Zhang, and Xin Chen. 2019. ManuChain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50, 1 (2019), 182–192.

[88] Dun Li, Noel Crespi, Roberto Minerva, Wei Liang, Kuan-Ching Li, and Joanna Kołodziej. 2025. DPS-IIoT: Non-interactive zero-knowledge proof-inspired access control towards information-centric Industrial Internet of Things. *Computer Communications* 233 (2025), 108065.

[89] Dun Li, Hongzhi Li, Noel Crespi, Roberto Minerva, Ming Li, Wei Liang, and Kuan-Ching Li. 2025. Hyper-IIoT: A Smart Contract-inspired Access Control Scheme for Resource-constrained Industrial Internet of Things. *IEEE Transactions on Sustainable Computing* (2025).

[90] Jiatao Li, Dezhi Han, Shuxin Shi, Xiaoqi Xin, Kuan-Ching Li, and Chin-Chen Chang. 2025. An Active Client Selection Scheme Based on Blockchain for Federated Learning in Shipping. *IEEE Trans. Intell. Transp. Syst.* (2025), 1–16. doi:10.1109/TITS.2025.3591530 Early Access.

[91] Jiatao Li, Dezhi Han, Tien-Hsiung Weng, Huafeng Wu, Kuan-Ching Li, and Arcangelo Castiglione. 2025. A secure data storage and sharing scheme for port supply chain based on blockchain and dynamic searchable encryption. *Comput. Stand. Interfaces* 91 (Jan. 2025). Art. no. 103887.

[92] Ming Li, Yelin Fu, Qiqi Chen, and Ting Qu. 2021. Blockchain-enabled digital twin collaboration platform for heterogeneous socialized manufacturing resource management. *International Journal of Production Research* (2021), 1–21.

[93] Ming Li, Zhi Li, Xidian Huang, and Ting Qu. 2021. Blockchain-based digital twin sharing platform for reconfigurable socialized manufacturing resource integration. *International Journal of Production Economics* 240 (2021), 108223.

[94] Tian Li, Huaqun Wang, Debiao He, and Jia Yu. 2022. Synchronized Provable Data Possession Based on Blockchain for Digital Twin. *IEEE Transactions on Information Forensics and Security* 17 (2022), 472–485.

[95] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2020. A survey on the security of blockchain systems. *Future Generation Computer Systems* 107 (2020), 841–853.

[96] Wei Liang, Yaqin Liu, Ce Yang, Songyou Xie, Kuanching Li, and Willy Susilo. 2024. On identity, transaction, and smart contract privacy on permissioned and permissionless blockchain: a comprehensive survey. *Comput. Surveys* 56, 12 (2024), 1–35.

[97] Siyi Liao, Jun Wu, Ali Kashif Bashir, Wu Yang, Jianhua Li, and Usman Tariq. 2021. Digital twin consensus for blockchain-enabled intelligent transportation systems in smart cities. *IEEE Transactions on Intelligent Transportation Systems* (2021).

[98] Yijing Lin, Zhipeng Gao, Hongyang Du, Dusit Niyato, Jiawen Kang, Zehui Xiong, and Zibin Zheng. 2024. Blockchain-based efficient and trustworthy AIGC services in metaverse. *IEEE Transactions on Services Computing* (2024).

[99] Jiongbin Liu, William Yeoh, Youyang Qu, and Longxiang Gao. [n. d.]. Blockchain-Based Digital Twin for Supply Chain Management: State-of-The-Art Review and Future Research Directions. *Available at SSRN 4113933* ([n. d.]).

[100] Jiongbin Liu, William G. S. Yeoh, Youyang Qu, and Longxiang Gao. 2022. Blockchain-based Digital Twin for Supply Chain Management: A Literature Review and Future Research Directions. *ArXiv* abs/2202.03966 (2022).

[101] Kangde Liu, Zheng Yan, Xueqin Liang, Raimo Kantola, and Chuangyue Hu. 2022. A survey on blockchain-enabled federated learning and its prospects with digital twin. *Digital Communications and Networks* (2022).

[102] Mengnan Liu, Shuiliang Fang, Huiyue Dong, and Cunzhi Xu. 2021. Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems* 58 (2021), 346–361.

[103] Tong Liu, Lun Tang, Weili Wang, Qianbin Chen, and Xiaoping Zeng. 2021. Digital-twin-assisted task offloading based on edge collaboration in the digital twin edge network. *IEEE Internet of Things Journal* 9, 2 (2021), 1427–1444.

[104] Xinlai Liu, Yishuo Jiang, Zicheng Wang, Ray Y Zhong, HH Cheung, and George Q Huang. 2021. imseStudio: blockchain-enabled secure digital twin platform for service manufacturing. *International Journal of Production Research* (2021), 1–20.

[105] Xin Liu, Gongfa Li, Feng Xiang, Bo Tao, and Guozhang Jiang. 2024. Blockchain-based cloud-edge collaborative data management for human-robot collaboration digital twin system. *Journal of Manufacturing Systems* 77 (2024), 228–245.

[106] Javier Lopez, Juan E Rubio, and Cristina Alcaraz. 2021. Digital twins for intelligent authorization in the B5G-enabled smart grid. *IEEE Wireless Communications* 28, 2 (2021), 48–55.

[107] Qiuchen Lu, Zhen Ye, Zigeng Fang, Jiayin Meng, Michael Pitt, Jinyi Lin, Xiang Xie, and Long Chen. 2021. Creating an inter-hospital resilient network for pandemic response based on blockchain and dynamic digital twins. In *2021 Winter Simulation Conference (WSC)*. IEEE, 1–12.

[108] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. 2020. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. *IEEE Internet of Things Journal* 8, 4 (2020), 2276–2288.

[109] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. 2020. Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks. *IEEE Transactions on Industrial Informatics* 17, 7 (2020), 5098–5107.

[110] Yunlong Lu, Sabita Maharjan, and Yan Zhang. 2021. Adaptive edge association for wireless digital twin networks in 6G. *IEEE Internet of Things Journal* 8, 22 (2021), 16219–16230.

[111] Zhihan Lv, Dongliang Chen, Hailin Feng, Amit Kumar Singh, Wei Wei, and Haibin Lv. 2022. Computational intelligence in security of digital twins big graphic data in cyber-physical systems of smart cities. *ACM Transactions on Management Information Systems (TMIS)* 13, 4 (2022), 1–17.

[112] Zhihan Lv, Chen Cheng, and Haibin Lv. 2023. Blockchain-based decentralized learning for security in digital twins. *IEEE Internet of Things Journal* 10, 24 (2023), 21479–21488.

[113] Zhihan Lv, Liang Qiao, Yuxi Li, Yong Yuan, and Fei-Yue Wang. 2022. BlockNet: Beyond reliable spatial Digital Twins to Parallel Metaverse. *Patterns* 3, 5 (2022), 100468.

[114] Claudio Mandolla, Antonio Messeni Petruzzelli, Gianluca Percoco, and Andrea Urbinati. 2019. Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry. *Computers in industry* 109 (2019), 134–152.

[115] Hariprasath Manoharan, Yuvaraja Teekaraman, Ramya Kuppusamy, Naveenkumar Kaliyan, and Amruth Ramesh Thelkar. 2022. Examining the Effect of Cyber Twin and Blockchain Technologies for Industrial Applications Using AI. *Mathematical Problems In Engineering* 2022 (2022).

[116] Xianghui Meng and Lingling Zhu. 2024. Augmenting cybersecurity in smart urban energy systems through IoT and blockchain technology within the Digital Twin framework. *Sustainable Cities and Society* 106 (2024), 105336.

[117] Roberto Minerva and Noel Crespi. 2021. Digital twins: Properties, software frameworks, and application scenarios. *IT Professional* 23, 1 (2021), 51–55.

[118] Roberto Minerva, Gyu Myoung Lee, and Noel Crespi. 2020. Digital twin in the IoT context: a survey on technical features, scenarios, and architectural models. *Proc. IEEE* 108, 10 (2020), 1785–1824.

[119] Roberto Minerva, Gyu Myoung Lee, and Noël Crespi. 2020. Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models. *Proc. IEEE* 108 (2020), 1785–1824.

[120] Mazin Abed Mohammed, Abdullah Lakhan, Karrar Hameed Abdulkareem, Mohd Khanapi Abd Ghani, Haydar Abdulameer Marhoon, Seifedine Kadry, Jan Nedoma, Radek Martinek, and Begonya Garcia Zapirain. 2024. Industrial Internet of Water Things architecture for data standarization based on blockchain and digital twin technology. *Journal of advanced research* 66 (2024), 1–14.

[121] James R. Moyne, Yassine Qamsane, Efe C. Balta, Ilya Kovalenko, John Faris, Kira Barton, and Dawn M. Tilbury. 2020. A Requirements Driven Digital Twin Framework: Specification and Opportunities. *IEEE Access* 8 (2020), 107781–107801.

[122] Nada A Nabeeh, Mohamed Abdel-Basset, Abduallah Gamal, and Victor Chang. 2022. Evaluation of Production of Digital Twins Based on Blockchain Technology. *Electronics* 11, 8 (2022), 1268.

[123] Hossein Naderi and Alireza Shojaei. 2024. Digital twin non-fungible token (DT-NFT): Enabling data ownership in the AEC industry. *Automation in Construction* 168 (2024), 105777.

[124] Hajar Kazemi Naeini, Roya Shomali, Abolhassan Pishahang, Hamidreza Hasanzadeh, Mahdieh Mohammadi, Saeid Asadi, and Ahmad Gholizadeh Lonbar. 2025. PINN-DT: Optimizing Energy Consumption in Smart Building Using Hybrid Physics-Informed Neural Networks and Digital Twin Framework with Blockchain Security. *arXiv preprint arXiv:2503.00331* (2025).

[125] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.

[126] Nawari O Nawari and Shriraam Ravindran. 2019. Blockchain technology and BIM process: review and potential applications. *J. Inf. Technol. Constr.* 24, 12 (2019), 209–238.

[127] Andrey Nechesov, Ivan Dorokhov, and Janne Ruponen. 2025. Virtual Cities: From Digital Twins to Autonomous AI Societies. *IEEE Access* (2025).

[128] Salvador Cuñat Negueroles, Raúl Reinosa Simón, Matilde Julián, Andreu Belsa, Ignacio Lacalle, Raúl S-Julián, and Carlos E Palau. 2024. A Blockchain-based Digital Twin for IoT deployments in logistics and transportation. *Future Generation Computer Systems* 158 (2024), 73–88.

[129] Christian Petersson Nielsen, Elias Ribeiro da Silva, and Fei Yu. 2020. Digital twins and blockchain–proof of concept. *Procedia CIRP* 93 (2020), 251–255.

[130] NVIDIA Corporation. 2025. NVIDIA Omniverse. https://www.nvidia.com/en-us/omniverse/. Accessed: May 5, 2025.

[131] Dominik Oehlschläger, Andreas H Glas, and Michael Eßig. 2024. How digital twins impact responsiveness: a dynamic fit approach to information processing for high-involvement product demand management. *Schmalenbach Journal of Business Research* (2024), 1–46.

[132] Samuel D Okegbile, Jun Cai, Jiayuan Chen, and Changyan Yi. 2024. A reputation-enhanced shard-based byzantine fault-tolerant scheme for secure data sharing in zero trust human digital twin systems. *IEEE Internet of Things Journal* (2024).

[133] Samuel D Okegbile, Jun Cai, Junjie Wu, Jiayuan Chen, and Changyan Yi. 2024. A prediction-enhanced physical-to-virtual twin connectivity framework for human digital twin. *IEEE Transactions on Cognitive Communications and Networking* (2024).

[134] Shahed Otoom. 2025. Risk auditing for Digital Twins in cyber physical systems: A systematic review. *Journal of Cyber Security and Risk Auditing* 2025, 1 (2025), 22–35.

[135] Louis Owusu-Berko. 2025. Advanced supply chain analytics: Leveraging digital twins, IoT and blockchain for resilient, data-driven business operations. (2025).

[136] Giacomo De Panfilis. March 17, 2021. A/RporTWIN: FIWARE powered AR tool created for airport operations. https://www.fiware.org/2021/03/17/a-rportwin-fiware-powered-ar-tool-created-for-airport-operations/.

[137] Yue Pang, Min Zhang, Yidi Wang, Mingzhi Tang, Yao Zhang, Yonghan Wu, Chunyu Zhang, Lifang Zhang, and Danshi Wang. 2024. Blockchain-Enabled Secure and Reliable Management for Digital Components in Digital Twin Optical Network. *Journal of Lightwave Technology* (2024).

[138] Dimitri Petrik and Georg Herzwurm. 2019. iIoT ecosystem development through boundary resources: a Siemens MindSphere case study. In *Proceedings of the 2nd ACM SIGSOFT International Workshop on Software-Intensive Business: Start-Ups, Platforms, and Ecosystems*. 1–6.

[139] Iakovos Pittaras, Nikos Fotiou, Christos Karapapas, Vasilios A Siris, and George C Polyzos. 2024. Secure smart contract-based digital twins for the Internet of Things. *Blockchain: Research and Applications* 5, 1 (2024), 100168.

[140] Benedikt Putz, Marietheres Dietz, Philip Empl, and Günther Pernul. 2021. Ethertwin: Blockchain-based secure digital twin information management. *Information Processing & Management* 58, 1 (2021), 102425.

[141] Qinglin Qi, Fei Tao, Ying Zuo, and Dongming Zhao. 2018. Digital twin service towards smart manufacturing. *Procedia Cirp* 72 (2018), 237–242.

[142] Youyang Qu, Longxiang Gao, Yong Xiang, Shigen Shen, and Shui Yu. 2022. FedTwin: Blockchain-Enabled Adaptive Asynchronous Federated Learning for Digital Twin Networks. *IEEE Network* (2022).

[143] Pethuru Raj. 2021. Empowering digital twins with blockchain. In *Advances in Computers*. Vol. 121. Elsevier, 267–283.

[144] Swarna Priya Ramu, Parimala Boopalan, Quoc-Viet Pham, Praveen Kumar Reddy Maddikunta, Thien Huynh-The, Mamoun Alazab, Thanh Thi Nguyen, and Thippa Reddy Gadekallu. 2022. Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions. *Sustainable Cities and Society* 79 (2022), 103663.

[145] Adil Rasheed, Omer San, and Trond Kvamsdal. 2020. Digital Twin: Values, Challenges and Enablers From a Modeling Perspective. *IEEE Access* 8 (2020), 21980–22012.

[146] Ingrid Carla Reinhardt, Jorge C Oliveira, and Denis T Ring. 2020. Current perspectives on the development of industry 4.0 in the pharmaceutical sector. *Journal of Industrial Information Integration* 18 (2020), 100131.

[147] Christos Roumeliotis, Minas Dasygenis, Vasilis Lazaridis, and Michael Dossis. 2024. Blockchain and Digital Twins in Smart Industry 4.0: The Use Case of Supply Chain-A Review of Integration Techniques and Applications. *Designs* 8, 6 (2024), 105.

[148] Pietro Ruiu, Michele Nitti, Virginia Pilloni, Marinella Cadoni, Enrico Grosso, and Mauro Fadda. 2024. Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction* 8, 6 (2024), 48.

[149] Mamoon Mohammed Ali Saeed, Rashid A Saeed, and Zeinab E Ahmed. 2024. Data security and privacy in the age of AI and digital twins. In *Digital twin technology and AI implementations in future-focused businesses*. IGI Global Scientific Publishing, 99–124.

[150] Radhya Sahal, Saeed H Alsamhi, Kenneth N Brown, Donna O'Shea, and Bader Alouffi. 2022. Blockchain-based digital twins collaboration for smart pandemic alerting: decentralized COVID-19 pandemic alerting use case. *Computational Intelligence and Neuroscience* 2022 (2022).

[151] Radhya Sahal, Saeed H Alsamhi, Kenneth N Brown, Donna O'Shea, Conor McCarthy, and Mohsen Guizani. 2021. Blockchain-empowered digital twins collaboration: smart transportation use case. *Machines* 9, 9 (2021), 193.

[152] Muhammad Bin Saif, Sara Migliorini, and Fausto Spoto. 2024. A Survey on Data Availability in Layer 2 Blockchain Rollups: Open Challenges and Future Improvements. *Future Internet* 16, 9 (2024), 315.

[153] Francesco Sanfilippo. 2019. Digital twin technology in the Industry 4.0 context.

[154] Iqbal H Sarker, Helge Janicke, Ahmad Mohsin, Asif Gill, and Leandros Maglaras. 2024. Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express* (2024).

[155] Ankit Satsangi, Pankaj Dashore, and Rachana Dashore. 2024. Secure Digital Identity Cards With Blockchain and Digital Twins Approach. In *Ensuring Security and End-to-End Visibility Through Blockchain and Digital Twins*. IGI Global, 350–361.

[156] Bassem Sellami, Akram Hakiri, and Sadok Ben Yahia. 2022. Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network. *Future Generation Computer Systems* (2022).

[157] Weidong Shen, Tianliang Hu, Chengrui Zhang, and Songhua Ma. 2021. Secure sharing of big digital twin data for smart manufacturing based on blockchain. *Journal of Manufacturing Systems* 61 (2021), 338–350.

[158] Arpit Shukla, Yagnik Pansuriya, Sudeep Tanwar, Neeraj Kumar, and Md Jalil Piran. 2021. Digital Twin-based Prediction for CNC Machines Inspection using Blockchain for Industry 4.0. In *ICC 2021-IEEE International Conference on Communications*. IEEE, 1–6.

[159] Siemens. 2017. MindSphere: The cloud-based, open IoT operating system for digital transformation. https://new.siemens.com/us/en/company/topic-areas/digitalization/mindsphere/mindsphere-whitepaper-download.html. Accessed: May 5, 2025.

[160] Maulshree Singh, Evert Fuenmayor, Eoin P Hinchy, Yuansong Qiao, Niall Murray, and Declan Devine. 2021. Digital twin: Origin to future. *Applied System Innovation* 4, 2 (2021), 36.

[161] Sachchidanand Singh and Nirmala Singh. 2016. Blockchain: Future of financial and cyber security. In *2016 2nd international conference on contemporary computing and informatics (IC3I)*. IEEE, 463–467.

[162] Giorgia Sirigu, Barbara Carminati, and Elena Ferrari. 2024. Human Digital Twins: Efficient Privacy-Preserving Access Control Through Views Pre-materialisation. In *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 24–43.

[163] Ellis Solaiman and Jorge Robins. 2024. The Internet of Value: Integrating Blockchain and Lightning Network Micropayments for Knowledge Markets. *arXiv preprint arXiv:2412.19384* (2024).

[164] Youngjun Song and Sunghyuck Hong. 2021. Build a Secure Smart City by using Blockchain and Digital Twin. *Int. J. Adv. Sci. Converg* 3 (2021), 9–13.

[165] Maximilian Speicher, Brian D Hall, and Michael Nebeling. 2019. What is mixed reality?. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–15.

[166] Mathis Steichen, Beltran Fiz, Robert Norvill, Wazen Shbair, and Radu State. 2018. Blockchain-based, decentralized access control for IPFS. In *2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData)*. IEEE, 1499–1506.

[167] Sabah Suhail, Rasheed Hussain, Raja Jurdak, and Choong Seon Hong. 2021. Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Computing* (2021).

[168] Sabah Suhail, Rasheed Hussain, Raja Jurdak, Alma Oracevic, Khaled Salah, Choong Seon Hong, and Raimundas Matulevičius. 2021. Blockchain-based digital twins: research trends, issues, and future challenges. *ACM Computing Surveys (CSUR)* (2021).

[169] Sabah Suhail and Raja Jurdak. 2021. Towards trusted and intelligent cyber-physical systems: A security-by-design approach. *arXiv e-prints* (2021), arXiv–2105.

[170] Sabah Suhail and Raja Jurdak. 2021. Towards trusted and intelligent cyber-physical systems: A security-by-design approach. *arXiv e-prints* (2021), arXiv–2105.

[171] Sabah Suhail, Saif Ur Rehman Malik, Raja Jurdak, Rasheed Hussain, Raimundas Matulevičius, and Davor Svetinovic. 2022. Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins. *Computers in Industry* 141 (2022), 103699.

[172] Wen Sun, Peng Wang, Ning Xu, Gaozu Wang, and Yan Zhang. 2021. Dynamic digital twin and distributed incentives for resource allocation in aerial-assisted internet of vehicles. *IEEE Internet of Things Journal* 9, 8 (2021), 5839–5852.

[173] Andy Swales et al. 1999. Open modbus/tcp specification. *Schneider Electric* 29 (1999), 3–19.

[174] Melanie Swan. 2015. *Blockchain: Blueprint for a new economy.* " O'Reilly Media, Inc.".

[175] Chenchen Tan, Xinghao Li, Tom H Luan, Bruce Gu, Youyang Qu, and Longxiang Gao. 2021. Digital twin based remote resource sharing in internet of vehicles using consortium blockchain. In *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 1–6.

[176] Kheng Leong Tan, Chi-Hung Chi, and Kwok-Yan Lam. 2023. Survey on digital sovereignty and identity: from digitization to digitalization. *Comput. Surveys* 56, 3 (2023), 1–36.

[177] Yongyi Tang, Kunlun Wang, Dusit Niyato, Wen Chen, and George K Karagiannidis. 2024. Digital Twin-Assisted Federated Learning with Blockchain in Multi-tier Computing Systems. *arXiv preprint arXiv:2411.02323* (2024).

[178] Fei Tao, He Zhang, Ang Liu, and Andrew YC Nee. 2018. Digital twin in industry: State-of-the-art. *IEEE Transactions on industrial informatics* 15, 4 (2018), 2405–2415.

[179] Fei Tao, Yongping Zhang, Ying Cheng, Jiawei Ren, Dongxu Wang, Qinglin Qi, and Pei Li. 2020. Digital twin and blockchain enhanced smart manufacturing service collaboration and management. *Journal of Manufacturing Systems* (2020).

[180] Benjamin Teisserenc and Samad Sepasgozar. 2021. Adoption of blockchain technology through digital twins in the construction industry 4.0: A pestels approach. *Buildings* 11, 12 (2021), 670.

[181] Benjamin Teisserenc and Samad Sepasgozar. 2021. Project Data Categorization, Adoption Factors, and Non-Functional Requirements for Blockchain Based Digital Twins in the Construction Industry 4.0. *Buildings* 11, 12 (2021), 626.

[182] Benjamin Teisserenc and Samad ME Sepasgozar. 2022. Software Architecture and Non-Fungible Tokens for Digital Twin Decentralized Applications in the Built Environment. *Buildings* 12, 9 (2022), 1447.

[183] Matthias Thürer, Shan Shan Li, and Ting Qu. 2022. Digital twin architecture for production logistics: the critical role of programmable logic controllers (PLCs). *Procedia Computer Science* 200 (2022), 710–717.

[184] Mohamed Torky, Ashraf Darwish, and Aboul Ella Hassanien. 2022. Integrated Digital Twins and Blockchain Framework for Privacy and Security of Applications. In *Digital Twins for Digital Transformation: Innovation in Industry*. Springer, 99–112.

[185] Mehrad Vaezi, Kiana Noroozi, Terence D Todd, Dongmei Zhao, George Karakostas, Huaqing Wu, and Xuemin Shen. 2022. Digital Twins from a Networking Perspective. *IEEE Internet of Things Journal* (2022).

[186] Denis Virovets, Sergiy Obushnyi, Andrii Ramskyi, and Hennadii Hulak. 2024. Soul Bound Token as Digital Twins in Peer-to-Peer Economic Systems. In *Digital Economy Concepts and Technologies Workshop 2024*, Vol. 3665. Germany, 97–105.

[187] Lokendra Vishwakarma, Ankur Nahar, and Debasis Das. 2022. LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-enabled IoV. *IEEE Transactions on Vehicular Technology* (2022).

[188] Chenyu Wang, Zhipeng Cai, and Yingshu Li. 2022. Sustainable Blockchain-based Digital Twin Management Architecture for IoT Devices. *IEEE Internet of Things Journal* (2022).

[189] Chenhao Wang, Yang Ming, Hang Liu, and Yutong Deng. 2025. Dual Fine-Grained Authentication Without Trusted Authority for Data Collection in TDT Systems. *IEEE Transactions on Mobile Computing* (2025).

[190] Chenhao Wang, Yang Ming, Hang Liu, Jie Feng, and Ning Zhang. 2024. Secure and flexible data sharing with dual privacy protection in vehicular digital twin networks. *IEEE Transactions on Intelligent Transportation Systems* (2024).

[191] Dan Wang, Bo Li, Bin Song, Yingjie Liu, Khan Muhammad, and Xiaokang Zhou. 2022. Dual-Driven Resource Management for Sustainable Computing in the Blockchain-Supported Digital Twin IoT. *IEEE Internet of Things Journal* (2022).

[192] Keqi Wang, Wei Xie, Bo Wang, Jinxiang Pei, Wencen Wu, Mike Baker, and Qi Zhou. 2020. Simulation-based digital twin development for blockchain enabled end-to-end industrial hemp supply chain risk management. In *2020 Winter Simulation Conference (WSC)*. IEEE, 3200–3211.

[193] Licheng Wang, Xiaoying Shen, Jing Li, Jun Shao, and Yixian Yang. 2019. Cryptographic primitives in blockchains. *Journal of Network and Computer Applications* 127 (2019), 43–58.

[194] Peng Wang, Ning Xu, Wen Sun, Gaozu Wang, and Yan Zhang. 2021. Distributed incentives and digital twin for resource allocation in air-assisted internet of vehicles. In *2021 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1–6.

[195] Shuai Wang, Liwei Ouyang, Yong Yuan, Xiaochun Ni, Xuan Han, and Fei-Yue Wang. 2019. Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49, 11 (2019), 2266–2277.

[196] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access* 7 (2019), 22328–22370.

[197] Weixi Wang, Xiaoming Li, Linfu Xie, Haibin Lv, and Zhihan Lv. 2021. Unmanned aircraft system airspace structure and safety measures based on spatial digital twins. *IEEE Transactions on Intelligent Transportation Systems* 23, 3 (2021), 2809–2818.

[198] Yin-chuan Wang, Na Zhang, Hongshun Li, and Junjie Cao. 2021. Research on digital twin framework of military large-scale UAV based on cloud computing. In *Journal of Physics: Conference Series*, Vol. 1738. IOP Publishing, 012052.

[199] Jiaqi Wen, Bogdan Gabrys, and Katarzyna Musial. 2022. Toward digital twin oriented modeling of complex networked systems and their dynamics: A comprehensive survey. *Ieee Access* 10 (2022), 66886–66923.

[200] Ming Hui Wen and Jerry Chun-Wei Lin. 2024. Twin3: pluralistic personal digital twins via blockchain. *IEEE Access* (2024).

[201] Jiajing Wu, Dan Lin, Qishuang Fu, Shuo Yang, Ting Chen, Zibin Zheng, and Bowen Song. 2023. Toward understanding asset flows in crypto money laundering through the lenses of Ethereum heists. *IEEE Transactions on Information Forensics and Security* 19 (2023), 1994–2009.

[202] Xichun Yang, Ananda Maiti, Jinhao Jiang, and Alexander Kist. 2021. Forecasting and Monitoring Smart Buildings with the Internet of Things, Digital Twins and Blockchain. In *International Conference on Remote Engineering and Virtual Instrumentation*. Springer,

213–224.

[203] Ibrar Yaqoob, Khaled Salah, Mueen Uddin, Raja Jayaraman, Mohammed Omar, and Muhammad Imran. 2020. Blockchain for digital twins: Recent advances and future research challenges. *IEEE Network* 34, 5 (2020), 290–298.

[204] Abbas Yazdinejad, Reza M Parizi, Ali Dehghantanha, Qi Zhang, and Kim-Kwang Raymond Choo. 2020. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Transactions on Services Computing* 13, 4 (2020), 625–638.

[205] Noe M Yungaicela-Naula, Cesar Vargas-Rosales, Jesús Arturo Pérez-Díaz, and Mahdi Zareei. 2022. Towards security automation in software defined networks. *Computer Communications* 183 (2022), 64–82.

[206] Shah Zeb, Aamir Mahmood, Syed Ali Hassan, MD Jalil Piran, Mikael Gidlund, and Mohsen Guizani. 2022. Industrial digital twins at the nexus of nextG wireless networks and computational intelligence: A survey. *Journal of Network and Computer Applications* (2022), 103309.

[207] Chao Zhang, Guanghui Zhou, Han Li, and Yan Cao. 2020. Manufacturing blockchain of things for the configuration of a data-and knowledge-driven digital twin manufacturing cell. *IEEE Internet of Things Journal* 7, 12 (2020), 11884–11894.

[208] Ke Zhang, Jiayu Cao, Sabita Maharjan, and Yan Zhang. 2021. Digital twin empowered content caching in social-aware vehicular edge networks. *IEEE Transactions on Computational Social Systems* 9, 1 (2021), 239–251.

[209] Shiwen Zhang, Zhixue Li, Wei Liang, Kuan-Ching Li, and Zakirul Alam Bhuiyan. 2024. Blockchain-based hybrid reliable user selection scheme for task allocation in mobile crowd sensing. *IEEE Transactions on Network Science and Engineering* (2024).

[210] Zhongfei Zhang, Ting Qu, George Q Huang, Kuo Zhao, Kai Zhang, Mingxing Li, Yongheng Zhang, Lei Liu, and Haihui Zhong. 2024. Digital twin and blockchain-enabled trusted optimal-state synchronized control approach for distributed smart manufacturing system in social manufacturing. *Journal of Manufacturing Systems* 76 (2024), 385–410.

[211] Zhongfei Zhang, Ting Qu, Kuo Zhao, Kai Zhang, Yongheng Zhang, Wenyou Guo, Lei Liu, and Zefeng Chen. 2024. Enhancing trusted synchronization in open production logistics: A platform framework integrating blockchain and digital twin under social manufacturing. *Advanced Engineering Informatics* 61 (2024), 102404.

[212] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. 2017. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*. Ieee, 557–564.

[213] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. 2020. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems* 105 (2020), 475–491.

[214] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2018. Blockchain challenges and opportunities: A survey. *International journal of web and grid services* 14, 4 (2018), 352–375.

[215] Yuchen Zhu. 2025. Research on evolutionary game of digital twin data information sharing based on blockchain technology. *Measurement and Control* 58, 1 (2025), 24–49.

[216] Weiqin Zou, David Lo, Pavneet Singh Kochhar, Xuan-Bach Dinh Le, Xin Xia, Yang Feng, Zhenyu Chen, and Baowen Xu. 2019. Smart contract development: Challenges and opportunities. *IEEE Transactions on Software Engineering* 47, 10 (2019), 2084–2106.