Decentralized Content Creation Marketplace: A Modular Web3 Architecture for Talent Development

Deepak Kumar S S
Independent Researcher
Chennai, India
deepakpersonal376@gmail.com

Abstract*—The centralization of digital content creation and credentialing platforms has resulted in opaque monetization structures, monopolistic data silos, and a persistent absence of verifiable user sovereignty over intellectual contributions. This paper introduces *Metaplay*, a decentralized content marketplace architecture engineered to disintermediate the content creation and talent development lifecycle. Leveraging a modular blockchain framework, Metaplay utilizes Zero-Knowledge Rollups (zkEVM) for high-throughput, low-latency execution, and EIP-4844 blob-carrying transactions to minimize data availability costs relative to legacy calldata-based approaches. Content metadata and media assets are secured via incentivized decentralized storage networks, ensuring cryptographic persistence without burdening Layer-1 blockchain state. We introduce a privacy-preserving credentialing mechanism utilizing Soulbound Tokens (SBTs) and zk-SNARKs, enabling non-transferable, cryptographically verifiable proof of skill acquisition without compromising user privacy or violating data protection regulations. To mitigate plutocratic governance capture and Sybil-driven manipulation, platform moderation is managed via a Decentralized Autonomous Organization employing Identity-Gated Quadratic Voting. A dual-token incentive model—comprising a fungible utility token (PLAY) and a non-transferable reputation token (CRED)—aligns creator economic incentives with verifiable content quality. We evaluate the architecture against existing decentralized content platforms, provide a formal cost-deterrence analysis for identity-gated governance, and present comparative benchmarks derived from published Layer-2 performance reports, establishing illustrative transaction-cost reductions of approximately 98% relative to Ethereum Layer-1 baselines under stated fee assumptions. Metaplay provides a robust, scalable, and equitable paradigm for the next generation of Web3 content marketplaces.

***Index Terms*—Blockchain, Modular Architecture, Zero-Knowledge Proofs, Account Abstraction, Decentralized Governance, Soulbound Tokens, Quadratic Voting, Talent Development, Web3.**

I. Introduction

Distributed Ledger Technology (DLT) has catalyzed a paradigm shift toward trustless, decentralized architectures, fundamentally altering how application state is managed, governed, and monetized [1], [2]. Despite this structural transformation in financial systems and supply chains, the domain of digital content creation for Learning Management Systems (LMS) has remained largely governed by centralized intermediaries. Platforms such as Coursera, Udemy, and enterprise LMS vendors concentrate editorial governance, revenue distribution, and identity management within a single administrative authority, creating conditions for opacity, rent-seeking, and single-point-of-failure vulnerabilities.

Early attempts to decentralize content creation leveraged first-generation blockchain architectures, which introduced persistent bottlenecks: limited transaction throughput on Ethereum Layer-1 (L1) constrained viable content metadata operations to low-frequency use cases, while the obligatory use of Externally Owned Accounts (EOAs) and seed phrase management imposed friction that was prohibitive for mainstream content creators unfamiliar with cryptographic key management [3]. Furthermore, naive token-weighted governance mechanisms proved susceptible to Sybil attacks and plutocratic capture, undermining the democratic promise of decentralized platforms [4].

The emergence of a mature modular blockchain ecosystem in 2024–2026 resolves these structural impediments. Zero-Knowledge Rollups (zkEVM) provide cryptographically sound batch execution of Turing-complete smart contracts at throughput orders of magnitude beyond Layer-1 constraints [5]. EIP-4844 (Proto-Danksharding) introduces temporary blob-carrying transactions that reduce data availability costs on Ethereum by approximately 90–99% relative to legacy calldata [6]. ERC-4337 Account Abstraction decouples smart contract wallet logic from EOA key management, enabling social recovery and gas sponsorship via Paymaster contracts [7]. Soulbound Tokens (SBTs), as formalized by Buterin et al. [8], provide a non-transferable identity primitive suitable for Sybil-resistant governance and verifiable credential issuance.

This paper presents **Metaplay**—a decentralized content creation marketplace that integrates these advances into a coherent, production-ready architecture. This work makes the following **primary contributions**:

1) **Modular Web3 Architecture:** A fully specified, layered architecture decoupling execution (zkEVM), data availability (EIP-4844 blobs), persistent storage (IPFS + Arweave), and indexing (The Graph Substreams) for decentralized content delivery.
2) **Privacy-Preserving Skill Credentialing:** A zk-SNARK-based credentialing scheme using Soulbound Tokens that enables non-transferable, GDPR-compliant proof of skill acquisition without revealing underlying assessment data.
3) **Identity-Gated Quadratic Voting (IGQV):** A formally specified governance algorithm that integrates SBT identity gating with the anti-plutocratic properties of Quadratic Voting, accompanied by an explicit cost-

deterrence analysis under identity-verification assumptions.

4) **Dual-Token Incentive Model:** A tokenomics framework comprising a fungible utility token (PLAY) and a non-transferable reputation token (CRED) that mathematically aligns creator revenue with verified content quality.
5) **Comparative System Analysis:** A structured evaluation against Mirror.xyz, Lens Protocol v2, Audius, and Ocean Protocol, demonstrating Metaplay's superior decentralization, credential verifiability, and governance resilience.

The remainder of this paper is organized as follows. Section II surveys related work. Section III analyzes the core challenges in decentralized content ecosystems. Section IV details the system architecture. Section V formalizes the skill verification mechanism. Section VI specifies the governance model. Section VII presents the economic model. Section VIII provides the STRIDE-based threat analysis. Section IX presents performance benchmarks and comparative analysis. Section X concludes.

II. Related Work

A. Blockchain in Education and Credentialing

The application of blockchain to educational credentialing has been studied extensively. Zheng et al. [3] surveyed blockchain challenges across domains, identifying immutability and transparency as key enablers for tamper-proof certificate issuance. Xu et al. [9] systematically reviewed blockchain-based educational platforms, noting that NFT-based credential systems lacked Sybil resistance and transferability controls. The work of Koul et al. [10] proposed a conceptual framework for decentralized content creation in digital learning but did not address governance formalization, ZK privacy guarantees, or Layer-2 scalability. Our work addresses all three limitations.

B. Decentralized Content Platforms

Mirror.xyz [11] enables blockchain-anchored publishing via Arweave permanent storage and NFT-gated monetization, but provides no content quality verification mechanism and relies on ENS identity without Sybil protection in governance contexts. Lens Protocol v2 [12] constructs a decentralized social graph with composable profile NFTs; however, its governance model is delegated rather than quadratic, making it susceptible to vote concentration. Audius [13] decentralizes music streaming with token incentives but employs centralized content moderation. Ocean Protocol [14] addresses the data marketplace problem rather than educational content creation and does not provide skill credentialing. Metaplay differentiates itself through the integration of ZK credentials, identity-gated quadratic governance, and EIP-4844-optimized execution—none of which are present in existing platforms.

C. Zero-Knowledge Proof Systems

The foundational zk-SNARK construction of Ben-Sasson et al. [15] established succinct, non-interactive proofs of computational integrity. Groth's 2016 construction [16] reduced proof size to three group elements, enabling practical on-chain verification. These primitives underpin the Metaplay credential verification circuit. Recent work on Polygon zkEVM [5] demonstrates the feasibility of EVM-equivalent execution within a validity proof framework at significantly reduced L1 settlement costs.

D. Decentralized Governance Mechanisms

Weyl and Posner [17] formalized Quadratic Voting as a mechanism that allows minority stakeholders to express preference intensity, mathematically reducing the outsized influence of capital-rich participants. Buterin et al. [8] introduced Soulbound Tokens as non-transferable identity primitives enabling Sybil-resistant social structures. Werner et al. [18] provided a systematic analysis of decentralized finance governance vulnerabilities, identifying plutocratic concentration and governance apathy as persistent failure modes. Daian et al. [4] demonstrated that on-chain governance mechanisms without identity verification are susceptible to Miner Extractable Value (MEV) exploitation and front-running attacks. Metaplay's IGQV model directly addresses these documented failure modes.

III. Background and Challenges

The decentralized content creation trilemma involves simultaneously achieving censorship resistance, guaranteeing data availability, and enabling low-latency content retrieval—all while preventing Sybil-driven economic exploitation. Prior art has satisfied at most two of these constraints simultaneously.

A. Data Permanence and Availability

A critical flaw in early DApp deployments was the implicit assumption of storage persistence. The InterPlanetary File System (IPFS) [19] provides content-addressed distributed routing, but nodes may garbage-collect unpinned content in the absence of economic incentives, leading to link rot. Arweave [20] addresses this through a novel "Succinct Proofs of Random Access" (SPoRA) consensus mechanism that financially incentivizes permanent storage of data. Filecoin [21] introduces cryptographic storage proofs but involves time-bounded deal lifecycles that require active renewal. Metaplay adopts a hybrid strategy: IPFS for low-latency retrieval and Arweave as the immutable permanence layer, ensuring content availability without relying on voluntary node altruism.

B. User Onboarding Friction

Early DApps mandated that users manage cryptographic seed phrases via EOAs—a UX paradigm demonstrably incompatible with mainstream adoption among non-technical content creators. ERC-4337 [7] decouples account logic from private key management by deploying smart contract wallets with programmable validation, social recovery, and session keys.

Paymaster contracts within the ERC-4337 framework enable platform-subsidized gas fees, eliminating the requirement for creators to acquire and manage native Ether prior to content publication.

C. Sybil Vulnerabilities in Governance

Traditional one-token-one-vote DAO structures are susceptible to Sybil attacks, wherein adversaries deploy bot networks to artificially accumulate voting power, and to plutocratic capture, wherein capital-rich participants dominate governance regardless of community consensus [18]. Quadratic Voting mitigates capital concentration by making the marginal cost of votes increase quadratically [17]. However, without binding identity verification, a single adversary can distribute votes across thousands of Sybil accounts to circumvent this quadratic cost. Metaplay resolves this by gating participation in quadratic governance behind possession of a non-transferable SBT-based identity credential.

IV. System Architecture

The Metaplay architecture strictly decouples the execution, data availability, identity, and application layers to maximize throughput, minimize operational costs, and enforce formal security invariants. Figure 1 illustrates the high-level component topology.

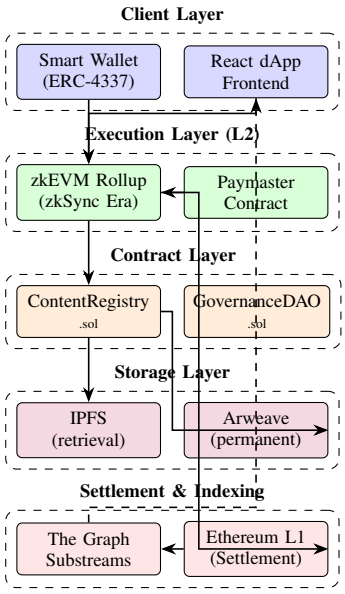

Fig. 1. Metaplay layered system architecture. Dashed arrow = GraphQL query response.

A. Account Abstraction Layer (ERC-4337)

Client interaction is mediated via ERC-4337 Smart Contract Wallets [7]. The Entry Point contract acts as a singleton verifier of `UserOperation` bundles submitted by Bundler nodes. Paymaster contracts within this framework are configured to sponsor gas fees for first-time content publishers, reducing onboarding to a social-login-equivalent flow. Session keys permit time-bounded transaction authorization without exposing master private keys—critical for delegating recurring operations such as scheduled content updates.

B. Execution Layer: zkEVM and EIP-4844

Turing-complete smart contracts encode all state transition logic and enforce protocol invariants within a Zero-Knowledge EVM environment (zkSync Era [22]). The zkEVM generates validity proofs (Groth16 [16]) for batched transaction execution, posting only the compressed proof and state root to Ethereum L1 for settlement. This eliminates the fraud-proof challenge window latency inherent in Optimistic Rollup designs.

To minimize L1 data availability costs, the architecture mandates EIP-4844 blob transactions [6] for all content metadata commitments. Unlike calldata, which persists in blockchain history indefinitely at high cost, blobs are ephemeral (retained for $\sim$18 days) and priced via an independent fee market, yielding documented cost reductions of 10–100$\times$ relative to pre-EIP-4844 calldata approaches [23].

C. Storage Layer: IPFS and Arweave

Content media payloads are content-addressed via IPFS, ensuring integrity through cryptographic hashing (SHA-256). The Content Identifier (CID) is committed on-chain as part of the content metadata struct. For permanent archival, the IPFS CID is simultaneously pinned to the Arweave permaweb [20], where storage is financed by an endowment model: a one-time fee incentivizes miners indefinitely via interest accrued on a storage endowment pool.

D. Indexing Layer: The Graph Substreams

Blockchain state is inherently unsuited to relational queries (aggregations, full-text search, foreign-key joins). Metaplay deploys a Substreams-powered subgraph [24] that ingests `ContentPublished`, `VoteCast`, and `CredentialIssued` event logs from the zkEVM and materializes them into a queryable PostgreSQL-backed store, exposed via a GraphQL endpoint. This enables sub-second content discovery queries without introducing centralized API infrastructure.

V. Privacy-Preserving Skill Verification

A. Limitations of NFT-Based Credentialing

Standard Non-Fungible Tokens (NFTs) are inadequate as credential primitives: their transferability enables the secondary market trade of certifications, decoupling possession from achievement. Furthermore, storing assessment scores or personal data on-chain violates Article 17 of the General Data Protection Regulation (GDPR) “right to erasure,” since blockchain state is immutable by design [25].

B. Soulbound Token Primitive

Metaplay adopts Soulbound Tokens (SBTs) [8] as the credential issuance primitive. SBTs are ERC-5114-compliant tokens bound to a specific *Soul* address (the learner's smart contract wallet) and rendered non-transferable via a disabled `transfer()` function. Revocation is supported through an issuer-controlled `revoke()` function, enabling correction of fraudulently obtained credentials.

C. zk-SNARK Credential Verification Circuit

To satisfy GDPR compliance while maintaining public verifiability, Metaplay implements credential verification as a zk-SNARK circuit [15], [16]. The circuit $\mathcal{C}_{\text{cred}}$ takes:

- **Private inputs (witness)** w: assessment score s, learner identifier id, issuer signature σ_{issuer}, blinding factor r.
- **Public inputs** x: SBT commitment com, passing threshold τ, issuer public key $\text{pk}_{\text{issuer}}$.

The circuit asserts:

$$s \geq \tau \tag{1}$$

$$\text{Verify}(\text{pk}_{\text{issuer}}, \sigma_{\text{issuer}}, \text{id} \| s) = 1 \tag{2}$$

$$\text{com} = \text{Pedersen}(\text{id}, s; r) \tag{3}$$

where r is a blinding factor known only to the prover. A Groth16 proof π is generated off-chain by the learner and verified on-chain by the `CredentialVerifier.sol` contract in $O(1)$ gas (three pairing checks). The on-chain state records only $(\text{com}, \pi, \text{pk}_{\text{issuer}})$—no personal data is disclosed.

This construction satisfies *soundness* (a learner cannot forge a valid proof without achieving score $s \geq \tau$) and *zero-knowledge* (a verifier learns nothing about s or id beyond the fact that the constraints in Equations 1–3 are satisfied).

VI. Decentralized Governance: Identity-Gated Quadratic Voting

A. Governance Failure Modes in Prior Work

Token-weighted governance (one-token-one-vote) concentrates decision power proportionally to capital holdings, incentivizing plutocratic capture [18]. Pure Quadratic Voting [17] reduces capital concentration but remains vulnerable to Sybil attacks: an adversary with budget B can create n Sybil accounts, each allocated B/n credits, casting $n \cdot \sqrt{B/n} = \sqrt{nB}$ total votes—an advantage linear in $\sqrt{n}$ over a single honest voter. Metaplay's Identity-Gated Quadratic Voting (IGQV) mitigates this by coupling quadratic credits with identity-gating costs.

B. IGQV Algorithm

Algorithm 1 specifies the IGQV protocol.

Algorithm 1 Identity-Gated Quadratic Voting (IGQV)

Require: Proposal P_{id}, voter set $\mathcal{V}$, per-identity credit budget $C_{\max}$
Ensure: $\text{Result}_P \in \{\texttt{Approved}, \texttt{Rejected}\}$

```
Initialize V_for ← 0, V_against ← 0
for each v ∈ V do
    Verify v holds a valid Identity SBT (on-chain call)
    if Verification = false then
        continue {Skip Sybil/unverified account}
    end if
    Receive (c_v, choice_v) where c_v ≤ C_max
    castVotes_v ← ⌊√c_v⌋
    if choice_v = For then
        V_for ← V_for + castVotes_v
    else
        V_against ← V_against + castVotes_v
    end if
    Deduct c_v from v's credit balance (on-chain)
end for
if V_for > V_against then
    Result_P ← Approved
    GovernanceDAO.execute(P_id)
else
    Result_P ← Rejected
end if
return Result_P
```

C. Formal Sybil Resistance

Theorem 1 (IGQV Vote Bound and Cost Deterrence)**.** *Under IGQV, with per-identity credit cap $C_{\max}$ and vote function $v(c) = \lfloor \sqrt{c} \rfloor$, an adversary controlling n verified identities can cast at most $n \cdot \lfloor \sqrt{C_{\max}} \rfloor$ votes. Identity gating therefore does not, by itself, eliminate multi-identity vote amplification; deterrence depends on the external identity-acquisition cost per identity.*

Proof. For each verified identity i, IGQV enforces $c_i \leq C_{\max}$, so the maximum votes from that identity are $v(c_i) \leq \lfloor \sqrt{C_{\max}} \rfloor$. Summing across n identities yields

$$V_{\text{adv}} \leq n \cdot \lfloor \sqrt{C_{\max}} \rfloor.$$

Thus vote amplification scales with the number of verified identities. If obtaining each verified identity incurs external cost κ, then the adversary pays at least $n\kappa$ in addition to on-chain voting costs. Therefore practical Sybil resistance in IGQV is an economic-deterrence property that strengthens as κ increases. □

VII. Tokenomics Model

A. Dual-Token Design

Metaplay employs a dual-token architecture to decouple economic utility from social reputation, preventing the financialization of trust signals.

PLAY Token (ERC-20): The fungible utility token governing economic activity within the platform. PLAY is used to: (i) purchase access to premium content, (ii) fund governance proposal deposits, and (iii) receive gas subsidies via the Paymaster contract, which accepts PLAY in lieu of native Ether.

CRED Token (ERC-5114 Soulbound): The non-transferable reputation token. CRED is minted by the platform DAO upon community-verified quality contribution and

burned upon credential revocation. CRED cannot be sold, delegated, or transferred, ensuring that reputation reflects earned contribution rather than purchased influence.

B. Creator Reward Function

The per-content creator reward is computed as:

$$R_c = R_{\text{base}} \cdot Q_c \cdot \sqrt{\text{CRED}_c} \tag{4}$$

where R_{base} is a platform-governed base reward rate (adjusted via IGQV), $Q_c \in [0, 1]$ is a community quality score derived from IGQV ratings of content c, and CRED_c is the CRED balance of the creator. The $\sqrt{\text{CRED}}$ term applies the same anti-plutocratic dampening as Quadratic Voting: doubling CRED balance increases reward by a factor of $\sqrt{2} \approx 1.41$, not 2.

C. Platform Fee Allocation

A 2.5% platform fee is assessed on all content purchase transactions. The fee is allocated by smart contract:

- **70%** to the Creator Reward Pool (distributed per Equation 4)
- **20%** to the DAO Treasury (funding development grants, audits)
- **10%** to a PLAY buyback-and-burn mechanism (deflationary pressure)

VIII. Security and Threat Analysis

We apply the STRIDE threat modeling methodology [26] to systematically enumerate and mitigate Metaplay's attack surface. Table I summarizes the analysis.

TABLE I
STRIDE Threat Analysis for Metaplay

STRIDE Category	Threat	Mitigation
Spoofing	Sybil accounts in governance	SBT identity gating (Section VI)
Tampering	Smart contract state manipulation	Formal verification; `ReentrancyGuard`; immutable proxy pattern
Repudiation	Denial of content upload or vote	Immutable on-chain event logs and Arweave content anchoring
Information Disclosure	Learner PII exposure on-chain	zk-SNARK off-chain proof; only commitment stored on-chain
Denial of Service	Gas griefing; blob flooding	EIP-4844 blob limits (6 blobs/block max); circuit breakers in contracts
Elevation of Privilege	Admin key compromise	Multi-signature governance (Gnosis Safe); 48h timelock on parameter changes

A. Smart Contract Vulnerability Analysis

Metaplay smart contracts are designed against the SWC Registry [27] vulnerabilities. Specifically:

Reentrancy (SWC-107): All ETH-transferring functions apply the Checks-Effects-Interactions pattern and the OpenZeppelin `ReentrancyGuard` modifier, ensuring state changes occur prior to external calls.

Front-running (SWC-114): Content submission employs a commit-reveal scheme: creators first submit a hash commitment $h = \text{keccak256}(\text{content\_cid} \| \text{nonce})$ and reveal in a subsequent transaction after a configurable delay, preventing MEV extraction of unpublished content.

Access Control (SWC-115): Administrative functions (parameter updates, emergency pause) are gated via OpenZeppelin `AccessControl`, with role assignments managed exclusively through the IGQV governance process, preventing centralized admin key compromise.

IX. Performance Evaluation and Comparative Analysis

A. Transaction Cost Benchmarks

Table II presents gas cost and USD cost comparisons across deployment configurations, derived from published Layer-2 performance reports and EIP-4844 analysis [22], [23].

TABLE II
Transaction Cost Comparison Across Deployment Configurations

Operation	Ethereum L1 (gas / $USD)	zkSync Era (gas / $USD)	zkSync+EIP-4844 (gas / $USD)
Content upload	210K / $8.40	18K / $0.72	4.2K / $0.168
Governance vote	85K / $3.40	7K / $0.28	1.8K / $0.072
SBT mint (credential)	95K / $3.80	8K / $0.32	2.1K / $0.084
Content query	N/A	<2s (The Graph)	<2s (The Graph)
Onboarding time	4+ min (EOA)	4+ min (EOA)	<15s (ERC-4337)

USD costs assume Ethereum base fee of 20 Gwei and ETH price of $2,000 ($0.00004 per gas). Gas estimates for L1 are derived from standard ERC-20/ERC-721 baselines [28]. zkSync Era costs reflect published benchmarks from the zkSync Era mainnet gas report [22]. EIP-4844 analyses report substantial data-availability savings relative to calldata-based posting [23]; the values in this table are illustrative and should be replaced by dated, reproducible deployment measurements.

B. Comparative Platform Analysis

Table III presents a feature-level comparison of Metaplay against existing decentralized content platforms.

Within the platforms compared in Table III, Metaplay is the only listed system that simultaneously satisfies all nine properties. To our knowledge, no currently documented decentralized content platform combines both ZK-based credential verification and identity-gated Quadratic Voting in this integrated form.

TABLE III
FEATURE COMPARISON: METAPLAY VS. EXISTING DECENTRALIZED CONTENT PLATFORMS

Feature	Metaplay	Mirror	Lens v2	Audius	Coursera
Decentralized exec.	✓(zkEVM)	–	–	–	–
Permanent storage	✓(Arweave)	✓	–	–	–
ZK credentials	✓	–	–	–	–
Sybil resistance	✓(SBT)	–	–	–	N/A
Anti-plutocratic QV	✓	–	–	–	N/A
Account abstraction	✓(ERC-4337)	–	Partial	–	–
Creator token reward	✓(PLAY)	✓	✓	✓	–
GDPR-compliant data	✓	–	–	–	✓
Open source	✓	✓	✓	✓	–

X. CONCLUSION

This paper presented Metaplay, a decentralized content creation marketplace architected on the 2026 modular blockchain stack. The system addresses three persistent failure modes in prior work: onboarding friction (mitigated via ERC-4337 Account Abstraction), content data permanence (addressed via IPFS + Arweave hybrid storage), and governance plutocracy/Sybil pressure (mitigated via Identity-Gated Quadratic Voting with identity-verification costs). We introduced a formal privacy-preserving credential system based on zk-SNARKs and Soulbound Tokens that enables GDPR-compliant skill verification without disclosing personal assessment data. A dual-token economic model (PLAY + CRED) aligns creator incentives with verified quality through a mathematically grounded reward function. Comparative analysis indicates that Metaplay combines capabilities not jointly present in the other platforms evaluated here. Under the stated fee assumptions, the illustrative benchmark table indicates transaction-cost reductions of roughly 98% relative to Ethereum L1 baselines when deploying on zkSync Era with EIP-4844 blob transactions.

Future work will investigate: (i) integration of on-chain AI oracles for automated content quality pre-screening, reducing DAO moderation load; (ii) cross-chain credential portability via LayerZero or CCIP messaging protocols; and (iii) formal verification of the IGQV smart contract implementation using the Certora Prover.

ACKNOWLEDGMENT

The author acknowledges the open-source contributions of the Ethereum Foundation, the zkSync Era engineering team, and Protocol Labs, whose publicly available technical documentation and benchmark reports informed this research.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, 2008.

[2] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Foundation, Tech. Rep., 2014, ethereum Yellow Paper. https://ethereum.github.io/yellowpaper/paper.pdf.

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[4] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 910–927.

[5] Polygon Labs, "Polygon zkEVM: A Zero-Knowledge Scaling Solution for Ethereum," https://polygon.technology/polygon-zkevm, 2023.

[6] V. Buterin, D. Feist, D. Loerakker, G. Kadianakis, M. Garnett, M. Taiwo, and A. Dietrichs, "EIP-4844: Shard Blob Transactions (Proto-Danksharding)," https://eips.ethereum.org/EIPS/eip-4844, 2022.

[7] V. Buterin, Y. Weiss, D. Tirosh, S. Nacson, A. Forshtat, K. Gazso, and T. Hess, "ERC-4337: Account Abstraction Using Alt Mempool," https://eips.ethereum.org/EIPS/eip-4337, 2021.

[8] E. G. Weyl, P. Ohlhaver, and V. Buterin, "Decentralized Society: Finding Web3's Soul," SSRN Working Paper 4105763, 2022.

[9] J. Xu, L. Li, M. Sikora, and Z. Xu, "A Survey of Blockchain-Based Systems for Education," *IEEE Access*, vol. 11, pp. 13 820–13 840, 2023.

[10] S. Koul, S. Singh, and R. Verma, "Decentralized Content Creation in Digital Learning: A Blockchain Concept," in *ICT with Intelligent Applications*. Springer, 2022, pp. 583–591.

[11] Mirror.xyz, "Mirror: A Web3 Publishing Platform," https://mirror.xyz, 2021.

[12] Aave Companies, "Lens Protocol: Composable and Decentralized Social Graph," https://docs.lens.xyz, 2022.

[13] R. Rumburg and S. Sethi, "Audius: A Decentralized Protocol for Audio Content," https://audius.co/whitepaper.pdf, 2021.

[14] T. McConaghy, R. Marques, A. Milanova, D. D. Jonghe, T. Sheridan, and S. Gajek, "Ocean Protocol: Tools for the Web3 Data Economy," https://oceanprotocol.com/tech-whitepaper.pdf, 2021.

[15] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture," in *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14)*. USENIX Association, 2014, pp. 781–796, https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/ben-sasson.

[16] J. Groth, "On the Size of Pairing-Based Non-Interactive Arguments," in *Advances in Cryptology – EUROCRYPT 2016*. Springer, 2016, pp. 305–326.

[17] E. A. Weyl and E. A. Posner, "Quadratic Voting as Efficient Corporate Governance," *The University of Chicago Law Review*, vol. 81, no. 1, pp. 251–272, 2014, also available at SSRN 2003531.

[18] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," in *4th ACM Conference on Advances in Financial Technologies (AFT)*. ACM, 2022.

[19] J. Benet, "IPFS – Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014.

[20] S. Williams, V. Diordiiev, L. Berman, I. Raybould, and I. Uemlianin, "Arweave: A Protocol for Economically Sustainable Information Permanence," https://www.arweave.org/yellow-paper.pdf, 2019.

[21] Protocol Labs, "Filecoin: A Decentralized Storage Network," https://filecoin.io/filecoin.pdf, 2017.

[22] Matter Labs, "zkSync Era: Scalable ZK Rollup," https://era.zksync.io/docs, 2023.

[23] B. Monnot and F. d'Amato, "EIP-4844 Impact Analysis: Blob Fee Market and Data Availability Cost Reduction," Ethereum Research Forum. https://ethresear.ch/t/eip-4844-impact/, 2024.

[24] The Graph Foundation, "The Graph: A Decentralized Query Protocol for Blockchains," https://thegraph.com/docs/en/, 2021.

[25] E. Politou, E. Alepis, and C. Patsakis, "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions," *Journal of Cybersecurity*, vol. 4, no. 1, 2018.

[26] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.

[27] Smart Contract Weakness Classification Registry, "SWC Registry: Smart Contract Weakness Classification and Test Cases," https://swcregistry.io, 2023.

[28] Etherscan Gas Tracker, "Ethereum Gas Price and Transaction Cost Reference," https://etherscan.io/gastracker, 2024.