https://doi.org/10.1038/s40494-025-01818-4

Blockchain in digital cultural heritage resources: technological integration, consensus mechanisms, and future directions

Check for updates

Xinda Liu[1,2], FeiHao Dong[1,2], Wuyang Shui[1] & Guohua Geng[1]

The integration of blockchain technology within the domain of digital cultural heritage resources (DCHR) has emerged as a pivotal approach over the past decade, offering a secure and transparent platform for documentation, ownership transfer, and verification. This paper investigates the current challenges in managing DCHR and analyzes the corresponding solutions. We discuss outstanding technical implementations such as the "Digital Dunhuang Open Material Library" and "Salsal." Our study identifies emerging blockchain trends in cultural heritage preservation and proposes future research directions. Through an analytical examination of distributed consensus mechanisms and blockchain deployment scenarios, this study proposes methodological pathways for implementing the DCHR management framework. We call for continued optimization of consensus protocols, expansion of blockchain application scenarios, and establishment of supportive policies to bridge the gap between decentralized innovation and institutional compliance requirements.

Digital Cultural Heritage Resources constitute a digital resource system formed through the digitization of tangible cultural heritage including artifacts and architectural monuments. These resources play a critical role in cultural heritage preservation, transmission, and dissemination. Stored digitally in cyberspace, DCHR effectively mitigates threats from natural disasters such as earthquakes, floods, and typhoons, as well as human-induced damages including armed conflicts. By digitizing cultural artifacts, these resources ensure that even if physical items are lost or damaged, their digital counterparts remain intact for future generations. This digital preservation fosters a deeper understanding and appreciation of cultural diversity, strengthening the notion of cultural heritage as a shared global asset.

Among emerging digital technologies, blockchain stands out for its transformative potential in the management and conservation of cultural heritage[1]. With its core attributes of decentralization and immutability, the blockchain offers a secure and transparent platform for documenting, owning, and transferring cultural assets. A primary application of blockchain in cultural heritage is verifying data integrity and authenticity certification. By providing an immutable historical record of artifacts, blockchain enhances the reliability of authenticity assessments and prevents forgery. Furthermore, tokenization of cultural assets, driven by innovations such as Non-Fungible Tokens (NFTs)[2,3], facilitates fractional ownership and decentralized stewardship of cultural relics[4]. This process democratizes access to cultural heritage and introduces novel avenues for fundraising and preservation. In addition, blockchain-based digital rights management systems play a critical role in protecting intellectual property associated with digital manifestations of cultural heritage, such as those displayed in digital museums and virtual exhibitions.

Central to blockchain technology is the distributed consensus mechanism, which underpins its effectiveness in cultural heritage management[5]. Consensus mechanisms further validate the authenticity of cultural relics, safeguarding against forgery and unauthorized transactions. Using decentralized storage, blockchain reduces the risk of data loss and theft, ensuring the longevity and accessibility of cultural information[6]. More importantly, the distributed consensus mechanism, built upon decentralized storage, fosters extensive community participation and enables various stakeholders to be deeply involved in the decision-making process. This collaborative approach encourages shared responsibility and cooperation in the preservation and promotion of cultural heritage.

The objective of this study is to investigate the application potential of blockchain technology in the management of DCHR, analyze the pathways for its technical implementation, and propose future development trends and key research directions. To this end, as illustrated in Fig. 1, this article is

[1]School of Information Science and Technology, Northwest University, Xi'an, Shaanxi, China. [2]These authors contributed equally: Xinda Liu, FeiHao Dong.
e-mail: ghgeng@nwu.edu.cn

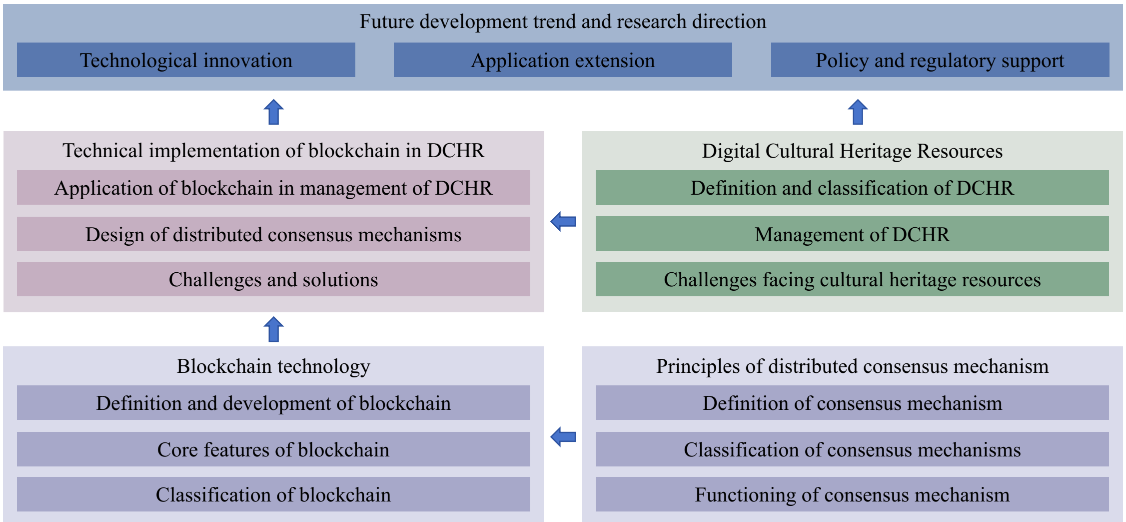
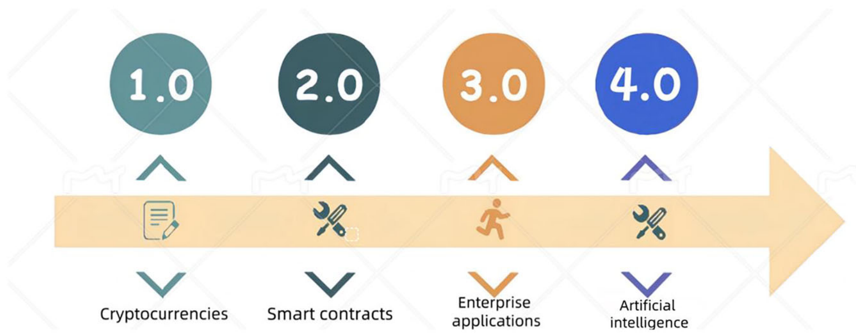


Fig. 1 | Article structure.

Fig. 2 | The development history of blockchain.



structured as follows: First, it presents an overview of the fundamental concepts and characteristics of blockchain technology, DCHR, and consensus mechanisms. Second, it explores in depth the technical implementation of blockchain in the management of cultural heritage resources. Finally, it examines the future development trends in this domain and proposes key research directions to advance the application of blockchain in the management of cultural heritage resources.

Through our research, multiple dimensions of the cultural heritage domain will be impacted. Economically, we propose constructing a blockchain and digital twin-driven assetization platform to explore NFT-based ownership authentication and global Intellectual Property (IP) derivative development. Smart contracts enable automated revenue reinvestment into conservation initiatives, establishing a "conservation-value-added-reconservation" closed-loop system. Technologically, we integrate blockchain, AI-driven restoration algorithms, and cross-chain protocols to address digitization precision and data silos, while promoting international standardization of metadata and smart contract frameworks. Policymaking, we design cross-border data circulation and tax incentive frameworks, advocating blockchain-enabled multinational collaborative governance alliances to enhance copyright authentication and illicit circulation tracking. Educationally, we develop globally accessible high-precision digital resource repositories and Virtual Reality (VR)/Decentralized Autonomous Organization (DAO)-based immersive tools to foster interdisciplinary research and cultivate technically skilled professionals. This tripartite model-leveraging technological empowerment, policy guidance, and educational innovation-provides a sustainable digital transformation pathway for cultural heritage, offering academically rigorous and practically viable solutions for global heritage revitalization.

Blockchain technology overview

Blockchain technology, as a rapidly evolving form of distributed ledger technology, is distinguished by its multiple core characteristics and extensive range of classifications. These features enable different types of blockchains to be uniquely adaptable to a broad spectrum of application scenarios.

Blockchain evolution

Each block comprises transaction records and is cryptographically linked to the preceding block, thereby forming an ever-expanding chain structure that epitomizes the genesis of blockchain technology. This structure enhances data transparency while enabling decentralized verification and transactions, thus obviating the need for a central authority.

Since its introduction by Satoshi Nakamoto in 2008 as the underlying technology for Bitcoin[7], blockchain has evolved through several stages, as depicted in Fig. 2. Initially, Blockchain 1.0 focused on cryptocurrencies and payment systems. The emergence of Blockchain 2.0[8] introduced platforms like Ethereum, enabling smart contracts and expanding blockchain's use in the financial sector. Blockchain 3.0[9] extended its applications beyond finance, encompassing sectors such as supply chain management and identity verification. Current developments signal the advent of Blockchain 4.0, integrating advanced features such as artificial intelligence and the Internet of Things.

This technological progression has garnered global attention, particularly in China, where the blockchain industry has seen steady growth and innovation. Despite a contraction in the industry size to approximately 6 billion RMB by 2023, the number of blockchain-related enterprises continues to rise, indicating robust interest and demand[10]. Notably, China has introduced national blockchain standards, setting guidelines for the industry's healthy development. Additionally, blockchain is increasingly integrated with the digital economy, Web3.0, and data assets, driving new breakthroughs and innovative applications.

Blockchain mechanisms

Blockchain is characterized by three core attributes: immutability[11], decentralization, and a high degree of transparency and security.

Immutability[12,13] ensures that once data is recorded on the blockchain, it cannot be altered or deleted. This is facilitated by the distributed ledger structure, where each block contains the hash of the previous block[12], forming an irreversible chain. Any attempt to modify the data would disrupt the hash value, causing a mismatch with subsequent blocks and triggering rejection by other network nodes[14]. This mechanism guarantees data integrity and security, making blockchain an ideal platform for transaction record storage and verification[15].

Decentralization[16,17] refers to the distribution of data across multiple nodes, eliminating a central control point[18]. This architecture enhances the network's resilience and attack resistance, as no single node can control or alter the system's operation. This mechanism enhances decentralized governance by granting transaction verification, ledger maintenance, and consensus participation rights to all nodes in public blockchains or authorized entities (e.g., cultural heritage institutions, regulatory agencies) in private/consortium chains[19]. Tampering with or gaining control of the network would require altering the majority of nodes, a task that is practically infeasible, thereby strengthening the network's security and trust[20].

Blockchain's distributed ledger structure provides a high level of transparency[21,22] and security[23,24]. Any alteration to a block within a blockchain will invalidate its hash value and will subsequently be detected and rejected by other nodes via the consensus mechanism. Additionally, blockchain's transparency ensures that all transaction records are visible to network participants, fostering trust and accountability, though encryption may be used to protect user privacy[25,26]. In conclusion, the characteristics of blockchain render it a potent tool for secure and transparent data management[27], with broad application prospects across various domains, including the management of Digital Cultural Heritage Resources (DCHR).

Classification of blockchain

Blockchain can be classified into three types based on access permissions and control mechanisms: public blockchains, private blockchains, and consortium blockchains[28]. Public blockchains are characterized by decentralization and transparency, as they enable anyone to participate in transactions and consensus processes. For instance, the "History_Memory_and_Identity" NFT collection employs blockchain technology to transform five Ukrainian cultural heritage sites damaged during the war-including the Holy Dormition Sviatohirsk Lavra and the Donetsk Drama Theater-into digital assets[29]. By integrating on-chain smart contracts with off-chain storage solutions like IPFS/Arweave, this collection ensures transparent ownership verification and persistent data integrity while enabling unrestricted participation in NFT transactions for all users (buyers and sellers alike). This blockchain-based distributed digital repository achieves comprehensive verifiability and full lifecycle traceability of cultural artifact information. Furthermore, the framework constructed through smart contracts establishes an immutable trust anchor for authenticity certification, providing a reliable foundation for the valuation of cultural assets.

Private blockchain, on the other hand, offers a controlled environment where write permissions are typically restricted to internal organizational entities, while read access can be configured as public or limited to authorized parties. In the context of DCHR management, as exemplified by the Byzantine Fresco case involving the Church of Cyprus and the Byzantine Fresco Foundation, private blockchain enables stringent control over critical data integrity[30]. Write permissions can be confined to protocol-bound stakeholders such as ownership entities, museums, and conservation institutions, ensuring that modifications to ownership records, exhibition timelines, or restoration milestones remain tamper-proof and exclusively managed by authorized participants. Read access, meanwhile, may be partially publicized to disseminate provenance details to broader audiences or selectively shared with collaborators to facilitate transparency in restoration progress. This framework safeguards sensitive transactional and contractual data while leveraging distributed ledger technology to establish verifiable, immutable records of multilateral agreements. Such an approach enhances the efficiency of cross-border cultural heritage stewardship by balancing confidentiality with collaborative accountability.

The application of consortium blockchains in the cultural heritage domain exemplifies their capacity to balance control and collaborative openness. For instance, the Florence Museum Consortium employs a consortium blockchain to establish a distributed ledger, where pre-selected authorized nodes jointly manage records of artwork loans[31]. This framework ensures data privacy-sensitive information, such as transportation conditions and certificates, remains accessible only to participating institutions-while enabling cross-institutional interoperability through multi-node consensus mechanisms, significantly enhancing the circulation efficiency of artworks. Compared to the closed architecture of private blockchains, consortium blockchains offer dynamic permission configurations, allowing flexible adjustment of data access levels across institutions. In contrast to fully open public blockchains, their access control mechanisms, as seen in UNESCO's intangible heritage projects that restrict node participation to authenticated cultural institutions and heritage custodians, reduce system complexity while ensuring transparency, security, and immutability of on-chain data, including intangible heritage documentation and artifact restoration records. This semi-open architecture preserves stakeholder control in multi-party cultural heritage collaborations while achieving cross-chain data interoperability through standardized interfaces, establishing a technical foundation for trusted sharing of digital cultural heritage resources.

Blockchain's technical evolution and core mechanisms, such as cryptographic chaining and smart contracts, underpin DCHR preservation frameworks, as evidenced by initiatives like Digital Dunhuang. However, inherent tensions between blockchain's immutability and openness and cultural heritage's dynamic and regulated nature necessitate a systematic analysis of implementation challenges. The following section dissects these technology-institution paradoxes to inform adaptive governance solutions.

DCHR management challenges

DCHR, as a cornerstone of modern cultural heritage preservation, has significantly impacted the field through digital transformation. Techniques such as high-precision scanning, photography, and 3D modeling[32] facilitate the accurate capture of cultural relics and their conversion into digital formats. This provides robust technical support for restoration and conservation efforts while offering researchers and enthusiasts global access to study and appreciate cultural heritage across time and space. By displaying DCHR on online platforms, individuals worldwide can engage with cultural heritage, enhancing public awareness and fostering a greater appreciation for its value and protection.

However, the management of DCHR presents several challenges. First, the high costs and technical demands of digitization place a significant burden on cultural institutions. Second, the large volume of digital data requires extensive storage, and as the data grows, issues related to storage, backup, and migration must be addressed. Additionally, ensuring data security to prevent loss, damage, or unauthorized access is critical to safeguarding digital resources. Moreover, the clarification of copyright and intellectual property rights[33] is necessary to ensure that DCHR can be shared and used responsibly without infringing on creators' rights.

To overcome these challenges, it is essential to develop comprehensive digitization strategies and standards, adopt advanced data management technologies, and strengthen legal frameworks. These measures will ensure the sustainability and effectiveness of DCHR, maximizing its value for the preservation and promotion of cultural heritage.

DCHR ontological taxonomy

DCHR, as the digital representation of physical cultural artifacts, can be primarily categorized into two major types: high-fidelity digital replicas[34]

Table 1 | Classification of digital cultural heritage resources

Category	Definition
Ontological digital resources	Data that directly represents the visual and structural attributes of cultural artifacts, including appearance, shape, and extent of physical damage.
Descriptive digital resources	Data capturing the physical characteristics of cultural artifacts, such as name, age, material composition, size, and other identifying properties.
Interpretative digital resources	Data facilitating the scientific, cultural, and artistic interpretation of artifacts, emphasizing archeological, historical, and contextual significance.
Derived digital resources	Data reconstructed or recontextualized from descriptive and interpretative resources, including digital collections, virtual reconstructions, and cultural games.
Management digital resources	Data produced by cultural institutions during the administration of cultural artifacts, such as cataloging identifiers, locations, acquisition dates, and storage details.

and metadata along with related information resources[35]. High-fidelity digital replicas employ techniques such as high-resolution photography, 3D[36] laser scanning, and CT scanning to capture the shape, color, texture, and material properties of cultural relics, creating digital representations that closely resemble the originals. These replicas are vital for research, education, exhibition, and restoration, offering access to users unable to physically interact with the artifacts. In contrast, metadata and related information resources encompass detailed data on the historical context, provenance, age, artistic style, and cultural significance of relics, as well as digital catalogs, exhibition records, scholarly articles, and multimedia content. This information is crucial for managing and deepening the understanding of cultural relics. Together, these two resource types form a comprehensive DCHR system, enhancing preservation, research, exhibition, and educational initiatives related to cultural heritage.

In addition to these categories, DCHR can be further classified into five primary types, as shown in Table 1: ontological digital resources, descriptive digital resources, interpretive digital resources, derivative digital resources, and managerial digital resources. While these classification methods differ in approach, the underlying nature of DCHR remains consistent.

Management of DCHR

The management of converting cultural heritage resources into DCHR encompasses three sequential phases: digitization, storage and preservation, and access and dissemination[37]. The digitization stage involves transforming non-digital cultural relics-such as text, images, audio, and video-into digital formats for computational processing and storage, exemplified by UNESCO's use of the Polycam mobile application during the Ukraine conflict to perform millimeter-level 3D scanning of endangered heritage sites. The storage and preservation phase focuses on securing digital assets through databases, cloud systems, or blockchain-based distributed storage, while systematically recording metadata about historical context and conservation status. Notably, UNESCO's cloud-based digital archive combined blockchain certification to create dynamic, permanently preserved digital assets. Finally, the access and dissemination phase shares resources via platforms like virtual museums and real-time collaborative systems, as seen in Ukraine's multinational restoration efforts through cloud-based tools. This integrated approach, merging preventive digitization with crisis-responsive technologies, demonstrates how physical cultural memory evolves into interactive DCHR, ensuring global accessibility and resilience against threats.

This three-phase framework has boosted cultural heritage preservation and global access but introduces risks through its reliance on cloud systems, data sharing, and decentralized storage. As institutions shift from physical to digital stewardship, they must balance technological advantages with robust vulnerability management.

Challenges facing DCHR

The primary challenges confronting DCHR can be broadly categorized into two major domains: data security and the efficiency of resource sharing and utilization. Data security encompasses issues such as data authentication and privacy protection.

Data authentication is critical in the digital cultural heritage field, as verifying the authenticity and provenance of digital cultural relics is essential. Issues such as forgeries or misattribution can undermine the reliability of digital resources. Blockchain technology, with its decentralized, irreversible, and transparent features, offers a reliable solution for data authentication[38]. By encrypting and storing critical information, including historical records of cultural relics, on the blockchain, it ensures that once recorded, this data is immutable. This aligns with the blockchain-based cultural relics management system proposed by Wang et al., which leverages smart contracts to automate authorization workflows and establish immutable audit trails, effectively addressing inefficiencies in traditional offline operations[39]. Furthermore, smart contracts can automate processes such as cultural relic transactions and verification, enhancing both efficiency and security. However, challenges remain in ensuring data accuracy before uploading to the blockchain, aligning with existing protection regulations, and addressing privacy and intellectual property concerns.

To systematically address these challenges, recent advancements establish dual-validation frameworks. First, cryptographic-Physical Unclonable Function (PUF, a security technology that generates unique digital fingerprints based on inherent hardware physical characteristics)[40] architectures enable data provenance assurance through blockchain-interfaced Internet of Things (IoT) devices, generating timestamped 3D models-demonstrated in the Digital Dunhuang Project's digitization pipeline. Second, blockchain-based metadata encapsulation automates IP management via smart contracts encoding copyright constraints and royalty distribution. This bimodal approach resolves pre-upload authentication issues while establishing regulatory-compliant governance for cross-border DCHR collaborations.

In terms of privacy protection[41,42], the key challenge lies in balancing transparency with privacy when dealing with sensitive or personal information related to cultural heritage. Given the immutable nature of blockchain, this necessitates stringent controls at the data input stage. To address these challenges, advanced encryption techniques, refined access control mechanisms, and the standardization of input data formats are required. Existing blockchain systems, such as Salsal[43] and Mapp[44], have demonstrated notable achievements in these aspects.

Blockchain can provide a decentralized platform for cultural heritage institutions and researchers to securely share and access cultural heritage data. However, this also introduces issues such as ensuring equitable resource sharing, preventing misuse, and balancing the interests of various stakeholders. Depending on the use case and the interests of the users, employing an appropriate distributed consensus mechanism can effectively address these issues. The following sections will analyze and discuss several classic consensus mechanisms.

Consensus mechanism principles

The consensus mechanism is a fundamental component of blockchain technology, ensuring that all nodes in the network reach agreement on the state of the data[45]. This chapter provides an overview of distributed consensus mechanisms, beginning with their definition, followed by a

Table 2 | Classification of consensus mechanisms

Type	Features and applications
PoW (Proof of Work)	- PoW achieves decentralized consensus in trustless networks through computational puzzles, preventing double-spending and Sybil attacks via economic cost[51].
	- The PoW proposed in this study enhances transaction throughput (60 TPS) while improving security by optimizing network parameters (e.g., block size and propagation mechanisms), effectively reducing orphan rates to mitigate double-spending and selfish mining attacks[81].
	- The evaluation framework proposed in this study reveals that PoW consensus protocols suffer from fundamental flaws in information asymmetry and the "reward-punishment dilemma," which prevent them from achieving complete resistance against attacks[50].
PoS (Proof of Stake)	- PoS selects validators based on stake ownership, ensuring security, decentralization, and operational efficiency while demonstrating significantly lower energy consumption compared to PoW. This approach enables rapid transaction finality and exhibits broad applicability in diverse application scenarios including IoT and vehicular networks[53].
	- This study proposes an enhanced PoS that integrates behavioral credit and credit rating systems with coin age to achieve more equitable reward distribution while mitigating centralization in blockchain networks[54].
PoA (Proof of Authority)	- PoA is a validator-based consensus algorithm that prioritizes efficiency and scalability over full decentralization by relying on trusted nodes, making it ideal for private or consortium blockchains[82].
	- Cobe's CPoA consensus protocol employs multi-dimensional node selection criteria and privacy-enhancing cryptographic techniques to optimize efficiency while ensuring robust security and confidentiality in permissioned blockchain systems[83].
	- PoA achieves efficient and low-energy decision-making through an identity-reputation mechanism, integrating authoritative node rotation and fuzzy logic-based expertise quantification to ensure security and transparency, making it suitable for collaborative decision-making scenarios[55].
BFT (Byzantine Fault Tolerance)	- BFT enhance the fault tolerance, security, and performance of distributed systems through methods such as grouping/hierarchical structures, multi-leader schemes, optimistic speculation, and trusted hardware, ensuring consensus among nodes even in the presence of Byzantine faults[84].
	- RBFT (Reputation-based Byzantine Fault Tolerance) is a Byzantine fault-tolerant consensus algorithm incorporating a reputation model, which dynamically adjusts node weights and optimizes primary node selection to enhance both the performance and security of consortium blockchains[85].
	- D-SBFT (Dynamic Scalable Byzantine Fault Tolerance) is an extensible Byzantine fault-tolerant protocol that supports dynamic node management, enhancing the flexibility and robustness of consortium blockchains through DKG (Distributed Key Generation) and BLS (Boneh-Lynn-Shacham) signature technologies[86].

discussion of the various types, and a detailed explanation of their operation within blockchain networks.

Definition of consensus mechanism

Blockchain's core features of decentralization and cryptographic chaining enable distributed nodes to achieve consensus without central authority[46], maintaining system consistency against malicious actors or faults. These mechanisms are characterized by security, liveness, and fault tolerance. Security[47,48] ensures data integrity by preventing tampering, while liveness incentivizes participation and maintains continuous network operation. Fault tolerance[49] ensures consensus can be achieved despite disruptions. Together, they form the basis for secure and efficient decentralized blockchain operations.

Classification of consensus mechanisms

Various consensus mechanisms are depoloyed in blockchain systems, with their primary classifications presented in Table 2. A particularly significant algorithm is Byzantine Fault Tolerance (BFT), which mitigates the impact of faulty nodes on system integrity. This section also introduces other consensus mechanisms, including Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Authority (PoA).

PoW[50]requires solving complex puzzles to validate transactions, offering robust security and decentralization. However, it faces high energy consumption, limited scalability, and potential centralization due to large mining pools[51]. It is also vulnerable to attacks like selfish mining and double spending[52]. The inherent characteristics of PoW exhibit fundamental incompatibility with DCHR application scenarios, while demonstrating operational viability in consensus operations for specific financial systems such as Bitcoin. This limitation is primarily attributable to dual constraints: structural deficiencies in its security architecture and disproportionately high energy expenditure inherent to the protocol design.

PoS[53] selects delegate nodes based on cryptocurrency holdings, improving energy efficiency and transaction speed. However, it is susceptible to "nothing-at-stake" attacks and potential manipulation by wealthy stakeholders[54]. PoS inherently centralizes the authority to validate transactions and generate new blocks among the most resource-endowed nodes. While this characteristic renders it suitable for NFT copyright systems, within DCHR systems, the centralization of power not only violates the principle of equitable stakeholder participation but may also lead to systemic failures due to targeted attacks on dominant nodes. Certainly, the partial adoption of PoS constitutes a viable approach for DCHR systems incorporating NFT transaction modules.

PoA[55] mechanism predicates block creation on validator identity and reputation, enhancing operational efficiency while reducing energy expenditure. However, this consensus architecture introduces centralization vulnerabilities, as system integrity becomes dependent on privileged validators[56]. Consequently, PoA demonstrates incompatibility with permissionless, egalitarian distributed DCHR architectures, whereas it exhibits implementation viability in centralized DCHR frameworks requiring trusted validators.

BFT[57] achieves consensus through voting and filtering, tolerating up to one-third malicious nodes. While effective for reliability, it incurs performance overhead and requires additional resources[58]. While BFT remains applicable to DCHR systems, efficiency considerations necessitate introducing consensus mechanisms better aligned with DCHR's operational requirements.

Beyond these mechanisms, Raft consensus algorithm[59] offers an alternative. Raft achieves high-efficiency consensus in blockchain systems through a tri-phase mechanism encompassing leader election, log replication, and safety guarantees. Its core operational workflow comprises: 1) Leader election triggered by heartbeat timeouts, where a unique leader is elected via majority voting among nodes; 2) Log replication whereby the leader encapsulates transaction data into sequentially ordered log entries, broadcasts them for synchronization, and commits entries to the state machine after majority acknowledgment to ensure strong consistency; 3) Safety assurance through log index verification, term constraints, and fault tolerance mechanisms (tolerating up to (N-1)/2 node failures, where N is the total number of nodes in the system). Compared to Byzantine Fault Tolerance (BFT) protocols, Raft demonstrates significantly enhanced throughput efficiency, making it particularly suitable for DCHR systems requiring deterministic coordination under trusted node assumptions.

For DCHR systems requiring centralized authority, the conventional Raft consensus algorithm proves suboptimal. To address this limitation, we propose an enhanced Raft algorithm. Prior to system initialization, a predefined leader node is established to govern blockchain operations. In the event of a predefined leader node failure, a leader election mechanism is triggered to select a new leader for system continuity. However, upon recovery of the predefined leader node, transaction validation and block generation authority are automatically restored to it. The enhanced Raft algorithm effectively addresses the single point of failure issue through election mechanism, significantly improving system security compared to the PoA algorithm, where the failure of an authoritative node can lead to a complete breakdown of the blockchain system. However, a critical limitation remains: if the predefined nodes suffer sustained attacks, they cannot recover their transaction validation and block generation privileges, which conflicts with application scenarios requiring stable centralized governance. Nevertheless, compared to PoA and traditional Raft algorithms, the enhanced Raft algorithm remains more suitable for DCHR systems that necessitate centralized administration.

Functioning of consensus mechanism

In blockchain systems, consensus mechanisms play a pivotal role in transaction verification and in ensuring the irreversibility and consistency of transactions. By coordinating distributed nodes to achieve consensus on data integrity, these mechanisms effectively mitigate fraudulent activities such as double-spending, thereby enhancing system security and trustworthiness[60]. Concurrently, these mechanisms maintain network stability through collective verification of transactions and blocks[61]. The decentralization of data storage and decision-making authority across network nodes significantly reinforces the system's decentralization capabilities. Smart contracts, deployed as codified protocols on the blockchain, automatically execute upon meeting predefined conditions. Their synergistic operation with consensus mechanisms substantially improves the operational efficiency of blockchain systems. The selection of consensus mechanisms must align with specific application scenarios and adapt to the functional requirements of system architectures. For instance, sharding-based consensus is suitable for high-concurrency environments, while Byzantine Fault Tolerance (BFT) mechanisms are essential in scenarios with low node trustworthiness.

Blockchain implementation in DCHR

The application of blockchain technology in the management of DCHR ensures the security and authenticity of these resources. To systematically evaluate blockchain's technical potential and implementation challenges in real-world scenarios, this section adopts a case study methodology. Case studies are particularly suited for exploring complex socio-technical systems like DCHR management, as they allow for in-depth analysis of contextual factors, stakeholder interactions, and systemic outcomes. By examining practical implementations, we bridge theoretical frameworks with empirical evidence, addressing our core research question: How can blockchain technology overcome institutional and technical barriers to enhance DCHR governance?

Blockchain for DCHR management

The application of blockchain technology in the management of DCHR ensures the security and authenticity of these resources. This section selects case studies based on three criteria: (1) data accessibility and technical validation, (2) institutional alignment with global preservation frameworks, and (3) demonstrable socio-economic impacts. The Digital Dunhuang Open Material Library is prioritized for its large-scale blockchain deployment (6500+ HD resources) and UNESCO-recognized governance model (Asia-Pacific Innovation Case Repository, 2023), which provides open-access empirical data for analyzing interoperability and stakeholder collaboration. Salsal is included for its Ethereum-based NFT authentication system that resolves ethical ambiguities in artifact curation through transparent metadata updates, while Heirloom exemplifies blockchain's role in mitigating funding shortages via IPFS-backed NFT tokenization of endangered heritage. MApp is chosen for addressing art forgery through role-based access control in minor artwork documentation, and BMDRM demonstrates decentralized copyright management via smart contract-driven authorization models. The MAXP platform is highlighted for its secure artifact exchange protocols enabling cross-border museum collaboration, and HeriLedger illustrates energy-efficient consensus mechanisms fostering collaborative preservation-tourism synergies. These cases collectively validate blockchain's capacity to balance technical innovation with institutional needs across diverse DCHR scenarios.

Digital Dunhuang open library: a case study. On December 8, 2022, under the guidance of the National Cultural Heritage Administration's "Internet + Chinese Civilization" action plan, the Dunhuang Research Institute, in collaboration with Tencent, launched the world's first blockchain-based open sharing platform for digital cultural heritage, the "Digital Dunhuang Open Material Library." This platform made available over 6500 high-definition digital resources, including materials from the Mogao Grottoes and Dunhuang Cave Temple Library, to a global audience. The initiative aims to provide scholars, cultural enthusiasts, and artists with a collaborative platform for sharing and co-creating Dunhuang cultural resources. Moreover, it establishes a secure, efficient foundation for the flow of cultural assets, supports accurate traditional cultural dissemination, and facilitates the management of digital rights, thus enhancing the social accessibility and interactive engagement between the Dunhuang Research Institute and the public.

The Digital Dunhuang project, through collaborations with enterprises such as Huawei and Bilibili, has developed over 60 cultural derivative products and 30 digital exhibitions, attracting 22 million visits from 78 countries and generating nearly 100 million RMB in revenue. Its blockchain technical standards have been adopted by 22 cultural heritage institutions across 9 Chinese provinces and municipalities, and were included in the UNESCO Asia-Pacific Cultural Heritage Innovation Case Repository (2023). This initiative validates blockchain's core value in reconstructing cultural heritage governance: ensuring resource authenticity through smart contracts and open ecosystems while fostering innovation, thereby shifting preservation paradigms from passive conservation to active revitalization. Emerging blockchain-based cultural asset exchanges are accelerating the establishment of a digital rights and virtual entitlements trading market for cultural relics, projected to exceed 1 billion RMB by 2030. This combination of reliable technology and financial benefits is transforming industries along the Silk Road cultural economic belt, creating a balanced system that protects heritage while also supporting its commercial value.

Cultural heritage blockchain platform. The application of blockchain technology in cultural heritage has been widely explored, demonstrating substantial potential in areas such as preservation, copyright management, and museum applications (see Table 3).

• Preservation of cultural heritage

Blockchain solutions enhance artifact authentication and funding mechanisms. The Salsal platform leverages Ethereum-based smart contracts and NFTs to transparently update collection metadata, resolving ethical ambiguities in artifact curation by incentivizing stakeholders to maintain accurate records. Recent studies further validate blockchain's adaptability to dynamic conservation scenarios, with proposing a traceability framework tailored for mobile artifacts through decentralized consensus and role-based access control[62]. For instance, the integration of blockchain with IoT in cultural relic transportation systems has demonstrated significant advancements in real-time monitoring and risk prevention. A study by Zhang introduced a blockchain-IoT transport monitoring system that

Table 3 | Technological platform for cultural heritage based on blockchain technology

Type	Relevant achievements
Preservation of cultural relics	- Salsal leverages the use of NFTs and smart contracts to authenticate and track cultural artifact collections, thereby addressing the ethical and legal challenges present in modern cultural artifact curation[43].
	- Heirloom, by utilizing NFTs and InterPlanetary File System (IPFS), has mitigated the risk of extinction or damage to cultural heritage due to lack of promotion and funding[64].
	- MApp, by integrating blockchain technology with IPFS, has addressed the challenges of protecting, documenting, and verifying minor artworks, including issues such as art forgery and the loss and tampering of art information[44].
Management of copyrights	- BMDRM has resolved issues such as centralized authorization, lack of transparency in transaction information, and risks of data tampering in traditional digital copyright management by introducing NFTs and smart contracts[66].
	- The Bitcoin blockchain supports a decentralized service that automatically adds trustworthy timestamps to digital content. This helps protect online cultural heritage from being changed or edited secretly, making it easier to spot and track any changes made later[67].
Application within museum contexts	- MAXP has addressed the security risks associated with the online exchange of digital museum collections by constructing a digital artifact exchange system[65].
	- A traceable one-time address scheme, by integrating blockchain technology, has resolved the contradiction between user anonymity and regulatory requirements in the interaction of digital museum assets. It protects user privacy while allowing regulators to effectively track and oversee transactions[8].
	- Combining BIM, IoT, and blockchain technology has created a smart museum system to help with challenges like protecting exhibits, monitoring the environment, improving visitor experiences, and managing security. This system uses the best features of each technology to meet the needs of today's museums[68].

tracks environmental variables (e.g., temperature, GPS location) and ensures data immutability, effectively safeguarding relics during transit while enabling dynamic remote management[63]. Similarly, Heirloom[64] employs NFTs to tokenize cultural assets, channeling preservation funds while utilizing InterPlanetary File System (IPFS)[65] for decentralized metadata storage-a critical mitigation against heritage loss due to financial constraints. For minor artworks susceptible to forgery, MApp integrates role-based access control (users, publishers, verifiers) with IPFS-backed blockchain architecture, ensuring tamper-proof documentation. These systems collectively address centralized data control and funding gaps inherent in traditional methods.

However, the ethical implications of blockchain adoption in cultural heritage demand critical scrutiny. While decentralization could empower marginalized communities to engage in heritage authentication, technical barriers like coding literacy and infrastructure access may still exclude them. Additionally, blockchain's immutability risks freezing heritage narratives, potentially suppressing dynamic or contested interpretations. Future implementations must adopt inclusive design to ensure decentralized technologies do not reinforce existing power imbalances under the guise of technological neutrality.

• Copyright management

Decentralized frameworks disrupt conventional digital rights management. BMDRM replaces centralized authorization models with NFT-driven smart contracts, eliminating opacity and tampering risks in transaction records[66]. Complementary to this, Bitcoin's blockchain provides immutable timestamping services for digital content, enabling audit trails to detect unauthorized alterations in online cultural heritage[67]. Such innovations reduce reliance on trusted third parties and enhance legal accountability.

Yet, NFT-based commodification of indigenous heritage risks reducing cultural value to transactional logic, conflicting with communal ownership norms. Policymakers and technologists must collaborate with communities to balance blockchain's transparency with cultural sovereignty.

• Museum applications

Blockchain integration optimizes security and operational workflows. MAXP establishes secure digital artifact exchange platforms, mitigating cybersecurity risks in online transactions through decentralized verification protocols[65]. To reconcile anonymity with regulatory compliance, traceable one-time address schemes embed privacy-preserving mechanisms into digital asset interactions, permitting regulatory oversight without compromising user privacy[8]. Hybrid architectures combining BIM, IoT, and blockchain further enable smart museum ecosystems for real-time exhibit monitoring and visitor engagement[68]. Oracle's blockchain-as-a-service solutions similarly emphasize secure multi-party collaboration and ERP integration, aligning with museum infrastructure needs.

• Infrastructure enhancement

Blockchain extends to institutional modernization. HeriLedger employs energy-efficient consensus mechanisms (Lamport signatures[69], Zero-Knowledge Proofs) and incentivizes user participation through redeemable contribution points, fostering collaborative preservation and tourism synergies[70]. For intelligent buildings, hybrid BIM-IoT-blockchain systems enforce secure data storage and risk management via smart contracts, enhancing operational transparency for museum administrators[68]. Oracle's blockchain platforms further exemplify this trend, offering scalable solutions for cross-organizational data sharing and anti-tampering databases.

• Emerging trends and interoperability

Scalability and cross-platform integration dominate recent advancements. Bela Gipp's timestamping service archives web content via Bitcoin's ledger, enabling censorship-resistant heritage preservation and legal dispute resolution[67]. Modular frameworks like MApp demonstrate frontend-backend interoperability, accommodating diverse user roles through decentralized databases[44]. Oracle's 2023 updates highlight Ethereum-compatible APIs and ERC-1155 token standards, enabling multi-chain asset management-a critical step toward industry-wide blockchain adoption.

• Criti109ctions

While existing platforms demonstrate efficacy, limitations persist:

Energy Efficiency: Ethereum-dependent systems face scalability and carbon footprint challenges. Lightweight alternatives like HeriLedger's Lamport signatures remain under-tested for large-scale deployment.

Metadata Sustainability: IPFS-reliant architectures risk data fragmentation without centralized redundancy.

Interoperability: Cross-platform standards (e.g., Oracle's Hyperledger Fabric-DAML integration) require broader adoption.

Future research should prioritize hybrid AI-blockchain models for predictive analytics and Oracle-style anti-tampering databases to address these gaps.

Challenges and solutions

In the application of blockchain technology to the management of DCHR, while numerous advantages have been brought, a series of challenges are inevitably faced. These challenges may involve multiple dimensions such as technology, regulation, and interoperability. This section will explore these challenges and propose corresponding solutions in order to provide a more robust development path for the application of blockchain in DCHR.

System efficiency and scalability. Blockchain's redundancy ensures data integrity[71] but imposes latency and storage costs. Practical mitigation strategies include:

• IPFS Integration: Offloading substantial portions of large metadata to IPFS mitigates on-chain storage overhead while retaining cryptographic verifiability[66,72]. Heirloom's adoption of this approach yielded measurable improvements in transaction efficiency for artifact provenance management[64].

• Role-Based Authorization: Yun-Ciao Wang's multi-stakeholder framework (museum, licensee, proxy) streamlines rights verification workflows through smart contract automation, reducing administrative complexity in digital heritage management[73].

• Organizational Impact: IT teams must adopt hybrid skills in blockchain-node management and IPFS metadata governance, merging curatorial and technical roles.

Cross-chain technology and interoperability

Fragmented heritage databases hinder global collaboration. Key interventions:

• Hyperledger Fabric Consortiums: MAXP's implementation of Fabric's private channels for cross-border artifact exchanges demonstrated enhanced operational synchronization among participating institutions, significantly improving data reconciliation processes in multi-stakeholder heritage networks[65,74].

• ERC-1155 Token Standard: MApp unified NFT-based artifact records (provenance, restoration) across Ethereum and Polygon chains, enhancing traceability for 15,000+ minor artworks[44].

• Workflow Shift: Museums now require "heritage data stewards" to oversee multi-chain metadata schemas, bridging legacy databases and blockchain ledgers.

Regulation and standardization. Blockchain compels regulatory modernization and organizational redesign, with three transformative effects:

• Decentralized Governance: Salsal's blockchain review system[43] prompted museums to restructure their acquisition teams into dual roles: blockchain auditors, tasked with verifying on-chain provenance, and ethics compliance officers, responsible for aligning smart contracts with UNESCO regulations. This operational specialization significantly reduced disputes related to illicit acquisitions over a multi-year period. Parallel advancements in institutional governance are evident in the work of Liang et al., whose blockchain-based traceable management system employs smart contracts to enforce dynamic access control lists, streamlining cross-border collaboration among heritage institutions and reducing administrative overhead in artifact circulation[75]. These systems collectively highlight blockchain's capacity to balance decentralized accountability with regulatory compliance. Concurrently, Hyperledger Fabric consortiums[76] decentralized governance by transferring decision-making authority from centralized administrators to multi-stakeholder committees comprising museums, NGOs, and governmental bodies. The adoption of consensus-driven protocols enhanced the efficiency of cross-institutional approval processes. Collectively, this dual restructuring-combining role specialization in operational workflows with decentralized governance mechanisms-illustrates blockchain's dual capability to strengthen regulatory compliance while optimizing collaborative frameworks in cultural heritage stewardship.

• Role evolution: Curators have transitioned into active co-designers of smart contracts incorporating ethical sourcing frameworks, as evidenced by BMDRM's NFT-based contractual systems that operationalize royalty distribution mechanisms through predefined governance protocols[66]. Concurrently, registrars have evolved into blockchain-authenticated validators, certifying metadata provenance through cryptographic verification processes - a shift exemplified by HeriLedger's replacement of physical loan documentation with smart contract-executed agreements, demonstrating measurable administrative efficiency gains[70]. This dual functional transformation - positioning curators as ethical contract architects and registrars as decentralized authenticity guarantors - illustrates blockchain's capacity to reconfigure institutional workflows. The technological integration enhances operational coordination while enforcing audit-compliant transparency standards in decentralized cultural heritage resource (DCHR) stewardship.

• Operational metrics: The integration of decentralized storage protocols with Building Information Modeling (BIM) systems[68] significantly optimized environmental monitoring expenditures in smart cultural institutions through decentralized Internet of Things (IoT) data synchronization, demonstrating blockchain's role in enhancing operational precision for heritage conservation. Concurrently, blockchain-driven frameworks leveraging GDPR-compliant cryptographic frameworks[70] achieved comprehensive donor data anonymization while maintaining cryptographically secured audit trails, exemplifying the technology's capacity to balance privacy safeguards with institutional compliance requirements. These complementary implementations highlight blockchain's dual utility in addressing both technical optimization imperatives and ethical governance requirements within DCHR ecosystems.

In this chapter, the application cases such as Salsal and the Digital Dunhuang project have addressed some difficulties encountered in the management of DCHR using blockchain, such as improving system efficiency and regulation, and standardization. Moreover, the deployment of blockchain solutions in this domain faces persistent systemic barriers, particularly (1) institutional competency gaps arising from technical literacy limitations among heritage custodians, requiring structured training initiatives such as HeriLedger's certification programs; and (2) regulatory asymmetries where legal frameworks remain misaligned with technological capabilities, as observed in heritage protection legislation[77], necessitating adaptive governance models like MAXP's cross-domain compliance testing platforms[65]. Addressing these interconnected challenges demands harmonized strategies that concurrently advance technical proficiency and regulatory agility to align distributed ledger innovations with institutional stewardship imperatives.

Future trends and directions

As blockchain technology continues to evolve, its application prospects in the management of DCHR are becoming increasingly broad. This chapter will explore the future development trends and research directions of blockchain technology, including technological innovation, application expansion, and support from policies and regulations, among other aspects.

Technological innovation

Future developments in digital cultural heritage (DCHR) management must prioritize addressing two critical technical challenges for blockchain implementation. First, context-aware unique identifiers in blockchain should extend beyond static metadata (e.g., provenance, ownership) to integrate IoT and incorporate additional conservation metrics, such as environmental conditions and restoration histories. Embedding sensor-generated contextual data into blockchain records enables adaptive conservation strategies for cultural heritage. Second, AI-based watermarking systems can use advanced cryptography such as zero-knowledge proofs (ZKP) to protect copyrights while maintaining data usability. These innovations are expected to address the inherent scalability and security limitations of existing systems, forming a focal point of our ongoing research.

Application extension

Blockchain applications must transition from passive documentation to active governance mechanisms. Decentralized autonomous organizations (DAOs) could optimize cross-border artifact loans by automating multi-stakeholder consensus via smart contracts, thereby streamlining approval processes[78]. Concurrently, programmable NFTs should incorporate usage-rights clauses, such as exhibition limits and reproduction terms, to enforce ethical access controls. Case studies, including BMDRM's implementation, highlight the potential of NFT-based licensing to mitigate unauthorized usage[79]. Furthermore, integrating blockchain with augmented reality (AR) platforms could establish immersive provenance verification systems, allowing public access to artifact histories through immutable ledger entries.

These advancements position blockchain as a participatory infrastructure for global heritage stewardship, transcending traditional archival roles.

Policy and regulatory support

Three policy initiatives are critical for scalable blockchain adoption. First, international regulatory sandboxes, led by organizations like UNESCO, should test hybrid frameworks that reconcile data privacy regulations across jurisdictions, such as GDPR and China's PIPL[80]. Second, mandatory blockchain provenance standards in national heritage laws could enhance traceability for high-risk artifacts, including conflict antiquities, by enforcing metadata consistency. Third, carbon-neutral consensus protocols aligned with global climate goals must incentivize transitions to energy-efficient mechanisms, significantly reducing the environmental footprint of blockchain operations. China's blockchain certification system exemplifies efforts to harmonize technical rigor with ethical imperatives[70].

Discussion

This study empirically validates the transformative potential of blockchain technology in DCHR governance through two pivotal case studies, advancing the discourse on this field. The Digital Dunhuang Open Material Library showcases blockchain's capacity to reconcile scalability with institutional collaboration in large-scale digitization efforts, while its NFT-driven economic model provides an innovative framework for sustainable cultural heritage valorization. Concurrently, the Salsal case study demonstrates how embedding the ethical guidelines of the International Council of Museums (ICOM) into Ethereum-based smart contracts enables ethical curation through decentralized governance, resolving persistent tensions between transparency and regulatory compliance.

Beyond technical efficacy, our case studies reveal blockchain's sociopolitical implications for heritage governance. Drawing on Smith's Authorized Heritage Discourse (AHD) framework, blockchain technology exhibits a dual impact on heritage studies. On one hand, its decentralized nature potentially challenges the traditional heritage discourse monopolized by professional institutions and governments. On the other hand, blockchain's inherent technical architecture may establish a new "technocratic authority," inadvertently transferring discursive power to developer communities through coding paradigms while potentially ossifying singular interpretations of digital heritage via algorithmic determinism.

Furthermore, the enhanced Raft algorithm and context-aware unique identifier mechanism proposed in this study are poised to expand blockchain's applicability in DCHR management. By optimizing consensus efficiency and enabling dynamic identifier tracking, these technical advancements promise to enhance the precision of ownership authentication and inter-institutional circulation efficiency. These innovations not only pioneer novel methodologies for blockchain adoption in heritage preservation but also chart new directions for future research and practical implementation.

Data availability

No datasets were generated or analysed during the current study.

Abbreviations

BFT	Byzantine-Fault-Tolerance
DCHR	digital cultural heritage resources
DPoS	Delegated-Proof-of-Stake
DAO	Decentralized Autonomous Organization
IPFS	InterPlanetary File System
IP	Intellectual Property
IoT	Internet of Thing
NFTs	Non-Fungible Tokens
PoW	Proof-of-Work
PoS	Proof-of-Stake
PoA	Proof-of-Authority
PoS	Proof-of-Stake
VR	Virtual Reality

Received: 15 December 2024; Accepted: 23 May 2025;
Published online: 05 June 2025

References

1. Whitaker, A. Art and blockchain: a primer, history, and taxonomy of blockchain use cases in the arts. *Artivate* **8**, 21–46 (2019).
2. Valeonti, F. et al. Crypto collectibles, museum funding and openglam: challenges, opportunities and the potential of non-fungible tokens (nfts). *Appl. Sci.* **11**, 9931 (2021).
3. Wang, Q., Li, R., Wang, Q. & Chen, S. Non-fungible token (nft): overview, evaluation, opportunities and challenges. *arXiv preprint at* https://arxiv.org/abs/2105.07447 (2021).
4. Roh, T. H. Digital transformation and introduction of NFT in the art market. *J. Converg. Cult. Technol.* **8**, 261–269 (2022).
5. Zhao, Z. & Wei, J. Blockchain technology in the protection and inheritance of non-traditional heritage. *Br. J. Philos. Sociol. Hist.* **2**, 05–08 (2022).
6. Zhong, X. The development and dissemination of intelligent storage management software of Chinese excellent traditional culture based on blockchain in the era of financial media. *Heliyon* **10**, e27262 (2024).
7. Popovski, L., Soussou, G. & Webb, P. B. A brief history of blockchain. *Legaltech N.* **2018**, 3 (2018).
8. Zhao, L., Zhong, L. & Zhang, J. Traceable one-time address solution to the interactive blockchain for digital museum assets. *Inf. Sci.* **625**, 157–174 (2023).
9. Samus, P. & Serhiienko, O. Modern blockchain and web3. 0 information technologies within the healthhelper startup (2023).
10. Cai, L., Sun, Y., Zheng, Z., Xiao, J. & Qiu, W. Blockchain in China. *Commun. ACM* **64**, 88–93 (2021).
11. Kim, H. S. & Wang, K. Immutability measure for different blockchain structures. In *2018 IEEE 39th Sarnoff Symposium*, 1–6 (IEEE, 2018).
12. Rahardja, U., Hidayanto, A. N., Lutfiani, N., Febiani, D. A. & Aini, Q. Immutability of distributed hash model on blockchain node storage. *Sci. J. Inform.* **8**, 137–143 (2021).
13. Hofmann, F., Wurster, S., Ron, E. & Böhmecke-Schwafert, M. The immutability concept of blockchains and benefits of early standardization. In *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, 1–8 (IEEE, 2017).
14. Landerreche, E. & Stevens, M. On immutability of blockchains. In *Proceedings of 1st ERCIM Blockchain Workshop 2018* (European Society for Socially Embedded Technologies) (EUSSET 2018).
15. Tariq, U., Ibrahim, A., Ahmad, T., Bouteraa, Y. & Elmogy, A. Blockchain in internet-of-things: a necessity framework for security, reliability, transparency, immutability and liability. *IET Commun.* **13**, 3187–3192 (2019).
16. Hongo, S., Sudrajat, R. & Yulita, I. N. Design of museum historical heritage management system using blockchain digital certificate and hyperledger composer. In *2021 International Conference on Artificial Intelligence and Big Data Analytics*, 231–235 (IEEE, 2021).
17. Zarrin, J., Wen Phang, H., Babu Saheer, L. & Zarrin, B. Blockchain for decentralization of internet: prospects, trends, and challenges. *Clust. Comput.* **24**, 2841–2866 (2021).
18. Chu, S. & Wang, S. The curses of blockchain decentralization. *arXiv preprint at* https://arxiv.org/abs/1810.02937 (2018).
19. Zhang, L., Ma, X. & Liu, Y. Sok: blockchain decentralization. *arXiv preprint at* https://arxiv.org/abs/2205.04256 (2022).
20. De Filippi, P. The interplay between decentralization and privacy: the case of blockchain technologies. *J. Peer Prod. 7* (2016).
21. Hellani, H., Sliman, L., Samhat, A. E. & Exposito, E. On blockchain integration with supply chain: overview on data transparency. *Logistics* **5**, 46 (2021).
22. Sedlmeir, J., Lautenschlager, J., Fridgen, G. & Urbach, N. The transparency challenge of blockchain in organizations. *Electron. Mark.* **32**, 1779–1794 (2022).

23. Dasgupta, D., Shrein, J. M. & Gupta, K. D. A survey of blockchain from security perspective. *J. Bank. Financ. Technol.* **3**, 1–17 (2019).
24. Halpin, H. & Piekarska, M. Introduction to security and privacy on the blockchain. In *2017 IEEE European symposium on security and privacy workshops (EuroS&PW)*, 1–3 (IEEE, 2017).
25. Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E. & Secundo, G. Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Inf. Manag.* **59**, 103508 (2022).
26. Ko, T., Lee, J. & Ryu, D. Blockchain technology and manufacturing industry: real-time transparency and cost savings. *Sustainability* **10**, 4274 (2018).
27. Cui, Y., Gaur, V. & Liu, J. Supply chain transparency and blockchain design. *Manag. Sci.* **70**, 3245–3263 (2024).
28. Cao, S., Cao, Y., Wang, X. & Lu, Y. A review of researches on blockchain. *BenchCouncil Transact. Benchmarks Stand. Evaluat.* **2**, 100073 (2017).
29. Kresyanpol, L., Novachevskyi, S. & Hranovskyi, M. Application of blockchain technologies for preservation and dissemination of cultural heritage through NFT. *Inform. Technol. Soc.* **3**, 54–62 (2023).
30. Whitaker, A., Bracegirdle, A., De Menil, S., Gitlitz, M. A. & Saltos, L. Art, antiquities, and blockchain: new approaches to the restitution of cultural heritage. *Int. J. Cult. Policy* **27**, 312–329 (2021).
31. Rubino, F., Agostino, D. & Spallazzo, D. Strategizing blockchain adoption in public cultural services: a comprehensive scoping review. *Int. J. Public Sect. Manag.* **38**, 77–97 (2025).
32. Hu, W., Han, H., Wang, G., Peng, T. & Yang, Z. Interactive design and implementation of a digital museum under the background of ar and blockchain technology. *Appl. Sci.* **13**, 4714 (2023).
33. Ch'ng, E. The first original copy and the role of blockchain in the reproduction of cultural heritage. *Presence* **27**, 151–162 (2019).
34. Hylland, O. M. Even better than the real thing? Digital copies and digital museums in a digital cultural policy. *Cult. Unbound* **9**, 62–84 (2017).
35. Dobreva, M. & Ikonomov, N. The role of metadata in the longevity of cultural heritage resources. In *Proceedings of the EACL 2009 Workshop on Language Technology and Resources for Cultural Heritage, Social Sciences, Humanities, and Education (LaTeCH–SHELT&R 2009)*, 69–76 (2009).
36. Peipei, Z., Huan, L. & Chenchen, H. Research on 3d digitization scheme of cultural relics preserved for a long time. iPRES 2021.
37. Siliutina, I., Tytar, O., Barbash, M., Petrenko, N. & Yepyk, L. Cultural preservation and digital heritage: challenges and opportunities. *Amazon. Investig.* **13**, 262–273 (2024).
38. Ghorpade, A. & Pandey, U. The implications of blockchain technology for the preservation of indian intangible cultural heritage. In *Building Secure Business Models Through Blockchain Technology: Tactics, Methods, Limitations, and Performance*, 194–208 (IGI Global, 2023).
39. Wang, Y.-C., Chen, C.-L. & Deng, Y.-Y. Museum-authorization of digital rights: A sustainable and traceable cultural relics exhibition mechanism. *Sustainability* **13**, 2046 (2021).
40. Al-Meer, A. & Al-Kuwari, S. Physical unclonable functions (PUF) for iot devices. *ACM Comput. Surv.* **55**, 1–31 (2023).
41. Henry, R., Herzberg, A. & Kate, A. Blockchain access privacy: Challenges and directions. *IEEE Secur. Priv.* **16**, 38–45 (2018).
42. Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T. & Skarmeta, A. Privacy-preserving solutions for blockchain: review and challenges. *IEEE Access* **7**, 164908–164940 (2019).
43. Khelifi, A., Altaweel, M., Hashir, M., Hadjitofi, T. & Ghazal, M. Salsal: blockchain for vetting cultural object collections. *Herit. Sci.* **12**, 15 (2024).
44. Bacciu, C., Duca, A. L. & Marchetti, A. A blockchain-based application to protect minor artworks. In *WEBIST*, 319–325 (2019).
45. Zhou, S. et al. A systematic review of consensus mechanisms in blockchain. *Mathematics* **11**, 2248 (2023).
46. Lashkari, B. & Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **9**, 43620–43652 (2021).
47. Abellán Álvarez, I., Gramlich, V. & Sedlmeir, J. Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake. In *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*, 278–287 (2024).
48. Baboi, M. Security of consensus mechanisms in blockchain. *Rom. Cyber Secur. J.* **5**, 45–53 (2023).
49. Ren, L. & Ward, P. A. Distributed consensus and fault tolerance mechanisms. In *Essentials of Blockchain Technology*, 1–26 (Chapman and Hall/CRC, 2019).
50. Zhang, R. & Preneel, B. Lay down the common metrics: Evaluating proof-of-work consensus protocols' security. In *2019 IEEE Symposium on Security and Privacy (SP)*, 175–192 (IEEE, 2019).
51. Porat, A., Pratap, A., Shah, P. & Adkar, V. Blockchain consensus: an analysis of proof-of-work and its applications (2017).
52. Beccuti, J. et al. The bitcoin mining game: On the optimality of honesty in proof-of-work consensus mechanism. *Swiss Economics Working Paper 0060* (2017).
53. Nguyen, C. T. et al. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access* **7**, 85727–85745 (2019).
54. Cheng, Y., Hu, X. & Zhang, J. An improved scheme of proof-of-stake consensus mechanism. In *2019 4th International conference on mechanical, control and computer engineering (ICMCCE)*, 826–8263 (IEEE, 2019).
55. Manolache, M. A., Manolache, S. & Tapus, N. Decision making using the blockchain proof of authority consensus. *Procedia Comput. Sci.* **199**, 580–588 (2022).
56. Wu, X., Chang, J., Ling, H. & Feng, X. Scaling proof-of-authority protocol to improve performance and security. *Peer-to-Peer Netw. Appl.* **15**, 2633–2649 (2022).
57. Driscoll, K., Hall, B., Sivencrona, H. & Zumsteg, P. Byzantine fault tolerance, from theory to reality. In *International Conference on Computer Safety, Reliability, and Security*, 235–248 (Springer, 2003).
58. Zhan, Y., Wang, B., Lu, R. & Yu, Y. Drbft: Delegated randomization byzantine fault tolerance consensus protocol for blockchains. *Inf. Sci.* **559**, 8–21 (2021).
59. Ni, L., Ye, Q., Yang, J., Zhang, S. & Xian, M. Research of raft algorithm improvement in blockchain. In *2024 IEEE 16th International Conference on Advanced Infocomm Technology (ICAIT)*, 290–294 (IEEE, 2024).
60. Stephen, R. & Alex, A. A review on blockchain security. In *IOP conference series: materials science and engineering*, vol. 396, 012030 (IOP Publishing, 2018).
61. Li, X., Jiang, P., Chen, T., Luo, X. & Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **107**, 841–853 (2020).
62. Zhang, Y., Liu, C., Zhu, Z. & Lu, Y. Research on information system model for movable cultural relics through blockchain technology. In *2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, 625–627 (IEEE, 2021).
63. Zhang, J., Guo, M., Li, B. & Lu, R. A transport monitoring system for cultural relics protection based on blockchain and internet of things. *J. Cult. Herit.* **50**, 106–114 (2021).
64. Ertürk, E., Doğan, M., Kadiroğlu, Ü. & Karaarslan, E. Nft based fundraising system for preserving cultural heritage: heirloom. In *2021 6th International Conference on Computer Science and Engineering (UBMK)*, 699–702 (IEEE, 2021).
65. Zhao, L., Zhang, J., Jing, H., Wu, J. & Huang, Y. A blockchain-based cryptographic interaction method of digital museum collections. *J. Cult. Herit.* **59**, 69–82 (2023).
66. Zhao, L., Zhang, J. & Jing, H. Blockchain-enabled digital rights management for museum-digital property rights. *Intelligent Automation & Soft Computing* **34** (Tech Science Press, 2022).

67. Gipp, B., Meuschke, N., Beel, J. & Breitinger, C. Using the blockchain of cryptocurrencies for timestamping digital cultural heritage. *Bull. IEEE Tech. Comm. Digit. Libr*. (2017).
68. Siountri, K., Skondras, E. & Vergados, D. D. Towards a smart museum using BIM, iot, blockchain and advanced digital technologies. In *Proceedings of the 3rd International Conference on vision, image and signal processing*, 1–6 (2019).
69. Trček, D. Cultural heritage preservation by using blockchain technologies. *Herit. Sci.* **10**, 6 (2022).
70. Trček, D. Heriledger-a new generation of blockchains for cultural heritage preservation. *Sensors* **22**, 8913 (2022).
71. Leng, J., Zhou, M., Zhao, J. L., Huang, Y. & Bian, Y. Blockchain security: a survey of techniques and research directions. *IEEE Trans. Serv. Comput.* **15**, 2490–2510 (2020).
72. Chen, Y., Li, H., Li, K. & Zhang, J. An improved p2p file system scheme based on IPFS and blockchain. In *2017 IEEE International Conference on Big Data (Big Data)*, 2652–2657 (IEEE, 2017).
73. Wang, Y.-C., Chen, C.-L. & Deng, Y.-Y. Authorization mechanism based on blockchain technology for protecting museum-digital property rights. *Appl. Sci.* **11**, 1085 (2021).
74. Sater, S. & Wright, R. A conversation on art, museums, and blockchain. *Tul. J. Tech. Intell. Prop.* **21**, 35 (2019).
75. Liang, X. et al. Blockchain-based traceable management system for entry and exit of cultural relics. In *2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS)*, 1–6 (IEEE, 2020).
76. Feng, Q., He, D., Zeadally, S., Khan, M. K. & Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **126**, 45–58 (2019).
77. Fincham, D. Assessing the viability of blockchain to impact the antiquities trade. *Cardozo Arts Ent. LJ* **37**, 605 (2019).
78. Pinto-Gutiérrez, C., Gaitán, S., Jaramillo, D. & Velasquez, S. The nft hype: What draws attention to non-fungible tokens? *Mathematics* **10**, 335 (2022).
79. Popescu, A.-D. Non-fungible tokens (nft)–innovation beyond the craze. *5th Int. Conf. Innov. Bus., Econ. Mark. Res.* **32**, 26–30 (2021).
80. Wang, Y. Media safety threshold for the digital protection and inheritance of dunhuang culture:–take nft technology as an example. *Front. Comput. Intell. Syst.* **7**, 80–84 (2024).
81. Gervais, A. et al. On the security and performance of proof of work blockchains. In *Proc. of the 2016 ACM SIGSAC conference on computer and communications security*, 3–16 (2016).
82. Joshi, S. Feasibility of proof of authority as a consensus protocol model. *arXiv preprint at* https://arxiv.org/abs/2109.02480 (2021).
83. Nazir, A. et al. An optimized concurrent proof of authority consensus protocol. In *2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 874–877 (IEEE, 2023).
84. Zhong, W. et al. Byzantine fault-tolerant consensus algorithms: a survey. *Electronics* **12**, 3801 (2023).
85. Lei, K., Zhang, Q., Xu, L. & Qi, Z. Reputation-based byzantine fault-tolerance for consortium blockchain. In *2018 IEEE 24th international conference on parallel and distributed systems (ICPADS)*, 604–611 (IEEE, 2018).
86. Tang, F., Peng, J., Wang, P., Zhu, H. & Xu, T. Improved dynamic byzantine fault tolerant consensus mechanism. *Comput. Commun.* **226**, 107922 (2024).

Acknowledgements
This work is partially supported by National Key R&D Program of China (No. 2023YFF0906504), by National Natural Science Foundation of China through Project 62271393, and by Open Project Program of State Key Laboratory of Virtual Reality Technology and Systems, Beihang University (No. VRLAB2024C02), by General Projects of the Shaanxi Provincial Department of Science and Technology (2025JC-YBQN-801), and by General Projects of the Shaanxi Provincial Education Department Research Program (24JK0675).

Author contributions
Xinda Liu: Writing original draft and editing, data collection. Feihao Dong: Conceptualization, data collection, writing original draft. Wuyang Shui: Writing review and editing, data collection. Guohua Geng: Supervision, Writing review, and editing. All authors reviewed the manuscript.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to Guohua Geng.