Date of publication DEC-31, 2025, date of current version AUG-07, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.24.4.4345

Decentralized Blockchain Framework for the Provenance of Cultural Heritage

TARAS MAKSYMYUK[1], FRANCESCO MELONI[2], MATIAS TORRES DIAZ[2], DOMENICO ROMANO[2], LORENZO BELUCCI[3], NATALIA CHUKHRAY[1]

[1]Lviv Polytechnic National University, Lviv 79013, Ukraine
[2]AVVALE, Rome 00144, Italy
[3]ONE TRUE ID, Chiari 25030, Italy

Corresponding author: Taras Maksymyuk (e-mail: taras.a.maksymiuk@lpnu.ua)

ABSTRACT This paper presents a blockchain-centered system architecture for cultural heritage provenance that replaces fragmented, paper-based tracking with a tamper-evident, auditable digital workflow. We assume that each object can be reliably bound to a stable physical fingerprint through an established scan-based pipeline, and we focus on how that fingerprint is represented, stored, and verified within a practical distributed ledger design. The proposed framework separates high-assurance settlement events, such as registration and ownership transfer, from high-volume operational records, such as condition updates and monitoring logs, by routing data across multiple layers and committing verifiable summaries of frequent activity to a high-security anchor chain. We also describe a deployable decentralized application stack that integrates standard token interfaces for asset representation, event-driven synchronization for user-facing services, and scalable node access to reduce read latency without requiring institutions to maintain their own node infrastructure. The result is a concrete system model that clarifies how the end-to-end provenance trail remains verifiable under realistic performance constraints.

KEYWORDS blockchain; non-fungible tokens; physically unclonable functions; inter-planetary file system, provenance, cultural heritage.

I. INTRODUCTION

The integrity of the global art market relies fundamentally on two pillars: the authenticity of the physical artifact and the immutability of its provenance history. However, the art ecosystem currently suffers from a "double-spend" problem of credibility: art counterfeiting and illicit trafficking erode the economic value of genuine works and destabilize trust among collectors, museums, and auction houses. The financial implications are severe, yet the technological infrastructure for verification remains largely analog, siloed, and vulnerable to manipulation.

Historical precedence demonstrates the catastrophic failure of traditional, centralized verification methods. The limitations of relying on subjective expert opinion and paper-based documentation are exemplified by the Knoedler Gallery scandal, where approximately $80 million in forged paintings, falsely attributed to abstract expressionists like Mark Rothko and Jackson Pollock, circulated for years, bolstered by fabricated provenance documents [1]. Similarly, the case of Wolfgang Beltracchi, who successfully mimicked early 20th-century styles and materials , and the Greenhalgh family’s 17-year operation producing counterfeit antiquities, highlight the sophistication of modern fraud [2]. These adversaries exploit the lack of a tamper-proof, synchronized ledger; if a forger can replicate a physical style, they can easily forge the accompanying paper history. Furthermore, the theft of masterpieces, such as the 2002 raid on the Van Gogh Museum, underscores the necessity for a persistent, traceable digital identity for high-value cultural assets [3].

To address these systemic vulnerabilities, this paper proposes a transition from analog certification to a cryptographically secured distributed ledger. Blockchain technology offers a decentralized, immutable state machine capable of recording an artifact's lifecycle from creation to current ownership, without reliance on central authority. By hashing transaction data into blocks linked via cryptographic pointers, the network ensures that historical records cannot be retroactively altered [4].

However, the application of blockchain to cultural heritage presents unique technical challenges. The primary obstacle is the "Oracle Problem," or the risk of "garbage in, garbage out": if a counterfeit item is tokenized as genuine, the blockchain merely immutabilizes a lie. Consequently, a robust system requires more than a simple ledger. It demands layered architecture integrating Non-Fungible Tokens (NFTs) for asset representation and advanced middleware for scalability.

This paper introduces a comprehensive framework that leverages the ERC-721 and ERC-1155 token standards to create unique digital twins of physical artifacts. Unlike fungible assets (e.g., Bitcoin), these standards allow for the embedding of distinct metadata, such as spectral analysis data and provenance logs, directly into the token’s Uniform Resource Identifier (URI). To overcome the scalability and latency limitations inherent in direct Layer-1 blockchain interactions, our proposed architecture incorporates Alchemy as a node provider and middleware layer. By utilizing Alchemy's Supernode infrastructure and NFT APIs, we enable high-throughput data retrieval and real-time state monitoring, essential for a user-friendly Decentralized Application (DApp).

The contributions of this paper are as follows:

1. We analyze the deficiencies of current provenance methods and the "garbage in" problem in blockchain integration.
2. We propose an interdisciplinary "Phygital" (physical-digital) binding mechanism combining Physically Unclonable Functions (PUFs) derived from chemical analysis with blockchain hashing.
3. We detail a technical architecture utilizing Smart Contracts for automated provenance updates and Alchemy for robust node management, ensuring a scalable and cost-effective solution for the art market.

The remainder of this paper is organized as following. Section II presents an overview of the blockchain based frameworks for cultural heritage management. Section III describes the system model and workflow of the proposed cultural heritage management framework. Section IV concludes the paper.

II. BLOCKCHAIN-BASED HERITAGE MANAGEMENT

A. MULTI-BLOCKCHAIN FRAMEWORKS FOR ADAPTIVE THROUGHPUT–SECURITY TRADE-OFFS

Blockchain is often described as a single ledger that is transparent, tamper resistant, and decentralized, but that framing is a poor fit for cultural heritage because the data is heterogeneous in both risk and volume. Figure 1 summarizes the main functions commonly attributed to blockchain in art-market integrity systems. It illustrates how a blockchain registry can anchor records about provenance, ownership history, and authenticity through tamper-evident storage (hash-linked blocks and consensus), support traceable transfer histories across institutions, and reduce single points of failure through decentralization. It also shows application-layer mechanisms, including tokenization (NFT-style digital representations) and smart contracts that automate payments and ownership transfers once conditions are met, with the intended effect of lowering fraud risk and improving auditability, assuming the underlying artwork-to-record binding and data entry are trustworthy.

High-stakes events such as registering an artifact's digital twin, committing ownership, or recording a legally relevant custody transfer are rare but demand strong finality and governance. Operational events such as condition reports, transport checkpoints, environmental sensor logs, and routine conservation notes are frequent and time sensitive, and they often prioritize throughput and latency. Treating both classes as identical transactions on one chain forces a brittle compromise that mirrors the scalability and security tensions highlighted in blockchain scalability surveys [5-7]. If the system is tuned for maximal decentralization and conservative finality, cost and throughput can become prohibitive for high-frequency updates. If it is tuned for speed and low cost, the security model may fall short of what high-value provenance requires [5-7].

A more defensible approach is a multi-blockchain framework in which different ledgers play distinct roles and the system routes data to the layer that matches its requirements. The central design principle is separation of concerns across settlement, execution, and storage. A highly secure settlement chain provides durable integrity for the claims that must be hardest to rewrite, while one or more high-throughput execution environments handle frequent updates and user-facing interactions. Large files and rich metadata are placed in an off-chain storage or data-availability layer and referenced by integrity commitments, rather than stored directly on a general-purpose chain. Where confidentiality is required, permissioned domains or privacy-preserving mechanisms can restrict disclosure while keeping public verifiability of commitments [10,13]. This composition is widely reflected in cross-chain and interoperability research, which frames multi-chain systems as an architectural choice rather than a single-protocol solution [10, 13, 14].

This adaptive routing can be formalized as a requirement profile for each record type. For a record r_i, the profile can include integrity and non-repudiation, finality strength and censorship resistance, throughput and latency targets, confidentiality and access constraints, and storage footprint. Each candidate blockchain $c_j$can be characterized by a capability profile that reflects its consensus assumptions, typical finality behavior, execution capacity, cost model, and privacy features. The system then selects a placement function $\pi(r_i) = c_j$ that assigns $r_i$to the lowest-cost environment that still satisfies minimum security and governance constraints. This makes the throughput–security trade-off explicit and data-driven, rather than an implicit global setting applied to every operation [5-7, 10].

In heritage provenance, three placement patterns are particularly useful. First, a settlement layer anchors the existence and evolution of the artifact's canonical digital identity, including initial registration, binding commitments that link a physical object to a digital representation, and major ownership transitions. These events are infrequent, so higher settlement cost is acceptable in exchange for stronger decentralization and finality. Second, a high-throughput execution layer handles operational provenance updates that are frequent and time sensitive, such as custody handoffs during transport and routine condition updates. These events can be aggregated and committed to the settlement chain through checkpoints or Merkle-root commitments, and where stronger guarantees are needed, rollup-style constructions provide a principled way to batch activity while retaining a secure settlement anchor [8]. Third, large and high-dimensional files such as spectral scans, 3D meshes, and conservation imagery should be stored off-chain and referenced on-chain by content hashes or authenticated commitments, so retrieval is off-chain while integrity remains on-chain [5-8].

Some workflows also benefit from off-chain execution paths with on-chain dispute hooks. State channels and related Layer 2 mechanisms can support repeated interactions among bounded participants, which is common in multi-step institutional processes such as internal approvals, restoration planning, and staged provenance validation. These protocols improve throughput and latency by keeping most updates off-chain while retaining an on-chain enforcement and dispute path when needed, although they also introduce liveness and monitoring assumptions that must be stated clearly [9]. In a routing framework, this means channels are suitable only when participants, operational uptime, and dispute-handling procedures align with the protocol's model [9].

The security case in a multi-blockchain design depends primarily on how layers are connected. If a fast execution layer can mint or mutate the canonical artifact identity without a settlement-layer check, the system's effective security collapses to the weaker domain. A safer pattern keeps the canonical registry or token on the settlement chain and treats other chains as execution venues whose effects become authoritative only after they are finalized and committed through explicit proofs or commitments [8, 10]. This requires the system to define which state is canonical, which state is derived, and what evidence is required to move information across domains. Cross-chain messaging, bridges, and interoperability protocols are therefore part of the threat model, not incidental infrastructure. Cross-chain surveys emphasize that interoperability mechanisms vary widely in trust assumptions and failure modes, and empirical research on cross-chain transfers and attacks reinforces that bridges are high-risk components that demand strong auditing, explicit assumptions, and safe failure behavior [10, 11, 16]. Where atomic outcomes across domains are required, protocols for decentralized cross-chain exchange are relevant because they focus on preventing partial completion without relying on centralized intermediaries [12].

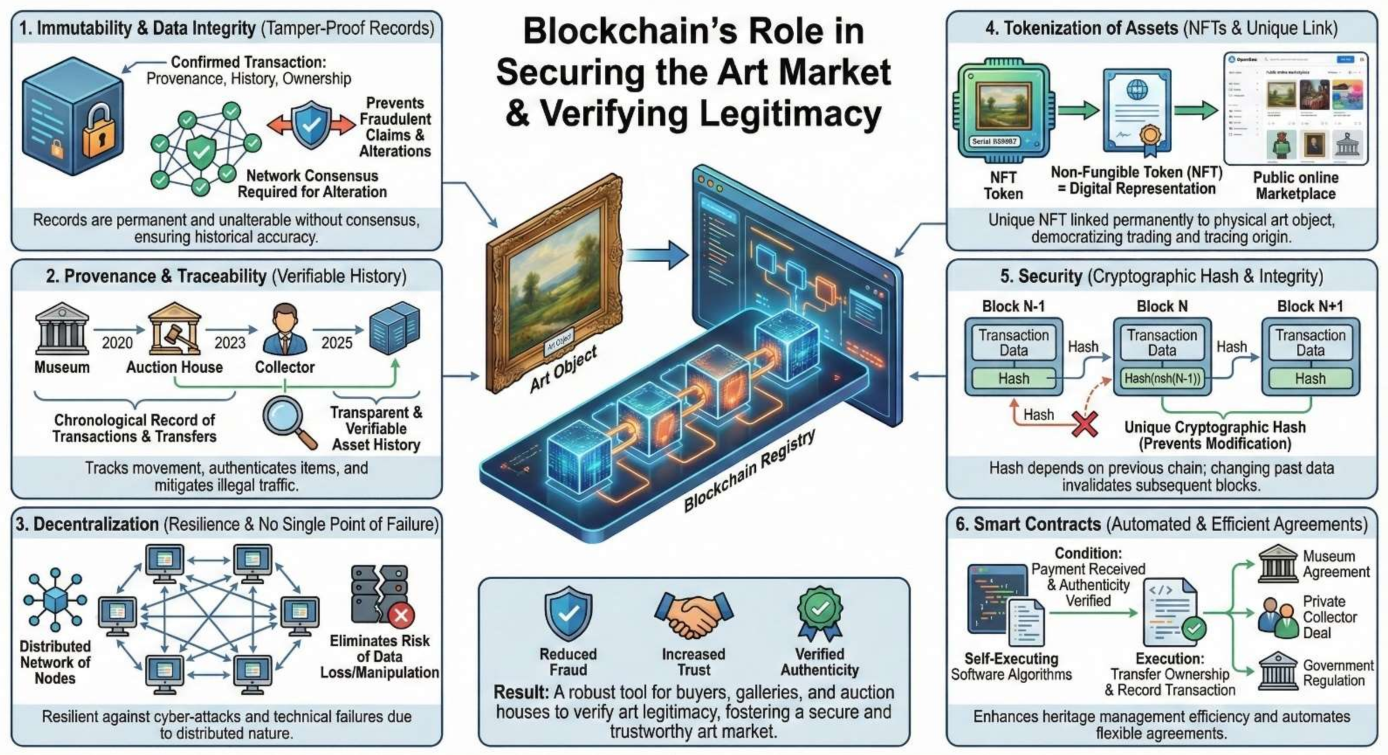
Blockchain's Role in Securing the Art Market & Verifying Legitimacy
1. Immutability & Data Integrity (Tamper-Proof Records)
Confirmed Transaction: Provenance, History, Ownership
Prevents Fraudulent Claims & Alterations
Network Consensus Required for Alteration
Records are permanent and unalterable without consensus, ensuring historical accuracy.
2. Provenance & Traceability (Verifiable History)
Museum
2020
Auction House
2023
Collector
2025
Chronological Record of Transactions & Transfers
Transparent & Verifiable Asset History
Tracks movement, authenticates items, and mitigates illegal traffic.
3. Decentralization (Resilience & No Single Point of Failure)
Distributed Network of Nodes
Eliminates Risk of Data Loss/Manipulation
Resilient against cyber-attacks and technical failures due to distributed nature.
Art Object
Blockchain Registry
Reduced Fraud
Increased Trust
Verified Authenticity
Result: A robust tool for buyers, galleries, and auction houses to verify art legitimacy, fostering a secure and trustworthy art market.
4. Tokenization of Assets (NFTs & Unique Link)
Serial RS9887
NFT Token
Non-Fungible Token (NFT) = Digital Representation
Public online Marketplace
Unique NFT linked permanently to physical art object, democratizing trading and tracing origin.
5. Security (Cryptographic Hash & Integrity)
Block N-1
Block N
Block N+1
Transaction Data
Hash
Transaction Data
Hash(nsh(N-1))
Hash
Transaction Data
Hash
Hash
Unique Cryptographic Hash (Prevents Modification)
Hash depends on previous chain; changing past data invalidates subsequent blocks.
6. Smart Contracts (Automated & Efficient Agreements)
Condition: Payment Received & Authenticity Verified
Self-Executing Software Algorithms
Execution: Transfer Ownership & Record Transaction
Museum Agreement
Private Collector Deal
Government Regulation
Enhances heritage management efficiency and automates flexible agreements.

Figure 1. The key features of the blockchain technology for enabling secure and art market.

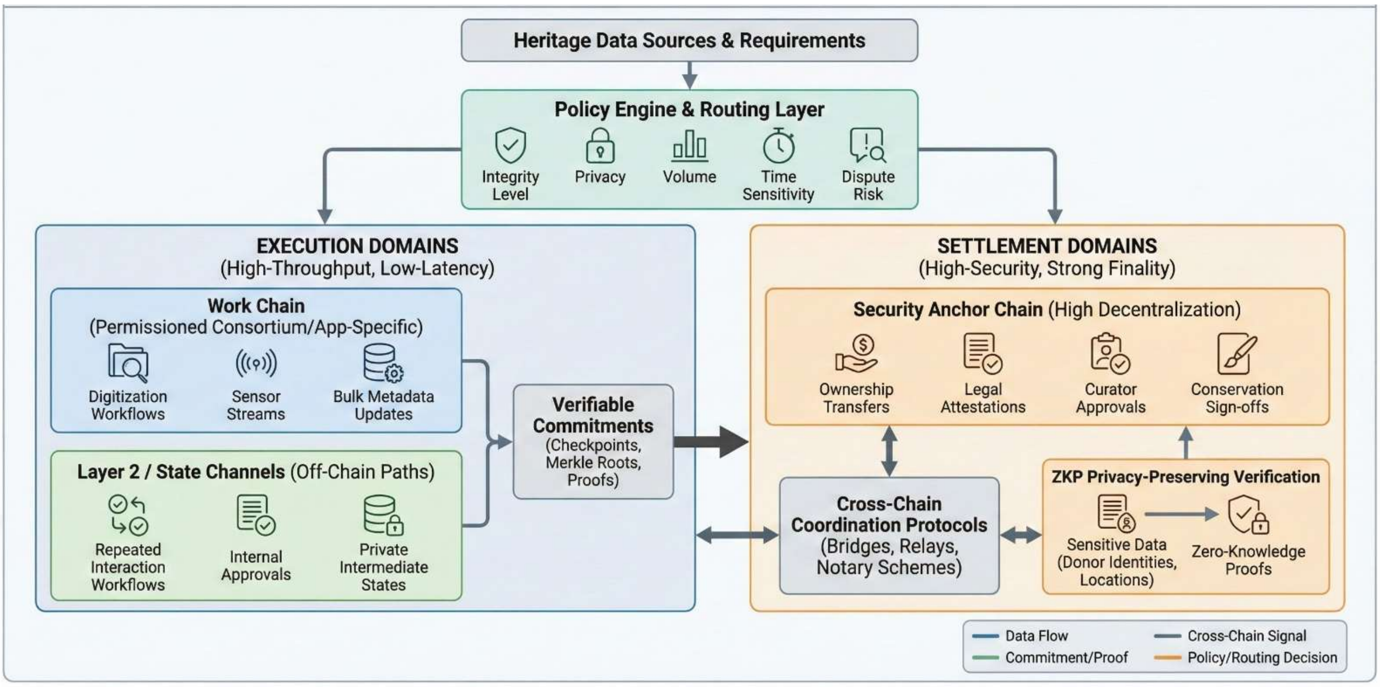
Heritage Data Sources & Requirements
Policy Engine & Routing Layer
Integrity Level
Privacy
Volume
Time Sensitivity
Dispute Risk
EXECUTION DOMAINS (High-Throughput, Low-Latency)
Work Chain (Permissioned Consortium/App-Specific)
Digitization Workflows
Sensor Streams
Bulk Metadata Updates
Layer 2 / State Channels (Off-Chain Paths)
Repeated Interaction Workflows
Internal Approvals
Private Intermediate States
Verifiable Commitments (Checkpoints, Merkle Roots, Proofs)
SETTLEMENT DOMAINS (High-Security, Strong Finality)
Security Anchor Chain (High Decentralization)
Ownership Transfers
Legal Attestations
Curator Approvals
Conservation Sign-offs
Cross-Chain Coordination Protocols (Bridges, Relays, Notary Schemes)
ZKP Privacy-Preserving Verification
Sensitive Data (Donor Identities, Locations)
Zero-Knowledge Proofs
Data Flow
Cross-Chain Signal
Commitment/Proof
Policy/Routing Decision

Figure 2. Multi-blockchain frameworks for adaptive throughput-security trade-offs in heritage management.

An adaptive trade-off framework also needs a coherent policy for confidentiality and selective disclosure. Heritage records may contain sensitive information such as donor identities, precise storage locations, transport routes, or private appraisals that stakeholders do not want fully public. A multi-blockchain architecture can accommodate this by publishing only public commitments on the settlement chain while keeping sensitive fields encrypted off-chain, restricted to a permissioned domain, or verified through privacy-preserving proofs. Zero-knowledge techniques are directly relevant here because they enable verification of a statement without revealing underlying sensitive data, which supports configurable transparency rather than unconditional disclosure [15]. Interoperability frameworks also motivate this separation by treating privacy, access control, and coordination as system-level properties rather than chain-specific features [13, 14].

Finally, the framework should support adaptation over time because workload and risk profiles change. Throughput demands can spike during auctions, exhibitions, and large digitization campaigns, while security requirements may tighten during cross-border movement or when legal disputes emerge. A multi-chain design can respond by shifting operational traffic toward higher-capacity execution domains while keeping the settlement anchor unchanged, and by adjusting checkpoint frequency so that high-risk periods reduce the exposure window between commitments [8, 10]. This makes the throughput–security trade-off a controllable parameter driven by data criticality and operational context, consistent with the scalability literature's view that there is no universal setting that dominates across all objectives [5-8].

In summary, the credible position for cultural heritage management is not that one blockchain satisfies every requirement. It is that provenance systems should be multi-layer and often multi-chain, with policy-driven routing based on explicit requirements, canonical identity anchored to the strongest available settlement layer, and cryptographic commitments binding high-throughput records to high-security finality [5-10, 13-15]. This architecture matches the practical structure of the heritage problem, where low-latency workflows and long-term, high-assurance provenance must coexist.

Figure 2 summarizes a technical overview of a multi-blockchain architecture for heritage management in which incoming heritage data sources and requirements are first evaluated by a policy engine and routing layer that weighs integrity level, privacy, data volume, time sensitivity, and dispute risk, then routes each record to an appropriate domain. High-throughput, low-latency needs are handled in execution domains through a permissioned or application-specific work chain (supporting digitization workflows, sensor streams, and bulk metadata updates) and through Layer 2 or state-channel paths for repeated interactions, internal approvals, and private intermediate states. These execution outputs are summarized into verifiable commitments such as checkpoints, Merkle roots, or proofs, which are anchored into settlement domains optimized for high security and strong finality, where a security anchor chain records high-stakes actions like ownership transfers, legal attestations, curator approvals, and conservation sign-offs. Cross-chain coordination protocols (bridges, relays, notary schemes) carry signals between domains, while a privacy-preserving verification module uses zero-knowledge proofs to validate sensitive information such as donor identities or locations without exposing raw data, and the legend distinguishes data flow, commitment proofs, cross-chain signals, and routing decisions.

B. EXISTING BLOCKCHAIN-BASED SOLUTIONS FOR THE ART MANAGEMENT

Early blockchain deployments in the art market largely converge on the same pattern: they treat the blockchain as a tamper-evident timestamping and registry layer for authenticity and provenance claims, often by anchoring a cryptographic identifier or a certificate record that can be checked later. Ascribe (2014) is a representative example. It focuses on registering creative works and associating them with a unique cryptographic identifier recorded on-chain to support later provenance and ownership assertions [17]. Verisart follows a similar registry logic but frames the anchored record as a digital certificate of authenticity that can be verified by market participants such as buyers, sellers, and auction houses [18]. The practical takeaway is not that these systems "solve authenticity," but that they provide an audit trail for claims that stakeholders are willing to treat as authoritative under their governance and identity assumptions.

A second cluster of solutions targets institutional provenance and collection records rather than creator registration. Artory positions itself as a registry for art and collectibles and emphasizes recording events such as provenance, exhibition history, and condition reporting in a way that is difficult to alter retroactively, including integrations with auction houses and galleries [19]. Codex Protocol similarly aims at a decentralized title registry that aggregates ownership and condition history to reduce disputes and fraud [20]. These platforms highlight a key design tension that motivates the multi-blockchain framing in Section II.A: the records they manage are not homogeneous. Some events are high-stakes settlement events, such as title transfer or legal attestation, while others are operational updates, such as routine condition notes. Many single-ledger implementations blur this distinction, which either drives costs up if every event is treated as settlement-grade, or weakens assurance if everything is pushed through a low-cost path.

A third line of work shifts from market provenance to logistics and physical inventory control, where volume and timeliness dominate and confidentiality can matter. Arteïa combines blockchain with RFID to track movement and condition, linking a physical tag to a digital record so that stakeholders can monitor objects as they move through storage, transport, and exhibition workflows [21]. This is exactly the regime where a single public settlement chain is often the wrong default. High-frequency tracking and sensor-linked events behave like execution-layer data, not settlement-layer data, and they should usually be aggregated into periodic commitments that anchor to a stronger chain only when needed. It is also where the "oracle problem" becomes unavoidable, since the integrity of the record depends on the integrity of the sensor, tag, and operator, not only the ledger.

Finally, several platforms focus on transactions and financialization rather than custody and conservation. Smart contracts are commonly proposed to automate parts of sale and transfer processes, reduce reliance on intermediaries, and encode market rules more transparently [22]. Maecenas extends this logic into fractional ownership by tokenizing artworks so that investors can buy shares, with smart contracts mediating transfers and accounting [23]. DADA Art Collective similarly uses tokenization to enable direct artist-to-collector exchange and to support royalty-like mechanisms on subsequent transfers [24]. These systems demonstrate that blockchain rails can reduce friction for certain transaction workflows, but they also reinforce the need for separation of concerns. Financial transactions and market interactions can be high volume and latency sensitive, while the authoritative provenance and legal title record should remain anchored to the strongest available settlement layer and governed with stricter controls.

Taken together, these solutions are useful case studies, but they also reveal why an adaptive multi-blockchain architecture is the more technically honest baseline for heritage and art management. The market already mixes rare, high-consequence events with frequent operational logging, and it mixes public verifiability with strong incentives to keep some details private. A system that routes records by data requirements can treat ownership transfers, legal attestations, and curator sign-offs as settlement-grade anchors, while pushing digitization workflows, RFID and sensor streams, and routine condition updates into higher-throughput execution domains with periodic cryptographic commitments. This framing also makes trust dependencies explicit, since the credibility of any on-chain record still depends on enrollment procedures, device integrity, and institutional governance, not on the blockchain alone.

III. BLOCKCHAIN-BASED FRAMEWORK FOR CULTURAL HERITAGE MANAGEMENT

A. GENERATION OF UNIQUE FINGERPRINTS OF ART OBJECTS USING XRF SCANNING

In this paper, we treat physical marking and scan acquisition as an upstream capability and focus on the system component that converts XRF measurements into a stable identifier that can be anchored on-chain. We adopt the notion of a digital fingerprint as a unique and non-replicable code derived from non-destructive XRF imaging over a small region of a cultural object. The fingerprint is required to satisfy two operational properties. It must be durable, meaning that the identifier remains invariant over time for the same object under acceptable conservation changes. It must also be repeatable, meaning that independent scans of the same region under realistic environmental and acquisition variability yield identifiers that match within a defined tolerance. The intended deployment context further constrains the pipeline to be non-invasive, non-contact, and suitable for in situ use with acquisition times on the order of minutes. The source of uniqueness is the object’s material and chemical microstructure rather than visible appearance, and the design targets features that are difficult to duplicate artificially, including sub-surface chemical characteristics that are expected to remain stable over long time horizons. The overall process of fingerprint generation is presented in Figure 3.

XRF measurements provide spectra whose characteristic peaks correspond to elemental emissions, enabling chemical composition analysis across a broad range of elements and concentrations. For identification, point spectra are insufficient because they do not capture spatial variability that makes artifacts distinctive. We therefore assume a microXRF scanning regime that produces dense area measurements and converts them into image-like representations. The scan of a region of interest is represented as a multi-channel tensor $X \in \mathbb{R}^{H\times W\times K}$, where $H \times W$is the spatial grid over the scanned area and each of the K channels corresponds to an elemental distribution map, or to selected characteristic line maps for a subset of elements chosen for that object and scanning campaign. When available, the acquisition workflow may also provide an optical overlay to support consistent region selection and to reduce operator-induced variability in repeated measurements.

The central technical objective is not pigment classification, but the construction of a fingerprint that remains stable across time, devices, and scanning conditions. Pre-processing therefore aims to suppress nuisance variation while preserving object-specific chemical microstructure. First, the pipeline harmonizes the spatial sampling by normalizing resolution and accounting for scan settings that affect blur and signal-to-noise, such as spot size, working distance, excitation power, and dwell time. Second, it applies count-stabilizing transforms and intensity normalization to reduce sensitivity to exposure and geometric effects while retaining relative elemental patterns. Third, repeated scans are aligned through rigid, or mildly non-rigid, registration so that embeddings are computed from comparable spatial support. If an optical overlay is available, it can be used as an additional alignment anchor. The overall goal is to achieve repeatability without smoothing away the heterogeneity that provides unclonability.

After pre-processing, the XRF tensor is mapped to a compact embedding through a learned encoder $f_\theta(\cdot)$, producing $z = f_\theta(X) \in \mathbb{R}^d$. The embedding is trained to be invariant within an object and discriminative across objects, including cases where different objects share similar palettes or materials. Metric learning objectives are a natural fit because the system must generalize to previously unseen artifacts. In this setting, two scans of the same object region, potentially acquired at different times or under different scanner configurations, form a positive pair, while scans from other objects form negatives. This directly optimizes the properties required for a stable identifier rather than relying on a closed-set classifier that assumes a fixed list of classes.

The blockchain does not require raw elemental maps, and storing them on-chain would be inefficient and unnecessary. Instead, the system stores a commitment that is stable for the genuine object and difficult to forge for another object. The embedding z is converted into a reproducible fingerprint code through robust quantization, such as sign-based or multi-bin quantization after normalization, combined with error tolerance to handle residual measurement noise. Enrollment produces a reference fingerprint code for the chosen region, which is stored off-chain for authorized verification workflows. On-chain, the system stores a cryptographic hash of the fingerprint code and essential metadata needed to make verification well-defined, including scanner type, region-of-interest definition, the selected element set, and a versioned description of the pre-processing profile. This separation preserves verifiability while keeping the blockchain architecture clean. Integrity is anchored at the settlement layer, high-volume scan artifacts remain in appropriate off-chain storage, and the link between them is enforced through cryptographic commitments rather than bulk on-chain data.

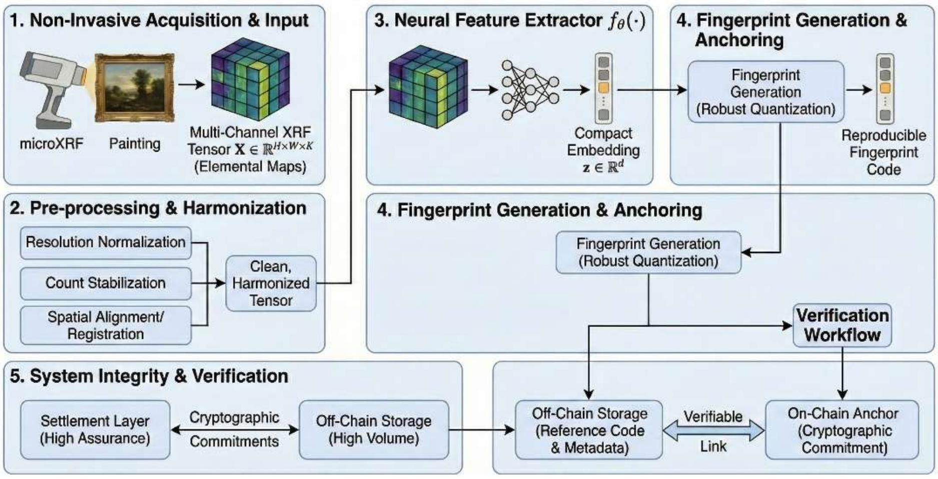
1. Non-Invasive Acquisition & Input
microXRF
Painting
Multi-Channel XRF Tensor $\mathbf{X} \in \mathbb{R}^{H\times W\times K}$ (Elemental Maps)
3. Neural Feature Extractor $f_\theta(\cdot)$
Compact Embedding $z \in \mathbb{R}^d$
4. Fingerprint Generation & Anchoring
Fingerprint Generation (Robust Quantization)
Reproducible Fingerprint Code
2. Pre-processing & Harmonization
Resolution Normalization
Count Stabilization
Spatial Alignment/ Registration
Clean, Harmonized Tensor
4. Fingerprint Generation & Anchoring
Fingerprint Generation (Robust Quantization)
Verification Workflow
5. System Integrity & Verification
Settlement Layer (High Assurance)
Cryptographic Commitments
Off-Chain Storage (High Volume)
Off-Chain Storage (Reference Code & Metadata)
Verifiable Link
On-Chain Anchor (Cryptographic Commitment)

Figure 3. The process of digital identity generation using XRF scanning of art objects.

B. SYSTEM MODEL OF THE BLOCKCHAIN-BASED ART MANAGEMENT SYSTEM

After physical fingerprint is generated we design blockchain architecture that stores these fingerprints, manages provenance and ownership, and supports verification workflows across stakeholders.

We define the system as a tuple $\langle \mathcal{A}, \mathcal{B}, \mathcal{S}, \mathcal{V} \rangle$, representing the set of physical Artifacts, the Blockchain ledger, the Scanning/Extraction mechanisms, and the Verification logic.

1. Modeling Physical Unclonable Functions (PUF)

Let $\mathcal{A} = \{a_1, a_2, \dots, a_n\}$ denote the set of physical cultural heritage artifacts. We assume that each artifact a_i possesses intrinsic, stochastic physical features (e.g., chemical composition, canvas grain) that function as a Physical Unclonable Function (PUF).

We define the Scanning Function S and the Feature Extraction Function Φ as follows:

$$S: \mathcal{A} \times \Theta \to \mathcal{D}$$
$$\Phi: \mathcal{D} \to \mathcal{F}$$

where:

- Θ represents the hyper-parameters of the scanning device (e.g., XRF wavelength, spectral resolution).
- $\mathcal{D}$ is the raw high-dimensional data space (spectrograms, point clouds).
- $\mathcal{F}$ is the extracted feature space (the digital fingerprint).

The composite fingerprint generation function Ψ for an artifact a_i is defined as:

$$f_i = \Psi(a_i, \theta) = \Phi\big(S(a_i, \theta)\big)$$

where f_i is the unique digital fingerprint.

To ensure the PUF property of Unclonability and Collision Resistance, for any two distinct artifacts a_i, a_j $(i \neq j)$, the probability of collision must be negligible:

$$P\left(\Psi(a_i) \approx \Psi(a_j)\right) \leq$$

where $\epsilon \to 0$ represents the False Acceptance Rate (FAR) of the system.

2. Cryptographic Binding and Tokenization

To link the physical fingerprint f_i to a blockchain asset, we utilize a cryptographic hash function $H: \{0,1\}^* \to \{0,1\}^{256}$ (e.g., Keccak-256).

The Digital Anchor h_i is computed as:

h_i = H(f_i || "{metadata}_i)

where | | denotes concatenation. This hash h_i is immutable and stored within the Smart Contract state.

We define the NFT Minting Function as a mapping from the digital anchor to a unique Token ID ($\tau \in \mathrm{N}$) within the ERC-721 contract:

$$\mathrm{Mint}: (\mathrm{Address}_{owner}, h_i, \mathrm{URI}) \to \tau_i$$

This establishes a bijection between the physical object a_i and the digital token τ_i.

3. Blockchain State and Transactions

We model the Blockchain Ledger $\mathcal{L}$ as an ordered sequence of blocks $B_0, B_1, \dots, B_n$. The state of the system at height t, denoted Σ_t, is updated by a set of valid transactions Tx.

A transaction Tx is defined as a tuple:

$$\mathrm{Tx} = (\mathrm{addr}_{from}, \mathrm{addr}_{to}, \tau_i, \sigma, \eta)$$

where:

- τ_i is the Token ID of the artifact.
- σ is the digital signature satisfying $\mathrm{VerifySig}(\mathrm{addr}_{from}, \mathrm{Tx}, \sigma) = \mathrm{True}$.
- η is the transaction payload (e.g., "Transfer Ownership" or "Update Condition Report").

The state transition function δ updates the global ledger:

$$\Sigma_{t+1} = \delta(\Sigma_t, \mathrm{Tx})$$

In the context of our Alchemy-based middleware, the read operation to retrieve the current state (e.g., owner of artifact a_i) is an $O(1)$ query via the API, rather than an $O(n)$ traversal of $\mathcal{L}$.

4. Automated Verification Logic

The core security utility is the Verification Function V, which determines if a presented physical object a_{query} corresponds to a claimed blockchain record τ_{claim}.

The verification process executes the following logic:

1. Generate query fingerprint: $f_{query} = \Psi\big(a_{query}, \theta\big)$.
2. Compute hash: $h_{query} = H\big(f_{query}\big)$.
3. Retrieve stored anchor h_{stored} associated with token τ_{claim} from the smart contract state Σ.

4. Compare:

$$V\big(a_{query}, \tau_{claim}\big) = \begin{cases} 1, \text{if } d\big(h_{query}, h_{stored}\big) < \delta_{threshold} \\ 0, otherwise \end{cases}$$

where $d(\cdot)$ is a distance metric (e.g., Hamming distance) appropriate for the hashing algorithm used. In strict hashing implementation, $\mathrm{h_{query}}$ must strictly equal $\mathrm{h_{stored}}$. The overall model of the proposed system is presented in Fig. 4.

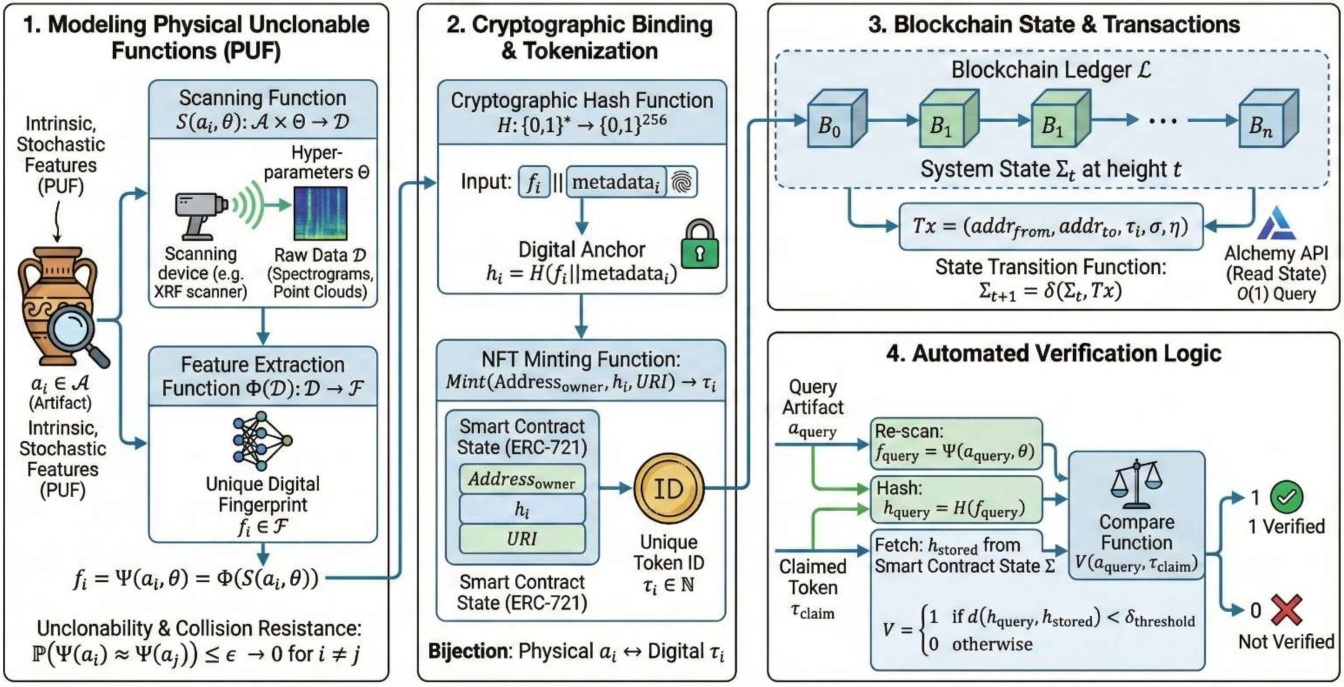
1. Modeling Physical Unclonable Functions (PUF)
Intrinsic, Stochastic Features (PUF)
$a_i \in \mathcal{A}$ (Artifact)
Intrinsic, Stochastic Features (PUF)
Scanning Function $S(a_i,\theta): \mathcal{A} \times \Theta \to \mathcal{D}$
Scanning device (e.g. XRF scanner)
Hyper-parameters Θ
Raw Data $\mathcal{D}$ (Spectrograms, Point Clouds)
Feature Extraction Function $\Phi(\mathcal{D}): \mathcal{D} \to \mathcal{F}$
Unique Digital Fingerprint $f_i \in \mathcal{F}$
$f_i = \Psi(a_i,\theta) = \Phi(S(a_i,\theta))$
Unclonability & Collision Resistance: $\mathbb{P}(\Psi(a_i) \approx \Psi(a_j)) \le \epsilon \to 0$ for $i \ne j$
2. Cryptographic Binding & Tokenization
Cryptographic Hash Function $H: \{0,1\}^* \to \{0,1\}^{256}$
Input: f_i || $\mathrm{metadata}_i$
Digital Anchor $h_i = H(f_i || \mathrm{metadata}_i)$
NFT Minting Function: $Mint(\mathrm{Address_{owner}}, h_i, URI) \to \tau_i$
Smart Contract State (ERC-721)
$Address_{owner}$
h_i
URI
ID
Unique Token ID $\tau_i \in \mathbb{N}$
Smart Contract State (ERC-721)
Bijection: Physical $a_i \leftrightarrow$ Digital τ_i
3. Blockchain State & Transactions
Blockchain Ledger $\mathcal{L}$
B_0
B_1
B_1
…
B_n
System State Σ_t at height t
$Tx = (addr_{from}, addr_{to}, \tau_i, \sigma, \eta)$
State Transition Function: $\Sigma_{t+1} = \delta(\Sigma_t, Tx)$
Alchemy API (Read State) $O(1)$ Query
4. Automated Verification Logic
Query Artifact a_{query}
Re-scan: $f_{\mathrm{query}} = \Psi(a_{\mathrm{query}}, \theta)$
Hash: $h_{\mathrm{query}} = H(f_{\mathrm{query}})$
Fetch: h_{stored} from Smart Contract State Σ
Claimed Token τ_{claim}
Compare Function $V(a_{\mathrm{query}}, \tau_{\mathrm{claim}})$
$V = \begin{cases} 1 & \text{if } d(h_{\mathrm{query}}, h_{\mathrm{stored}}) < \delta_{\mathrm{threshold}} \\ 0 & \text{otherwise} \end{cases}$
1 ✓
1 Verified
0 ✗
Not Verified

Figure 4. The overall model of the proposed blockchain-based art provenance system.

C. SELECTION OF CONSENSUS PROTOCOL AND NETWORK INFRASTRUCTURE

Blockchain technology is a peer-to-peer system where nodes communicate directly without the need for a central authority. For managing cultural heritage, a system must ensure *immutability*, *transparency*, *security*, and the ability to handle multiple stakeholders with different levels of access and authority. For a global cultural heritage management system, the underlying blockchain network must balance high security with environmental sustainability and transactional efficiency [25]. While early blockchain implementations relied on Proof-of-Work (PoW), this mechanism is increasingly untenable for heritage applications due to its prohibitive energy consumption and limited throughput. Consequently, our framework utilizes Proof-of-Stake (PoS), specifically the Ethereum 2.0 consensus protocol, which replaces computational expenditure with economic security [26-30].

In the PoS model, the security of the ledger is guaranteed by a set of validators $\mathcal{V} = \{\mathrm{v_1}, \mathrm{v_2}, \dots, \mathrm{v_n}\}$ who lock capital (stake) into a smart contract. The probability of a validator $\mathrm{v_i}$ being selected to propose the next block is proportional to their staked assets relative to the total network stake. Let *S* denote the total staked value in the network and $\mathrm{s_i}$ represent the stake of validator $\mathrm{v_i}$. The probability $\mathrm{P_{selection}(v_i)}$ is defined as:

$$\mathrm{P_{selection}(v_i)} = \frac{\mathrm{s_i}}{\sum_{\mathrm{j=1}}^{\mathrm{N}} \mathrm{s_j}} = \frac{\mathrm{s_i}}{\mathrm{S}}$$

This probabilistic selection mechanism eliminates the hardware arms race of PoW, significantly reducing the carbon footprint of the heritage management system. To ensure honest behavior, the protocol implements a mechanism known as *Slashing*. If a validator attempts to propose conflicting blocks or validate fraudulent transactions (an "equivocation" event), a portion of their stake is programmatically destroyed. The penalty function $\mathcal{L}$ for a malicious validator $\mathrm{v_{adv}}$ is proportional to the severity of the fault and the total stake:

$$\mathcal{L}(\mathrm{v_{adv}}) = \alpha \cdot \mathrm{s_{adv}}$$

where $\alpha \in (0,1]$ is the slashing factor. For the network to remain secure against a 51% attack, the total stake controlled by adversarial nodes $\mathrm{S_{adv}}$ must satisfy the condition:

$$\frac{\mathrm{S_{adv}}}{\mathrm{S}} < \frac{1}{3}$$

This threshold ensures that the economic cost of attacking the network exceeds the potential gain, providing a strong deterrent against provenance manipulation or censorship of art records. Ethereum 2.0 was selected as the settlement layer because its sufficiently large value of *S* makes the cost of corruption prohibitively high for any single actor, ensuring the immutable persistence of cultural heritage records.

While Ethereum provides the necessary security guarantees, direct interaction with Layer-1 nodes often introduces latency bottlenecks and synchronization issues that degrade the user experience in real-time applications. To address this, our system architecture integrates Alchemy as the primary node infrastructure provider, effectively operating as a specialized Blockchain-as-a-Service (BaaS) layer.

Directly managing self-hosted Ethereum nodes requires significant technical overhead to prevent "block drift," where nodes fall out of sync with the global state. Alchemy mitigates this through its *Supernode* architecture–a distributed system that replaces the concept of a single node with a scalable fleet of nodes behind a load balancer. This ensures that read operations, such as verifying an artifact's ownership history or retrieving its metadata, are served with high availability and data consistency. Furthermore, this infrastructure layer abstracts the complexity of the consensus mechanism, allowing the heritage application to scale horizontally as the number of registered artifacts and museum interactions grows. By coupling the economic security of Ethereum's PoS consensus with the high-throughput capabilities of Alchemy's middleware, the proposed system achieves a balance of decentralization, security, and operational efficiency suitable for the global art market.

D. PRACTICAL DEPLOYMENT AND SOFTWARE ARCHITECTURE OF THE DECENTRALIZED APPLICATION

The implementation of the cultural heritage management system relies on a decentralized application (DApp) architecture that bridges the gap between the deterministic state of the blockchain and the dynamic requirements of user interaction [31]. Unlike traditional web applications, this framework distributes the execution logic across three distinct layers: the presentation layer, the logic layer (Smart Contracts), and the data availability layer (IPFS/Blockchain) [32].

The presentation layer is developed as a web-based interface, leveraging libraries such as Web3.js or Ethers.js to establish a communication channel with the Ethereum network. However, direct communication from a client browser to the blockchain is resource-intensive and prone to connection timeouts. To resolve this, architecture utilizes Alchemy as the remote procedure call (RPC) provider. Alchemy acts as a middleware gateway, routing client requests (e.g., querying an artifact's provenance) through its distributed Supernode infrastructure. This ensures that the application maintains high responsiveness and data consistency without requiring the museum to host and maintain its own Ethereum nodes (Fig. 5).

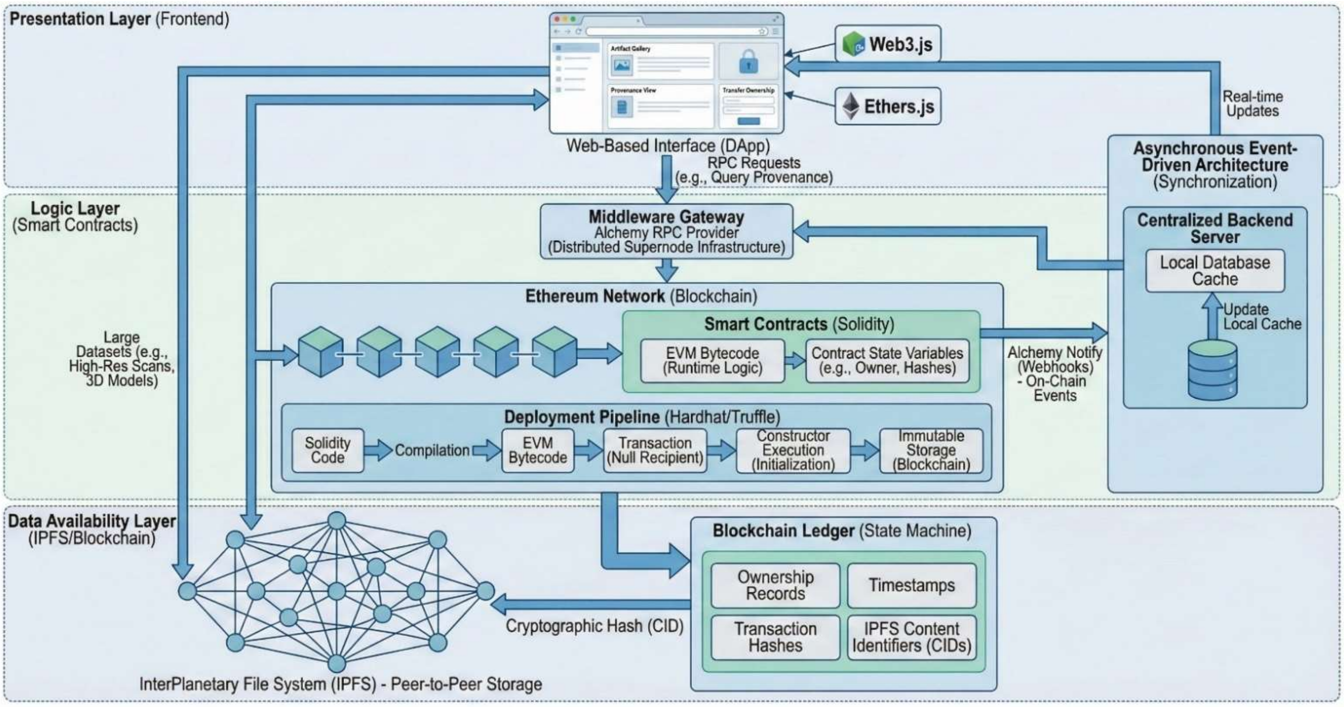
Presentation Layer (Frontend)
Artifact Gallery
Provenance View
Transfer Ownership
Web3.js
Ethers.js
Real-time Updates
Web-Based Interface (DApp)
RPC Requests (e.g., Query Provenance)
Asynchronous Event-Driven Architecture (Synchronization)
Logic Layer (Smart Contracts)
Middleware Gateway
Alchemy RPC Provider
(Distributed Supernode Infrastructure)
Centralized Backend Server
Local Database Cache
Update Local Cache
Ethereum Network (Blockchain)
Smart Contracts (Solidity)
EVM Bytecode (Runtime Logic)
Contract State Variables (e.g., Owner, Hashes)
Alchemy Notify (Webhooks) - On-Chain Events
Large Datasets (e.g., High-Res Scans, 3D Models)
Deployment Pipeline (Hardhat/Truffle)
Solidity Code
Compilation
EVM Bytecode
Transaction (Null Recipient)
Constructor Execution (Initialization)
Immutable Storage (Blockchain)
Data Availability Layer (IPFS/Blockchain)
Blockchain Ledger (State Machine)
Ownership Records
Timestamps
Transaction Hashes
IPFS Content Identifiers (CIDs)
Cryptographic Hash (CID)
InterPlanetary File System (IPFS) - Peer-to-Peer Storage

Figure. 5. The workflow of the cultural heritage DAPP.

The deployment process is a critical initialization phase. It begins with the compilation of the Solidity code into the Ethereum Virtual Machine (EVM) bytecode. A specialized transaction is then constructed containing this bytecode as the input data, with the recipient address field intentionally left null. Upon broadcast to the network, this transaction triggers the execution of the contract's constructor function. This constructor executes once, initializing the contract's state variables (e.g., setting the museum as the initial owner) and permanently writing the bytecode to the blockchain's immutable storage . Subsequent interactions with the contract invoke the *runtime* bytecode, which executes the specific logic for functions such as transferFrom or updateConditionReport.

To address the technical constraints of blockchain storage–specifically the high cost of storing large binary data like high-resolution spectral scans or 3D models–the system employs a hybrid storage strategy [33]. The blockchain serves exclusively as the "state machine" for essential transactional data (ownership, timestamps, and hashes) . Large datasets are offloaded to the InterPlanetary File System (IPFS), a decentralized peer-to-peer storage network. The smart contract stores only the cryptographic hash (Content Identifier or CID) of these files, ensuring that the off-chain data remains immutable and verifiable.

To maintain synchronization between the on-chain ledger and the off-chain user interface, the system implements an asynchronous event-driven architecture. The centralized backend server utilizes Alchemy Notify (Webhooks) to listen for specific on-chain events emitted by the smart contract. When a transaction is confirmed (e.g., an artifact is sold), Alchemy pushes the event data to the backend, which updates the local database cache. This design pattern ensures high system throughput and low latency for the end-user while guaranteeing that the blockchain remains the ultimate, tamper-proof source of truth.

IV. CONCLUSIONS

This research establishes a robust, technically viable architecture for the digital preservation of cultural heritage, effectively resolving the systemic inefficiencies of analog provenance tracking. By synthesizing cryptographic security with material science, the proposed framework bridges the critical gap between physical artifacts and their digital identities through the novel integration of Physically Unclonable Functions (PUFs). This "phygital" binding mechanism ensures that the blockchain record is not merely a registry of ownership, but a verifiable cryptographic anchor linked to the atomic structure of the art object itself.

Crucially, this work addresses the implementation barriers of latency and scalability by introducing an adaptive multi-blockchain framework. We demonstrated that a hierarchical infrastructure, anchoring high-value settlement on Layer-1 for maximum security while routing high-velocity telemetry to Layer-2 sidechains, dynamically resolves the trade-off between throughput and trust. This layered approach, supported by Alchemy's Supernode middleware for efficient data retrieval, ensures the system can handle continuous IoT monitoring without congestion. The proposed framework transforms the theoretical potential of distributed ledger technology into a concrete, deployable software supply chain. By replacing centralized reliance with scalable, tiered cryptographic verification, the system fosters a "trustless" environment where the authenticity of cultural history is preserved not by institutional authority, but by mathematical consensus and automated smart contract logic. This methodology lays the technical foundation for a globally interoperable art market, safeguarding the world's cultural assets against fraud and illicit trafficking for future generations.

ACKNOWLEDGEMENT

This research was supported by the Horizon Europe AURORA project, GA number: 101094245, and by the by the Ukrainian government project # 0123U100232 "Development the innovative methods and means for the deployment of the dual-purpose information infrastructure for the digital transformation of Ukraine". During the preparation of this work, the authors used OpenAI's GPT 5.2, Grammarly and Writefull tools for English proofreading and grammar correction of the original article text. Some images in the paper were generated using Google's Gemini 3, with detailed instructions and further editing by authors.

References

[1] D. Fincham, "Case Study 2: The Knoedler Art Forgery Network," *in The Palgrave Handbook on Art Crime*, 2019, pp. 343-361. https://doi.org/10.1057/978-1-137-54405-6_17.

[2] N. Charney, *The Art of Forgery: The Minds, Motives and Methods of the Master Forgers*, Germany: Phaidon Press, 2015.

[3] S. Greenhalgh, *A Forger's Tale: Confessions of the Bolton Forger*, Allen & Unwin, 2018.

[4] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available at: bitcoin.org, 2008.

[5] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440-16455, 2020, https://doi.org/10.1109/ACCESS.2020.2967218.

[6] A. Hafid, A. S. Hafid and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244-125262, 2020, https://doi.org/10.1109/ACCESS.2020.3007251.

[7] T. A. Alghamdi, R. Khalid and N. Javaid, "A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges," *IEEE Access*, vol. 12, pp. 79626-79651, 2024, https://doi.org/10.1109/ACCESS.2024.3408868.

[8] L. T. Thibault, T. Sarry and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, vol. 10, pp. 93039-93054, 2022, https://doi.org/10.1109/ACCESS.2022.3200051.

[9] L. D. Negka and G. P. Spathoulas, "Blockchain state channels: A state of the art," *IEEE Access*, vol. 9, pp. 160277-160298, 2021, https://doi.org/10.1109/ACCESS.2021.3131419.

[10] H. Mao, T. Nie, H. Sun, D. Shen and G. Yu, "A survey on cross-chain technology: Challenges, development, and prospect," *IEEE Access*, vol. 11, pp. 45527-45546, 2023, https://doi.org/10.1109/ACCESS.2022.3228535.

[11] M. Borkowski, M. Sigwart, P. Frauenthaler, T. Hukkinen and S. Schulte, "Dextt: Deterministic cross-blockchain token transfers," *IEEE Access*, vol. 7, pp. 111030-111042, 2019, https://doi.org/10.1109/ACCESS.2019.2934707.

[12] H. Tian et al., "Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3928-3941, 2021, https://doi.org/10.1109/TIFS.2021.3096124.

[13] S. Khan, M. B. Amin, A. T. Azar and S. Aslam, "Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability," *IEEE Access*, vol. 9, pp. 116672-116691, 2021, https://doi.org/10.1109/ACCESS.2021.3106384.

[14] D. Reijsbergen, A. Maw, J. Zhang, T. T. A. Dinh and A. Datta, "Demo: PIEChain - A practical blockchain interoperability framework," *Proceedings of the 2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS)*, Hong Kong, 2023, pp. 1021-1024, https://doi.org/10.1109/ICDCS57875.2023.00119.

[15] J. Seo, J. Lee, Y. Joo, K. Lee, V. Sugumaran and S. Park, "A blockchain-based e-participation framework utilizing zero-knowledge proofs with guaranteed sampling and differential reward mechanisms," *IEEE Access*, vol. 13, pp. 25752-25764, 2025, https://doi.org/10.1109/ACCESS.2025.3538006.

[16] L. Duan, Y. Sun, W. Ni, W. Ding, J. Liu and W. Wang, "Attacks against cross-chain systems and defense approaches: A contemporary survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 8, pp. 1647-1667, 2023, https://doi.org/10.1109/JAS.2023.123642.

[17] R. O'Dwyer, "Limited edition: Producing artificial scarcity for digital art on the blockchain and its implications for the cultural industries," *Convergence*, vol. 26, no. 4, pp. 874-894, 2020. https://doi.org/10.1177/1354856518795097.

[18] "Verisart | Protect your art with Web3 tools," [Online]. Available at: https://verisart.com/.

[19] "Artory - The Artory Registry," [Online]. Available at: https://www.artory.com/.

[20] "Transforming the Art Market with Blockchain Protocols; Codex Partnerships," *Medium*, 2018. [Online]. Available at: https://medium.com/codexprotocol/transforming-the-art-market-with-blockchain-protocols-codex-partnerships-96475d8f376.

[21] "Arteïa - Collection Management," [Online]. Available at: https://arteia.com/.

[22] "Blockchain, Creativity and Arts Intertwine: Use Cases and Notable Projects," *Medium*, 2019. [Online]. Available at: https://medium.com/the-capital/blockchain-creativity-and-arts-intertwine-use-cases-and-notable-projects-87cbb8797965.

[23] "Maecenas | The Art Investment Platform," [Online]. Available at: https://www.maecenas.co/.

[24] "5 companies using blockchain to open the art industry," *Decrypt*, 2018. [Online]. Available: https://decrypt.co/resources/how-blockchain-will-open-the-art-industry-up-to-the-everyday-person.

[25] D. Denysiuk, et al., "Blockchain-based deep learning algorithm for detecting malware," *CEUR Workshop Proceedings*, vol. 3373, 2023, pp. 529–538.

[26] I. Bashir, *Blockchain Consensus: An Introduction to Classical, Blockchain, and Quantum Consensus Protocols*, *Apress*, 2022. https://doi.org/10.1007/978-1-4842-8179-6.

[27] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: mechanism, design and applications," *Science China Information Sciences*, vol. 64, pp. 1–15, 2021. https://doi.org/10.1007/s11432-019-2790-1.

[28] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms," *Future Internet*, vol. 14, no. 2, p. 47, 2022. https://doi.org/10.3390/fi14020047.

[29] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Computing Surveys*, vol. 55, no. 13s, Article 278, pp. 1-35, 2023. https://doi.org/10.1145/3579845.

[30] Kraken, "Ethereum 2.0: The New Frontier of Blockchain Scalability," [Online]. Available at: https://www.kraken.com/uk-ua/learn/ethereum-2-0?utm_source=chatgpt.com.

[31] W. Cai et al., "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018. https://doi.org/10.1109/ACCESS.2018.2870644.

[32] Y. Zhao, R. An, D. Ou, and C. Jiang, "An InterPlanetary file system based picture archiving and communication system," *Proceedings of the 2020 Int. Conf. on Computer, Information and Telecommunication Systems (CITS)*, Hangzhou, China, 2020, pp. 1–5. https://doi.org/10.1109/CITS49457.2020.9232495.

[33] S. Schauer, J. Sieck, K. Lipianina-Honcharenko, A. Sachenko and I. Kit, "Use of digital auralised 3D models of cultural heritage sites for long-term preservation," *Proceedings of the 2023 IEEE 12th International*

Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 708-712, https://doi.org/10.1109/IDAACS58523.2023.10348637.

***TARAS MAKSYMYUK** is currently a Professor with the ICT Department, Lviv Polytechnic National University, and a Senior Systems Engineer of Advanced System Research Group at Infineon Technologies. His research interests include blockchain, Internet of Things and artificial intelligence.*

***FRANCESCO MELONI** works as an Advanced Analytics Professional for Avvale. He has worked in multiple projects covering both technical and Agile project management roles for the implementation of AI algorithms in different contexts, including artwork authenticity.*

***MATIAS TORRES DIAZ** is a blockchain consultant at Avvale with a background in programming and distributed systems. He focuses on developing practical blockchain solutions for real-world business challenges. Technology enthusiast with experience in implementing innovative applications in the emerging digital ledger space.*

***DOMENICO ROMANO** is the Lead AI R&D Researcher at AVVALE. He is a Member of the winter over crew at the Antarctic Italo/French base of Dome C(Concordia) Experienced Astrophysicist Doctoral Researcher with a demonstrated history of working in the higher education industry. Skilled in Mathematical Modeling, IDL, Python, PHP, Fortran, Javascript.*

***LORENZO BELUCCI** is a scientist in the field of diagnostics applied to the study of cultural heritage. He gained experience in some leading private companies and has been scientific director of DRIART AG since 2010. He collaborates with the University of Florence and contributed to founding OTID srl, a start-up created for the technological development of Digital Identity applied to Cultural Heritage.*

***NATALIA CHUKHRAY** Prof. Dr. hab. is a Head of the Department of Management of Organizations at Lviv Polytechnic National University. Prof. Chukhray has a Habilitation in Innovation Management from Lviv Polytechnic National University (Ukraine, 2003) and Ph.D. in Economics from Lviv Polytechnic National University (Ukraine, 1993). Nataliya has a good track record in acquiring national research projects and leads interdisciplinary research projects and groups. She has published more than 350 scientific papers in conferences and journals and has supervised more than 20 doctoral students. Nataliya has also extensive experience in delivering professional consulting and training support to Ukrainian and foreign companies, local authorities, and potential businessmen in the sphere of knowledge management processes, services design and business models.*