Peer-to-Peer Networking and Applications (2025) 18:254
https://doi.org/10.1007/s12083-025-02032-6

Scalable & secure real-world asset tokenization using ethereum staking & layer-2 solutions

Xiaofei Zhao[1,2] · Jieqiong Ding[3] · Yunqi Su[1] · Hua Wang[4] · Fanglin Guo[4] · Qianggang Zhang[1] · Mingyang Mu[1]

Received: 3 January 2025 / Accepted: 30 May 2025
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2025

Abstract

Real-world asset (RWA) tokenization holds immense promise for revolutionizing financial markets, but existing solutions face a critical bottleneck: the simultaneous need for scalability, security, and decentralized governance. Many platforms prioritize one or two of these, often at the expense of the others. Scalability and security challenges hinder its widespread adoption. This paper proposes a novel framework leveraging Ethereum staking and Layer-2 scaling solutions to address these limitations. Our framework utilizes a hybrid token standard (ERC-20/ERC-721) for representing diverse asset classes and incorporates a robust due diligence process. Uniquely, ETH staking is integrated to incentivize validators and secure the Layer-2 network, which employs Optimistic Rollups for enhanced transaction throughput and reduced costs. A decentralized oracle network provides secure real-world data feeds, while a Decentralized Autonomous Organization (DAO) governs the platform. The parameters of core system such as reward mechanism, slashing and oracle are determined by DAO. The framework acknowledges and addresses the complex and evolving regulatory landscape surrounding RWA tokenization, including considerations related to asset classification, KYC/AML compliance, and jurisdictional variations. A comprehensive security analysis identifies and mitigates potential vulnerabilities, focusing on smart contract security, oracle manipulation, and Layer-2 attacks. A case study demonstrates the practical application of the framework for metering electricity consumption in appliances. Experimental results, based on a simulated blockchain environment, validate the framework's feasibility and efficiency, achieving significant improvements in transaction throughput and gas cost reductions compared to traditional Layer-1 solutions. These results demonstrate the potential of the framework to address the key challenges of RWA tokenization. We discuss the framework's advantages and limitations, highlighting its novel combination of staking for Layer-2 security and a DAO-governed approach, and analyze its potential to democratize access to RWAs, enhance liquidity, and streamline asset management processes. Future research directions include exploring alternative Layer-2 solutions, enhancing security measures, and investigating interoperability with other blockchain platforms.

Keywords Real-world asset tokenization · Blockchain · Ethereum · Layer-2 scaling · Optimistic rollups · Staking · Decentralized governance · DAO · Oracle · Security · Smart contracts

1 Introduction

Real-world asset (RWA) tokenization represents a paradigm shift in finance, bridging the gap between traditional assets and the burgeoning blockchain ecosystem. This process involves representing ownership of physical or digital assets, such as real estate [1], commodities [2], intellectual property [3], or fine art [4], as digital tokens on a blockchain [5, 6]. This unlocks a multitude of benefits, including increased liquidity, fractional ownership, faster and more efficient settlement, reduced transaction costs, and enhanced transparency [7, 8]. The growing importance of RWA tokenization stems from its potential to democratize access to previously illiquid investments, streamline complex processes, and create new opportunities for global capital formation [9]. By leveraging the inherent security and immutability of blockchain technology, RWA tokenization offers a more efficient and transparent way to manage and transfer ownership of valuable assets, paving the way for a more inclusive and dynamic financial landscape [9–11]. The potential for growth in this sector is substantial, with projections indicating a significant expansion of the RWA tokenization market in the coming years as institutional and individual investors alike recognize its transformative power. However, realizing this potential requires

Extended author information available on the last page of the article

Published online: 25 July 2025

overcoming existing limitations in scalability and security, which are crucial for fostering widespread adoption and trust [5, 9]. Table 1 lists the abbreviations used throughout this paper with their full forms and example usages.

The current RWA landscape presents a compelling mix of challenges and opportunities, as illustrated in Fig. 1. While the potential benefits of tokenization are substantial, several obstacles hinder its widespread adoption. Scalability remains a major hurdle, as existing blockchain networks struggle to handle the high transaction volume required for efficient RWA trading [11, 12]. This limitation leads to increased transaction costs and slower settlement times, diminishing the appeal of tokenized assets. Security concerns also loom large, with the risk of smart contract vulnerabilities and exploits posing a significant threat to investor funds. Furthermore, the complex regulatory landscape surrounding digital assets adds another layer of complexity, requiring careful navigation to ensure compliance and build trust [13, 14]. Establishing clear legal frameworks for tokenized assets is crucial for fostering institutional adoption and mitigating regulatory uncertainty. Interoperability between different blockchain platforms is also a key challenge, limiting the seamless transfer and exchange of tokenized assets across various ecosystems [15, 16].

Despite these challenges, the opportunities within the RWA landscape are immense. The sheer size of the global asset market, encompassing trillions of dollars worth of real estate, commodities, and other assets, presents a vast potential market for tokenization. Moreover, the increasing demand for fractional ownership and greater liquidity is driving innovation in RWA platforms [17, 18]. The development of robust Layer-2 scaling solutions and more secure smart contract technologies offers promising pathways to address the scalability and security challenges [19, 20]. Furthermore, ongoing efforts to establish clearer regulatory frameworks and improve interoperability are laying the groundwork for a more mature and accessible RWA ecosystem. The convergence of these factors creates a fertile ground for innovation and growth, promising to revolutionize how real-world assets are managed, traded, and invested in [17, 19].

The transformative potential of RWA tokenization hinges critically on the development and implementation of scalable and secure solutions. Without the capacity to handle a high throughput of transactions, the efficiency gains promised by tokenization are severely hampered, limiting its applicability to large-scale asset markets [18, 20]. Bottlenecks in transaction processing lead to increased costs and delays, negating the benefits of streamlined settlement and hindering broader adoption. Furthermore, robust security measures are paramount [16, 19]. The decentralized and immutable nature of blockchain technology, while offering inherent advantages, also presents unique security challenges. Smart contract vulnerabilities can be exploited, potentially leading to the loss of investor funds and eroding trust in the entire ecosystem. Therefore, prioritizing security through rigorous auditing, formal verification, and robust security protocols is non-negotiable for establishing a credible and sustainable RWA market [12, 13, 15]. Only by addressing these scalability and security concerns can RWA tokenization truly unlock its potential to revolutionize traditional finance and democra-

Table 1 List of Abbreviations with Full Textwidth Style

	Abbreviation Descriptions			
Abbreviation	Description	Example Use	Related Standard	Context
RWA	Real-World Asset	Asset-backed tokens	N/A	Blockchain
DLT	Distributed Ledger Technology	Blockchain tech	N/A	Ledger tech
STO	Security Token Offering	Tokenized security	N/A	Finance
KYC	Know Your Customer	Identity verification	N/A	Compliance
AML	Anti-Money Laundering	Fraud prevention	N/A	Compliance
ERC-20	Ethereum Fungible Token Standard	Crypto tokens	ERC-20	Tokenization
ERC-721	Ethereum Non-Fungible Token Standard	NFTs	ERC-721	Tokenization
SPV	Special Purpose Vehicle	Investment vehicles	N/A	Finance
ETH	Ether	Ethereum currency	N/A	Cryptocurrency
DAO	Decentralized Autonomous Organization	Governance tools	N/A	Blockchain
TPS	Transactions Per Second	Blockchain speed	N/A	Performance
PoS	Proof-of-Stake	Consensus mechanism	N/A	Blockchain
zk-Rollup	Zero-Knowledge Rollup	Scaling solution	N/A	Blockchain
HSM	Hardware Security Module	Key storage	N/A	Security
DoS	Denial-of-Service	Attack prevention	N/A	Cybersecurity

Note: This table follows the style of a full-textwidth table with additional contextual columns for enhanced readability

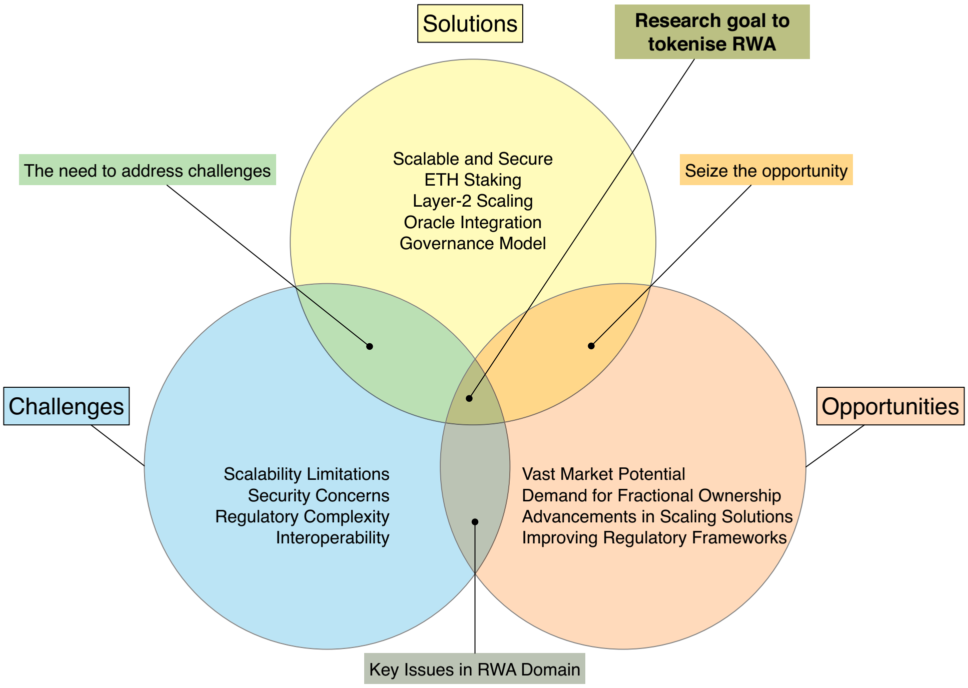

Fig. 1 Interplay of Challenges, Opportunities, and Solutions in RWA Tokenization

tize access to a wider range of investment opportunities. The need for solutions that can effectively handle the volume and complexity of real-world asset transactions while guaranteeing the security and integrity of the underlying blockchain is therefore of paramount importance [14, 15, 17, 19].

While the potential of RWA tokenization is clear, existing solutions face a critical bottleneck: the simultaneous need for scalability, security, and decentralized governance. Many platforms prioritize one or two of these aspects, often at the expense of the others. For example, permissioned blockchains achieve high throughput but sacrifice decentralization. Layer-1 solutions offer security but struggle with scalability. Existing Layer-2 solutions improve scalability, but often lack robust, decentralized security mechanisms or flexible, community-driven governance. Therefore, the core research problem addressed in this paper is the design and evaluation of a framework for RWA tokenization that achieves high scalability, robust security, and decentralized governance without compromising any of these fundamental requirements. This paper addresses this critical need by proposing a novel framework leveraging the Ethereum staking mechanism and Layer-2 scaling solutions. Critically, we explore how ETH staking can be leveraged not only for overall network security but also to specifically enhance the security and decentralization of the Layer-2 scaling solution.

To address the core research problem defined above, this paper investigates the following key research questions:

1. Can a framework combining Ethereum staking and Layer-2 scaling solutions effectively address the scalability limitations of current RWA tokenization platforms, while maintaining a high level of security?
2. How can ETH staking be integrated into a Layer-2 environment to enhance the security and decentralization of the RWA tokenization process?
3. What governance mechanisms are best suited for managing a decentralized RWA tokenization platform, and how can they ensure adaptability and resilience to evolving regulatory landscapes?
4. What are the trade-offs between security, scalability, and user experience within the proposed framework, and how can these trade-offs be optimized?
5. How can a decentralized oracle network be effectively integrated to provide reliable and secure real-world data feeds for the tokenized assets?
6. What are the potential vulnerabilities of the proposed framework, and what mitigation strategies can be employed to address them?

Existing Real-World Asset (RWA) tokenization platforms often struggle to balance scalability, security, and decentralization. Some prioritize scalability using permissioned blockchains, sacrificing decentralization. Others focus on Layer-1 solutions, which are inherently limited in scalability. While Layer-2 solutions improve throughput, they frequently rely on smaller validator sets, raising security concerns, or they lack robust governance.

This research distinguishes itself by proposing a unique, integrated framework that combines Ethereum staking, Layer-2 scaling (specifically Optimistic Rollups), a decen-

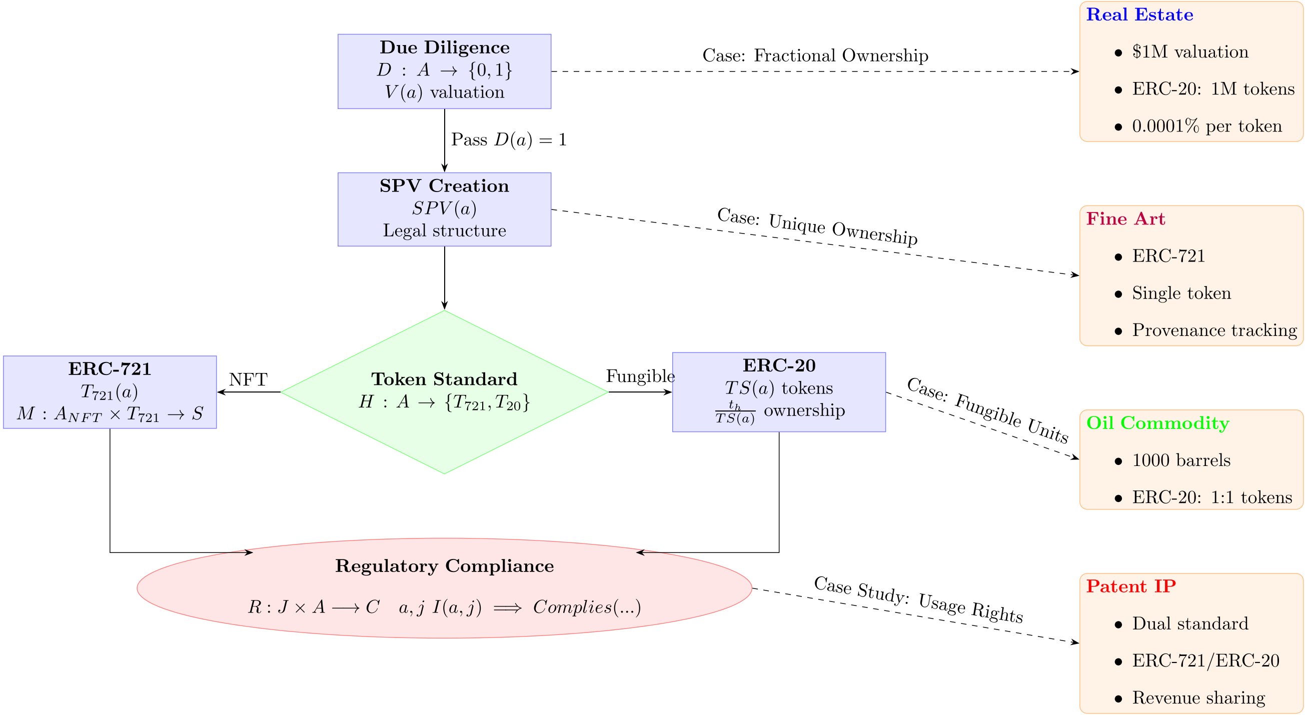

Fig. 2 RWA Tokenization Process

tralized governance model (DAO), and robust oracle integration (Chainlink). This integrated approach addresses scalability, security, and governance simultaneously. A key innovation is leveraging ETH staking to directly secure the Layer-2 network. This provides a higher level of security and decentralization compared to approaches relying solely on separate, smaller validator sets. Validators are incentivized and disincentivized through the same mechanisms as Ethereum itself (rewards and slashing). Furthermore, the DAO governs the parameters of core system components, including reward mechanisms, slashing, and oracle selection, providing flexibility and adaptability often lacking in more centralized platforms. Finally, a thorough security analysis addresses potential vulnerabilities at multiple levels, encompassing smart contracts, oracles, Layer-2, and governance, with specific mitigation strategies.

In summary, the key contributions of this research are: a novel framework design that integrates the aforementioned technologies; enhanced Layer-2 security via ETH staking; DAO-governed parameters for flexibility; a comprehensive security analysis; and a proof-of-concept implementation and case study demonstrating practical application and feasibility. These differentiators position our framework to overcome the limitations of existing approaches, providing a more robust, scalable, and secure platform for RWA tokenization.

2 Related work

Building upon this broad overview, the following sections delve into specific aspects of existing RWA tokenization

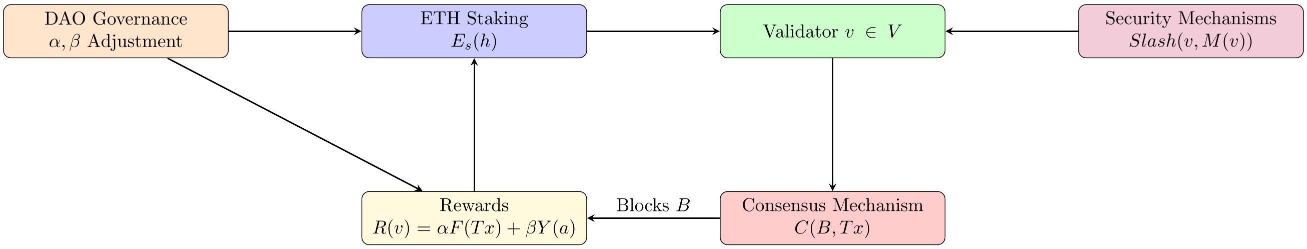

Fig. 3 ETH Staking and Reward Mechanism

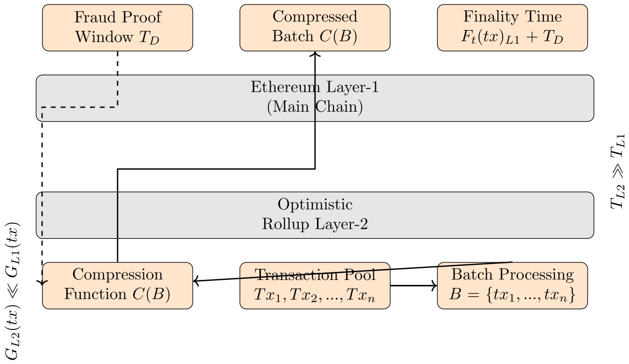
Fraud Proof Window T_D
Compressed Batch $C(B)$
Finality Time $F_t(tx)_{L1} + T_D$
Ethereum Layer-1 (Main Chain)
$T_{L2} \gg T_{L1}$
Optimistic Rollup Layer-2
$G_{L2}(tx) \ll G_{L1}(tx)$
Compression Function $C(B)$
~~Transaction Pool~~ $Tx_1, Tx_2, ..., Tx_n$
Batch Processing $B = \{tx_1, ..., tx_n\}$

Fig. 4 Layer-2 Integration using Optimistic Rollups

efforts, starting with an examination of prominent tokenization platforms.

2.1 Tokenization platforms

Existing literature explores various approaches to RWA tokenization, each with its own strengths and limitations. Platforms like Polymath and Harbor focus on simplifying the legal and technical complexities of security token offerings (STOs) [8], but often rely on the underlying blockchain's capabilities, inheriting its scalability limitations. In contrast, platforms built on more scalable blockchains like Solana or Avalanche might offer higher throughput, but potentially at the cost of reduced decentralization or compatibility with the Ethereum ecosystem. Projects like Centrifuge and RealT utilize specific blockchain networks like Polkadot and Ethereum [21], respectively, to tokenize assets like real estate and invoices [1, 2]. These platforms offer specialized solutions for their respective asset classes, but may face challenges related to interoperability and the specific constraints of their chosen blockchain, compared to a more general-purpose approach. While some platforms have explored the use of private or permissioned blockchains for enhanced performance, these solutions often sacrifice the decentralization and transparency benefits of public blockchains [15], a trade-off our framework aims to avoid (Figs. 2, 3, 4, 5 and 6).

2.2 Staking & layer-2

Research on ETH staking highlights its role in securing the Ethereum network and transitioning to a Proof-of-Stake (PoS) consensus mechanism. Studies have explored the economic and security implications of staking, demonstrating its potential to enhance network resilience and reduce energy consumption [22, 23]. However, the impact of staking on the performance and scalability of decentralized applications, particularly in the context of RWA tokenization, remains an area requiring further investigation [24]. Furthermore, the

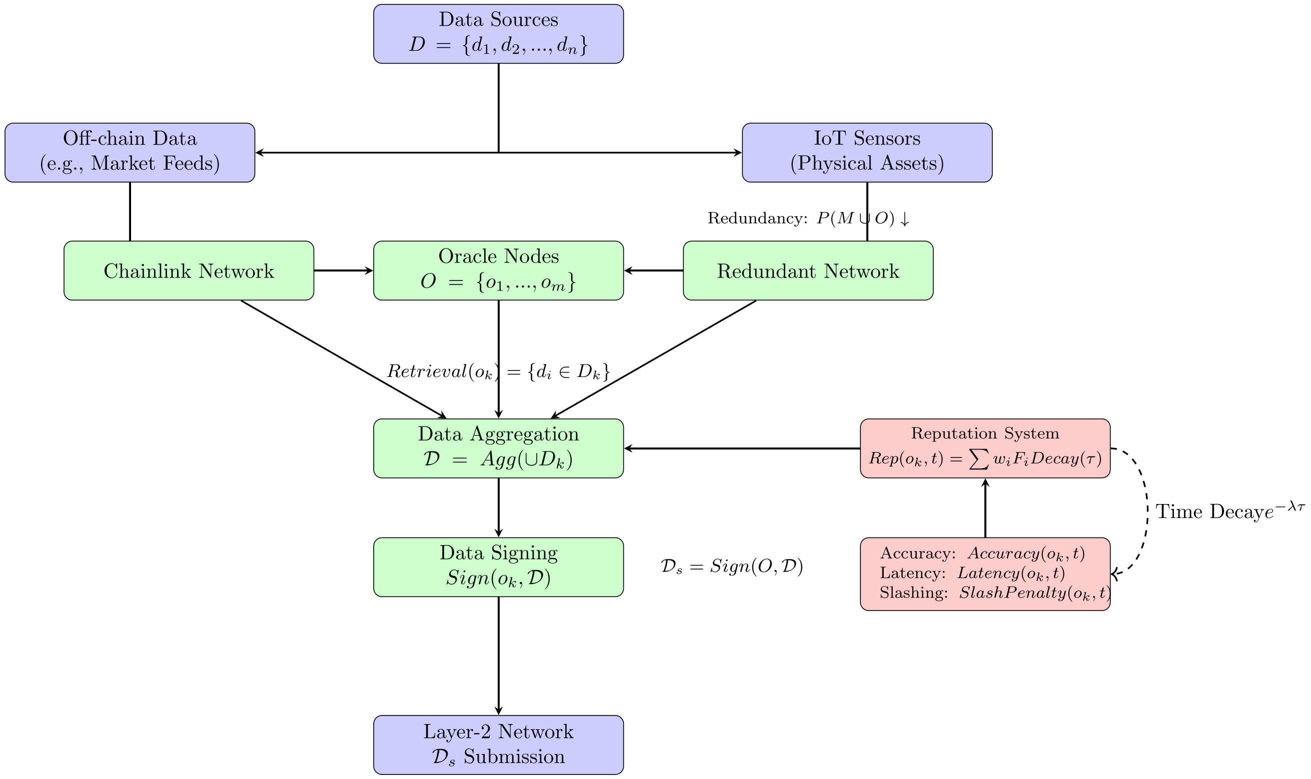
Data Sources $D = \{d_1, d_2, ..., d_n\}$
Off-chain Data (e.g., Market Feeds)
IoT Sensors (Physical Assets)
Redundancy: $P(M \cup O) \downarrow$
Chainlink Network
Oracle Nodes $O = \{o_1, ..., o_m\}$
Redundant Network
$Retrieval(o_k) = \{d_i \in D_k\}$
Data Aggregation $\mathcal{D} = Agg(\cup D_k)$
Reputation System $Rep(o_k, t) = \sum w_i F_i Decay(\tau)$
Time Decay$e^{-\lambda\tau}$
Data Signing $Sign(o_k, \mathcal{D})$
$\mathcal{D}_s = Sign(O, \mathcal{D})$
Accuracy: $Accuracy(o_k, t)$
Latency: $Latency(o_k, t)$
Slashing: $SlashPenalty(o_k, t)$
Layer-2 Network $\mathcal{D}_s$ Submission

Fig. 5 Decentralized Oracle Network Integration

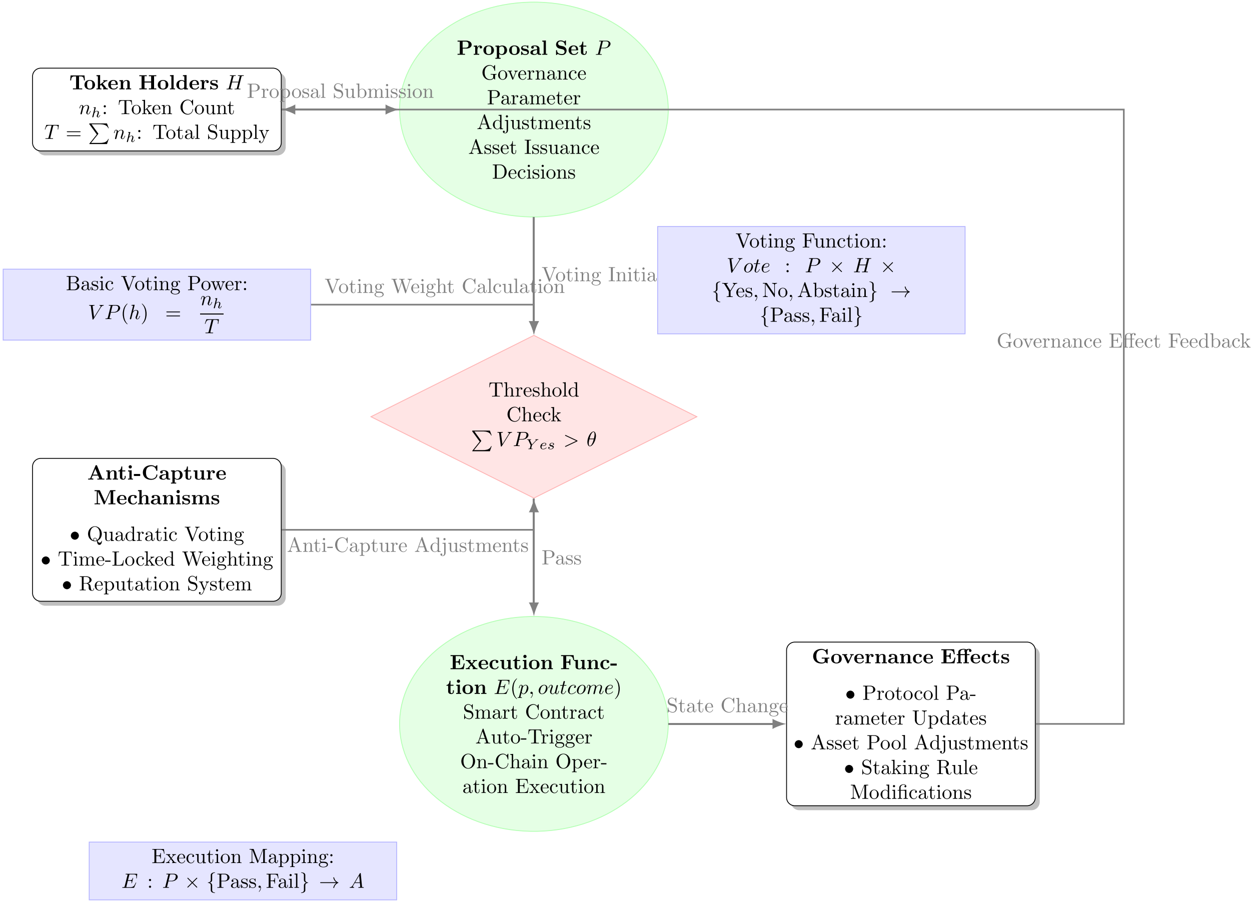

Fig. 6 DAO Governance Model

literature on Layer-2 scaling solutions has explored various approaches, including state channels, sidechains, Plasma, Optimistic Rollups, and zkRollups [25, 26]. Each solution offers different trade-offs in terms of security, scalability, and development complexity [22, 24–26]. Research has demonstrated the potential of these solutions to significantly increase transaction throughput and reduce costs compared to the Ethereum mainnet [27, 28]. For instance, Optimistic Rollups have gained traction for their relatively simple implementation and compatibility with existing Ethereum smart contracts, while zkRollups offer stronger security guarantees through cryptographic proofs [26]. However, the specific suitability of different Layer-2 solutions for RWA tokenization, considering the unique requirements of asset management and regulatory compliance, requires further analysis [26–28].

While both ETH staking and Layer-2 solutions offer individual benefits, their combination presents a unique opportunity to address the core challenges of RWA tokenization. Layer-2 solutions, such as Optimistic Rollups [19, 20], provide scalability by processing transactions off-chain. However, they typically rely on a smaller set of validators than the main Ethereum chain, potentially raising concerns about centralization and security [22, 23]. By integrating ETH staking [24], we leverage the large and decentralized validator set of Ethereum to secure the Layer-2 network [21]. Stakers are incentivized to act honestly on Layer-2 through the same mechanisms (rewards and slashing) that secure the main chain [25]. This creates a synergistic relationship: Layer-2 provides scalability, while ETH staking provides enhanced security and decentralization for the Layer-2 solution [1, 2, 17, 29].

This paper builds upon existing research by exploring the synergistic combination of ETH staking and Layer-2 solutions to create a more secure and scalable platform for RWA tokenization, addressing the limitations of current approaches and paving the way for wider adoption (Tables 2 and 3).

2.3 Strengths & weaknesses

Existing approaches to RWA tokenization demonstrate a variety of strengths and weaknesses. Platforms utilizing permissioned blockchains or private networks often achieve

Table 2 List of Mathematical Symbols

Symbol	Type	Description
$T(A)$	Token	Tokenized form of asset A
$D(a)$	Binary Function	Due diligence assessment of asset a (1 if suitable, 0 otherwise)
$V(a)$	Scalar	Intrinsic value of asset a
$SPV(a)$	Entity	Special Purpose Vehicle for asset a
A_{NFT}	Subset	Subset of A representing non-fungible assets
$T_{721}(a)$	Token	ERC-721 token representing asset $a \in A_{NFT}$
$M(a, T_{721}(a))$	Function	Management function for NFT $T_{721}(a)$ of asset a
A_F	Subset	Subset of A representing fungible assets
$TS(a)$	Scalar	Total supply of ERC-20 tokens for asset $a \in A_F$
t_h	Scalar	Number of tokens held by holder h
J	Set	Set of jurisdictions
$R(j, a)$	Mapping	Regulatory mapping for asset a in jurisdiction j
$I(a, j)$	Function	Issuance process of asset a in jurisdiction j
H	Set	Set of token holders
$E_s(h)$	Scalar	Amount of ETH staked by holder h
v	Element	A validator in the set V
$M(v)$	Binary Function	Malicious behavior of validator v
$Slash(v, M(v))$	Function	Amount of ETH slashed from validator v for behavior $M(v)$
C	Protocol	Consensus mechanism
Tx	Set	Transactions
B	Set	Blocks in the blockchain
$F(Tx)$	Function	Transaction fees
$Y(a)$	Function	Yield generated by asset a
$R(v)$	Function	Reward for validator v
α, β	Coefficients	Coefficients determined by the DAO
$ROI(h)$	Function	Return on investment for holder h
T_{L1}, T_{L2}	Scalars	Transaction throughput of Layer-1 and Layer-2
tx_i	Element	Individual transactions
$C(B)$	Function	Compressed representation of a batch of transactions B
$G_{L1}(tx), G_{L2}(tx)$	Scalars	Gas cost of transaction tx on Layer-1 and Layer-2
$Sec(L1), Sec(L2)$	Scalars	Security of Layer-1 and Layer-2
T_D	Scalar	Dispute period
$F_t(tx)$	Function	Finality time of transaction tx
S_t	Function	Settlement time
P_{fraud}	Probability	Probability of a fraudulent transaction being finalized
$D(B)$	Function	Fraud detection function (1 if fraud detected, 0 otherwise)
d_i	Element	Data from data source i
O	Set	Set of oracle nodes
$Retrieval(o_k)$	Function	Data retrieval process for node o_k
Agg	Function	Aggregation function for oracle data
$Sign$	Function	Signing function for oracle data
$Rep(o_k)$	Scalar	Reputation score of oracle node o_k
M	Event	Event of data manipulation
O (in security context)	Event	Event of an outage
P (in governance context)	Set	Set of proposals
p	Element	A proposal in the set P
v_h	Scalar	Vote of holder h

Table 2 continued

Symbol	Type	Description
$Vote(p, H, v_H)$	Function	Voting function
θ	Scalar	Voting threshold
$E(p, outcome)$	Function	Execution function for proposal p
n_h	Scalar	Number of governance tokens held by holder h
T (in governance context)	Scalar	Total token supply
$VP(h)$	Scalar	Voting power of holder h

higher transaction throughput but sacrifice the decentralization and transparency benefits of public blockchains [30]. Those built on public blockchains like Ethereum benefit from greater security and decentralization but are often constrained by scalability limitations and high gas costs [31]. Furthermore, while security tokens offer a compliant framework for regulated assets, they often introduce complexities in issuance and trading, limiting accessibility for smaller investors [32]. Current oracle solutions, while crucial for connecting on-chain and off-chain data, often present vulnerabilities to manipulation and single points of failure [33].

To provide a clearer comparison of these existing approaches, Table 4 summarizes their key characteristics, advantages, and limitations across several important dimensions.

Following this comparative analysis, we present our proposed framework, which aims to address the limitations identified in existing solutions.

2.3.1 Strengths of existing approaches

Existing tokenization approaches offer several key advantages, as summarized in Table 5. These advantages stem from the core properties of blockchain technology and smart contracts. Fractional ownership, facilitated by tokenization $T(A)$, enhances liquidity by allowing multiple investors $I = \{i_1, i_2, ..., i_n\}$ to own portions f_k of an asset A, where $\sum_{k=1}^{n} f_k = 1$ [1, 2, 7, 17, 37]. Blockchain immutability $Immutability(B)$ ensures transparency and auditability by creating a permanent record of all transactions involving the tokenized asset [14, 39, 40]. Smart contracts SC automate processes P, denoted by $SC(P)$, improving efficiency and reducing operational overhead [1, 6, 41, 42]. Finally, global accessibility expands market reach by allowing investors worldwide to access and trade tokenized assets, fostering greater market participation [5, 6, 17, 29].

2.3.2 Weaknesses of existing approaches

Existing RWA tokenization platforms face several limitations, hindering their widespread adoption and highlighting key areas for improvement. These weaknesses, along with the proposed mitigations within our framework, are summarized in Table 6. Scalability bottlenecks, often arising from limited transaction throughput ($TPS(P)$), can cause congestion

Table 3 Comparison of Existing Tokenization Platforms

P	T	S_c	S_e	D	G	O	I	A	R
Traditional Systems	C Databases	H	M	L_o	C	N	N	G_E	Basic
Polymath	E_T	L_o	H	H	Limited	Limited	N	S_E	Strong
Harbor	E_T	L_o	H	H	Limited	Limited	N	S_E	Strong
Centrifuge	P_{O_L}/E_T	M	M	M	P_S	Y (Chainlink)	N	R_{W_A}, invoices	Some
RealT	E_T/Gnosis	L_o	H/M	M	Limited	Limited	N	R_E	Strong
Permissioned Blockchain (H_F)	Permissioned Blockchain	H	H	L_o	Configurable	P_C	P_O	G_E	Configurable
zk-Rollup based Platform	$E_T + Z_R$	H	H	M	V	Y (Chainlink)	V	G_E	V
Our Framework	$E_T + O_R$	**H**	**H**	**H**	D_{A_O}	**Y** (Chainlink)	**Y** (E_T Staking)	G_E	**Strong**

Symbol Definitions: P: Platform, T: Underlying Technology, S_c: Scalability, S_e: Security, D: Decentralization, G: Governance, O: Oracle Integration, I: Staking Integration, A: Asset Type Focus, R: Regulatory Compliance Features, Ad: Advantages, L: Limitations, H: High, M: Medium, L_o: Low, Y: Yes, N: No, V: Varies, C: Centralized, D_{A_O}: DAO-governed, P_S: Project-specific, P_C: Possible, P_O: Potentially, E_T: Ethereum, P_{O_L}: Polkadot, H_F: Hyperledger Fabric, Z_R: zk-Rollups, O_R: Optimistic Rollups, R_{W_A}: Real-world Assets, R_E: Real Estate, G_E: General, S_E: Securities

Bold entries denote the framework proposed in this paper

Table 4 Comparison of RWA Tokenization Approaches

Category	Parameter Name	Value(s) and Rationale
Platform	Traditional Systems	Centralized Databases. High scalability (but limited by central server), medium security (single point of failure), low decentralization, centralized governance, no oracle or staking integration, general asset type focus, basic regulatory compliance features. Advantages: Familiar, established. Limitations: Opaque, inefficient, limited access.
Platform	Polymath	Ethereum. Low scalability, high security, high decentralization, limited governance, limited oracle integration, no staking integration, securities asset type focus, strong regulatory compliance features. Advantages: Security token focus, compliance tools. Limitations: Scalability limitations, Ethereum-dependent.
Platform	Harbor	Ethereum. Low scalability, high security, high decentralization, limited governance, limited oracle integration, no staking integration, securities asset type focus, strong regulatory compliance features. Advantages: Regulatory compliance, investor management. Limitations: Scalability limitations, Ethereum-dependent.
Platform	Centrifuge	Polkadot/Ethereum. Medium scalability, medium security, medium decentralization, project-specific governance, yes oracle integration (Chainlink), no staking integration, real-world assets and invoices asset type focus, some regulatory compliance features. Advantages: Specific use cases, interoperability challenges.
Platform	RealT	Ethereum/Gnosis. Low scalability, high/medium security, medium decentralization, limited governance, limited oracle integration, no staking integration, real estate asset type focus, strong regulatory compliance features. Advantages: Real estate tokenization, fractional ownership. Limitations: Limited to real estate, scalability concerns.
Platform	Permissioned Blockchain (e.g., Hyperledger Fabric)	Permissioned Blockchain. High scalability, high security (but centralized), low decentralization, configurable governance, possible oracle integration (but often centralized), potentially staking integration (but not inherent), general asset type focus, configurable regulatory compliance features. Advantages: High throughput, controlled environment. Limitations: Lack of transparency, centralization risks.
Platform	zk-Rollup based Platform	Ethereum + zk-Rollups. High scalability, high security, medium decentralization, varies governance, yes oracle integration (Chainlink), varies staking integration, general asset type focus, varies regulatory compliance features. Advantages: High throughput, strong security guarantees. Limitations: Complexity, potential for centralization in sequencer.
Platform	**Our Framework**	**Ethereum + Optimistic Rollups**. **High** scalability, **high** security, **high** decentralization, **DAO-governed** governance, **yes** oracle integration (Chainlink), **yes** staking integration (ETH Staking), **general** asset type focus, **strong** regulatory compliance features. Advantages: Scalability, security, decentralized governance, flexibility. Limitations: Complexity, reliance on Ethereum ecosystem.

Bold entries denote the framework proposed in this paper

and delays when transaction volume V_T exceeds capacity [19, 20]. Security vulnerabilities introduce significant risks, represented by the probability of exploitation $P(V)$ and potential losses $L(V)$ [4, 13, 14]. Regulatory uncertainty U_R poses compliance challenges [15, 16], while interoperability issues ($Interop(B_1, B_2)$) limit cross-platform asset transfers [45]. Oracle limitations, impacting data reliability $R(O)$ and cost $C(O)$ [33, 46], and complex user interfaces (affecting accessibility, $Acc(P)$) further restrict broader adoption [1]. These challenges underscore the need for more robust, secure, and user-friendly platforms. Our proposed framework, leveraging ETH staking [22–24] and Layer-2 solutions [19, 25], directly addresses these limitations, aiming to enhance scalability, security, and platform efficiency for a more robust and accessible RWA ecosystem [2, 17].

Table 5 Strengths of Existing Tokenization Approaches

	Description		References
Strength	Summary	Details	Sources
Liquidity & Fractionalization	Fractional Ownership	$T(A) \implies \exists f_k : A = \sum_{k=1}^{n} f_k \cdot A, I = \{i_1, ..., i_n\}$	[7, 34]
Transparency & Auditability	Blockchain Immutability	$Tx(T(A)) \xrightarrow{B} Immutable$	[35, 36]
Automation & Efficiency	Smart Contracts	$SC(P) \implies Efficiency \uparrow, Overhead \downarrow$	[37, 38]
Global Reach & Accessibility	Wider Investor Pool	$T(A)$ Global Access	-

This table summarizes the strengths of tokenization approaches

Table 6 Weaknesses of Existing RWA Tokenization Platforms and Proposed Mitigations

	Weaknesses[1]			Mitigations[2]		
Aspect	Description	Metric	Example	Description	Mechanism	Example
Scalability	Bottlenecks	$TPS(P) \ll V_T$	Low TPS [38]	Layer-2 scaling	Optimistic Rollups	$TPS \uparrow$
Security	Vulnerabilities	$P(V) \uparrow, L(V) \uparrow$	Exploits [43]	Enhanced security	Formal verification, bug bounties, staking	$P(V) \downarrow, L(V) \downarrow$
Regulation	Uncertainty	High U_R	Undefined compliance [44]	Legal compliance framework	Integration in tokenization	$U_R \downarrow$
Interoperability	Issues	Low $I(B_1, B_2)$	Limited chain comm. [45]	Ethereum-based solutions	Cross-chain bridges (future)	$I \uparrow$
Oracle	Limitations	Low $R(O)$, High $C(O)$	Data issues [46]	Decentralized oracles	Chainlink	$R(O) \uparrow, C(O) \downarrow$
Complexity	User experience	Low $Acc(P)$	Low usability [47]	Simplified interface	Modular design	$Acc(P) \uparrow$

Weaknesses highlight limitations in existing platforms, measured by metrics and supported by references.
Mitigations summarize proposed mechanisms in our framework to address these weaknesses

3 Framework

Having outlined the high-level components and principles of our proposed framework, we now proceed to describe the specific mechanisms employed for RWA tokenization within this structure.

3.1 Tokenization mechanism

Let A represent the set of real-world assets (RWAs) to be tokenized. The tokenization process begins with a due diligence assessment

$$D : A \to \{0, 1\}, \tag{1}$$

where $D(a) = 1$ indicates that asset $a \in A$ is suitable for tokenization based on legal, financial, and technical criteria. This assessment also establishes the intrinsic value of the asset, denoted by $V(a)$. Following due diligence, a Special Purpose Vehicle (SPV), denoted by $SPV(a)$, is established to hold the asset a, providing a clear legal ownership structure.

We utilize a hybrid token standard. For non-fungible assets $A_{NFT} \subset A$, we leverage ERC-721, issuing a unique token $T_{721}(a)$ for each $a \in A_{NFT}$. This allows granular tracking and management, represented by a function

$$M : A_{NFT} \times T_{721}(A_{NFT}) \to S, \tag{2}$$

where S is the set of possible states of the asset. For fungible assets $A_F \subset A$, we use ERC-20, issuing a total supply of $TS(a)$ tokens for each $a \in A_F$. Fractional ownership is then represented by $\frac{t_h}{TS(a)}$, where t_h is the number of tokens held by holder h. This hybrid approach, denoted by

$$H : A \to \{T_{721}, T_{20}\}, \tag{3}$$

where $H(a)$ determines the appropriate token standard, provides flexibility to represent diverse asset classes.

Let J be the set of jurisdictions and

$$R : J \times A \to C \tag{4}$$

be the regulatory mapping, where $R(j, a)$ determines the token classification $c \in C$ (e.g., security, utility token) for asset a in jurisdiction j. The token issuance process adheres to all relevant regulations defined by $R(j, a)$, ensuring compliance with KYC/AML requirements and other legal frameworks. This meticulous approach, formalized as

$$\forall a \in A, \forall j \in J, I(a, j) \implies Complies(I(a, j), R(j, a)), \tag{5}$$

where $I(a, j)$ represents the issuance process of asset a in jurisdiction j and $Complies$ is a function checking compliance with regulations, fosters trust and promotes sustainable ecosystem development.

3.1.1 Real-world examples of tokenization

To illustrate the practical application of our tokenization mechanism, consider the following examples across different asset classes:

Real estate (fractional ownership) A commercial property, valued at \$1 million, could be tokenized using ERC-20 tokens. After due diligence confirms ownership, valuation, and legal compliance $D(a) = 1$, an SPV is established to hold the legal title $SPV(a)$. The property is then represented by 1,000,000 ERC-20 tokens, each representing a 0.0001% ownership share $TS(a) = 1,000,000$. Investors can purchase these tokens, with an investor holding 10,000 tokens $t_h = 10,000$ owning 1% of the property. Rental income would be distributed proportionally to token holdings.

Fine art (unique ownership) A valuable painting would be tokenized using an ERC-721 token. Following due diligence to verify authenticity, provenance, and ownership $D(a) = 1$, an SPV is created to hold the painting $SPV(a)$. A single ERC-721 token $T_{721}(a)$ is issued, representing complete ownership. Transferring this token represents transferring ownership of the painting, with the management function $M(a, T_{721}(a))$ tracking the asset's state and ownership.

Commodity (fungible units) For 1000 barrels of oil stored in a certified facility, ERC-20 tokens are appropriate. Due diligence confirms the existence, quantity, quality, and ownership of the oil $D(a) = 1$. An SPV is created to hold the legal title $SPV(a)$. 1000 ERC-20 tokens are issued, each representing one barrel of oil $TS(a) = 1000$. Trading these tokens represents the transfer of ownership of the corresponding barrels.

Intellectual property (usage rights) A patent for a new technology could be tokenized using either ERC-721 or ERC-20 tokens, depending on the use case. After due diligence confirms the patent's validity and ownership, and an SPV is created, tokens could represent different rights. An ERC-721 token could represent a unique license to use the technology (for a specific purpose or period). Alternatively, ERC-20 tokens could represent fractional ownership of the patent itself, or shares in the revenue it generates.

These examples demonstrate the flexibility of our hybrid tokenization approach, allowing for the representation of diverse asset classes with appropriate token standards and ownership models.

3.2 Staking integration

To achieve both scalability and robust security, our framework integrates ETH staking to directly secure the Layer-2 network. While integrating ETH staking enhances security, it's crucial to address the potential for validator centralization, where larger holders could disproportionately influence validation and governance. Our framework incorporates several mechanisms to mitigate this risk.

Let H be the set of token holders. A holder $h \in H$ can stake an amount of ETH, denoted by $E_s(h)$, to become a validator v in the set of validators V on our Layer-2 network. This staked ETH, $E_s(h)$, acts as collateral specifically securing the Layer-2 network where RWA transactions are processed. This is a crucial distinction: we are not simply leveraging general ETH staking; we are directly tying the staked ETH to the security of the tokenized assets. By doing so, we inherit the large and decentralized validator set of Ethereum, significantly enhancing the decentralization and security of our RWA tokenization platform compared to solutions relying on smaller, potentially more centralized, validator sets. Let $M(v)$ represent the malicious behavior of validator v. The slashing condition can be defined as

$$Slash : V \times M(V) \rightarrow \mathbb{R}, \tag{6}$$

where $Slash(v, M(v))$ represents the amount of ETH slashed from validator v for engaging in malicious behavior $M(v)$. This disincentivizes malicious behavior, aiming to ensure honest validation. Validators participate in the consensus mechanism C, validating transactions Tx and adding blocks B to the Layer-2 chain. Crucially, the same economic incentives that secure the Ethereum mainnet apply here: validators are rewarded for honest behavior and penalized (through slashing) for malicious actions. This direct application of ETH staking's security model to the Layer-2 context provides strong guarantees against censorship, double-spending, and invalid state transitions, all of which are critical for the integrity of RWA tokenization.

The reward mechanism R for validators is defined as a function of transaction fees $F(Tx)$ and yield $Y(a)$ generated by the underlying real-world asset

$$a : R(v) = \alpha F(Tx) + \beta Y(a), \tag{7}$$

where α and β are coefficients determined by the DAO. The transaction fee component, $\alpha F(Tx)$, incentivizes active participation and efficient transaction processing. The yield component, $\beta Y(a)$, aligns validator incentives with the performance of the tokenized assets, fostering a collaborative ecosystem. The DAO governance ensures transparent and community-driven determination of α and β. This dual reward system, by combining both $F(Tx)$ and $Y(a)$, encourages participation in staking, bolstering the security and stability of the platform. Furthermore, it provides stakers with a potentially compelling return on investment, represented by

$$ROI(h) = \frac{R(v) - E_s(h)}{E_s(h)} \tag{8}$$

over a defined period, assuming v corresponds to holder h.

To prevent validator centralization, our framework employs several strategies (detailed further in Section 4). These include staking limits, which can be "soft" (reducing rewards beyond a threshold) or "hard" (an absolute maximum stake). We support delegated staking, allowing smaller holders to delegate their ETH, and we can implement incentives to encourage delegation to smaller validators, further promoting decentralization. Validator selection mechanisms can also be designed to favor a more distributed validator set, for example, using variations of round-robin selection or stake-weighted random sampling with adjustments to reduce the advantage of very large stakes. Slashing conditions and penalties can be adjusted based on validator stake, increasing the risk for larger, potentially colluding validators. The DAO governs staking parameters (limits, rewards, penalties – see Section 3.5), allowing the community to adapt to changing conditions. Finally, continuous monitoring of stake distribution and alerts for excessive concentration are integral parts of the system.

3.3 Layer-2 scaling solution

To address scalability limitations, our framework utilizes Optimistic Rollups. Let T_{L1} and T_{L2} represent the transaction throughput of Layer-1 and Layer-2 respectively. Optimistic Rollups significantly increase throughput: $T_{L2} \gg T_{L1}$. This is achieved by bundling multiple transactions tx_i into a batch $B = \{tx_1, tx_2, ..., tx_n\}$ off-chain and submitting a compressed representation $C(B)$ to Layer-1, where C is a compression function. This reduces the computational burden on Layer-1, allowing for higher T_{L2}. Let $G_{L1}(tx)$ and $G_{L2}(tx)$ represent the gas cost of a transaction tx on Layer-1 and Layer-2, respectively. Optimistic Rollups drastically reduce gas costs: $G_{L2}(tx) \ll G_{L1}(tx)$. This is particularly beneficial for RWA transactions, which might involve more complex operations than simple token transfers. By batching transactions, especially those related to the same asset class or SPV, we maximize the efficiency of the compression function, C(B), and further reduce the per-transaction cost. Given the typically lower frequency of RWA transactions compared to cryptocurrency trading, we can also employ time-delayed batching, accumulating transactions over a longer period to achieve larger batch sizes and greater gas cost savings. This is acceptable because the traditional settlement times for RWAs are already relatively long, so a slightly longer delay on Layer-2 is not a significant drawback. Optimistic Rollups inherit the security of Ethereum. While Optimistic Rollups inherit the security of Ethereum, the relationship is best approximated as:

$$Sec(L2) \approx Sec(L1). \tag{9}$$

This equation represents an approximation, and it's crucial to acknowledge the specific risks associated with the Layer-2 implementation. While the underlying security guarantees are inherited from Ethereum, the practical security of the Layer-2 network depends on factors such as the effectiveness of the fraud-proof mechanism, the length of the dispute period, the availability of data, and the decentralization of the validator set. These risks, and our strategies for mitigating them, are discussed in detail in Section 4.3. However, the dispute period T_D introduces a delay in transaction finality. Let $F_t(tx)$ represent the finality time of a transaction. Then,

$$F_t(tx)_{L2} = F_t(tx)_{L1} + T_D. \tag{10}$$

For RWA transactions, where settlement times S_t are typically long ($S_t \gg T_D$), this delay is less impactful. For RWA transactions, where security and regulatory compliance are paramount, this inheritance of Ethereum's security is a crucial advantage. While a longer dispute period might be a concern for applications requiring very fast finality, the higher value and regulatory scrutiny of RWA transactions generally justify a longer dispute period to minimize the risk of fraudulent transactions being finalized. This trade-off is carefully considered and can be adjusted through DAO governance.

RWA transactions differ significantly from typical cryptocurrency transactions, exhibiting characteristics that inform our design choices within the Optimistic Rollup framework. They generally occur at a lower frequency than high-volume cryptocurrency trading, involve higher monetary values, are subject to greater regulatory scrutiny and compliance requirements (KYC/AML, reporting), and have longer traditional settlement times (often days or weeks, rather than seconds). These combined factors—lower frequency, higher value, increased regulation, and longer settlement times—influence our optimizations and trade-off decisions.

Let P_{fraud} be the probability of a fraudulent transaction being finalized. Robust fraud detection mechanisms, represented by a function

$$D : B \to \{0, 1\}, \tag{11}$$

where $D(B) = 1$ indicates detection of fraud in batch B, aim to minimize P_{fraud}. The staking mechanism, with slashing conditions $S(v, M(v))$ for malicious validator behavior $M(v)$, further incentivizes honest validation, reducing P_{fraud}. This approach allows us to maximize the scalability benefits of Optimistic Rollups, expressed by the increase in T_{L2} and decrease in $G_{L2}(tx)$, while maintaining high security and efficiency for our platform.

3.4 Oracle integration

Let $D = \{d_1, d_2, ..., d_n\}$ represent the set of independent data sources used by our decentralized oracle network. Chainlink retrieves data $d_i \in D$ from each source. Let $O = \{o_1, o_2, ..., o_m\}$ represent the set of oracle nodes. Each node $o_k \in O$ retrieves data from a subset of data sources $D_k \subset D$. The data retrieval process for node o_k can be represented as $Retrieval(o_k) = \{d_i | d_i \in D_k\}$. These nodes then aggregate the retrieved data using an aggregation function

$$Agg : \mathcal{P}(D) \to \mathcal{D}, \tag{12}$$

where $\mathcal{P}(D)$ is the power set of D and $\mathcal{D}$ represents the aggregated data. The aggregated data is then signed using a signing function

$$Sign : O \times \mathcal{D} \to \mathcal{D}_s, \tag{13}$$

producing signed data $\mathcal{D}_s$. This signed data is submitted to the Layer-2 network.

While Chainlink provides a robust and decentralized oracle solution, it's crucial to acknowledge that no oracle system is perfect. Data manipulation and failures in redundancy mechanisms are potential risks that must be addressed. For example, multiple oracle nodes could collude to report incorrect data, the underlying data sources could be compromised, or an attacker could intercept and modify the data in transit. Furthermore, even with multiple independent oracle networks, there's a risk of correlated failures if they share common vulnerabilities or dependencies.

Chainlink's reputation system can be represented as a function

$$Rep : O \to \mathbb{R}, \tag{14}$$

where $Rep(o_k)$ is the reputation score of node o_k. This score is based on the node's past performance and track record. Let M represent the event of data manipulation. Data signing, combined with the reputation system, aims to minimize $P(M|Rep, Sign)$, the probability of manipulation given the reputation and signing mechanisms. However, this probability is not zero. To further mitigate the risk of data manipulation, our framework employs multiple independent data sources for each data feed, implements on-chain data validation mechanisms, and utilizes a robust aggregation function (as discussed above) that is resistant to outliers and weighted by node reputation.

To address the risk of failures in redundancy mechanisms, we employ a multi-layered approach. We use multiple independent oracle networks ($N > 1$) for redundancy. This redundancy minimizes the probability of data manipulation or outages, represented as $P(M \cup O)$, where O is the event of an outage. Formally, using multiple independent oracle networks reduces $P(M \cup O)$ compared to a single oracle network. This multi-layered approach, combining decentralized data retrieval, aggregation, signing, reputation systems, and redundancy, ensures that smart contracts operate based on accurate and trustworthy data, ultimately enhancing the integrity of the tokenized asset ecosystem.

This score is not static; it's dynamically updated based on the node's ongoing performance and behavior. We model the reputation of oracle o_k at time t, $Rep(o_k, t)$, as a weighted sum of factors, each subject to time decay:

$$Rep(o_k, t) = \sum_{i=1}^{n} w_i F_i(o_k, t) Decay(t - t_i) \tag{15}$$

where n is the number of factors, w_i are the weights assigned to each factor, and $F_i(o_k, t)$ represents various factors. These include an Accuracy Factor ($Accuracy(o_k, t)$), a Latency Factor ($Latency(o_k, t)$), an Uptime Factor ($Uptime(o_k, t)$), and a Slashing Factor ($SlashPenalty(o_k, t)$). The $Decay(t - t_i)$ term is a time decay function (e.g., $Decay(\tau) = e^{-\lambda\tau}$), where t_i is the time of event i, ensuring that more recent events have a greater influence.

The reputation score is updated both periodically and in response to specific events. The time decay function continuously reduces the weight of past events. Event-driven updates occur for successful and unsuccessful data provisions (increasing and decreasing the score, respectively), slashing events (significantly decreasing the score), and successful or failed challenges. The frequency of periodic updates is a configurable parameter, with a trade-off between responsiveness to recent behavior and computational overhead. This parameter, along with the weights in the reputation formula, can be adjusted through DAO governance (See Section 3.5). To enhance the system's resilience to Sybil attacks, the cost of acquiring and maintaining a large number of identities is designed to be prohibitively high.

The reputation model incorporates several features to enhance its resilience to collusion attacks. The use of multiple, independent data sources makes it more difficult for colluding nodes to consistently report incorrect data without being detected. The aggregation function, which may use a weighted average based on reputation, reduces the influence of low-reputation (potentially colluding) nodes. Furthermore, a larger number of independent oracle nodes increases the difficulty of successful collusion. The threat of slashing, combined with reputational damage, also serves as a deterrent.

3.5 Governance model

Our platform utilizes a Decentralized Autonomous Organization (DAO) for governance. Let H be the set of token holders, where each holder $h \in H$ possesses n_h governance tokens. Total token supply is denoted by $T = \sum_{h \in H} n_h$. Voting rights are proportional to token holdings; thus, the voting power of holder h is $VP(h) = \frac{n_h}{T}$. While this equation represents the basic principle of token-weighted voting, it's crucial to acknowledge the inherent risk of governance capture by large stakeholders. Therefore, this is not the only factor determining voting power, and our framework incorporates several mechanisms to mitigate this risk. ... A proposal passes if the weighted sum of "Yes" votes exceeds a predefined threshold θ:

$$\sum_{h \in H : v_h = Yes} VP(h) > \theta. \tag{16}$$

This threshold, and the voting mechanism itself, are subject to DAO governance and can be adjusted to prevent governance capture. For example, the DAO could implement quadratic voting, where the cost of votes increases quadratically, making it disproportionately expensive for large holders to dominate votes. Alternatively, time-locked voting could be introduced, giving a voting power boost to token holders who commit to locking their tokens for a longer period, thus incentivizing long-term commitment and reducing the influence of large, short-term holders.

Let P be the set of proposals submitted for voting. For a given proposal $p \in P$, each holder h can cast a vote $v_h \in \{Yes, No, Abstain\}$. The outcome of a vote on proposal p is determined by a voting function

$$Vote : P \times H \times \{Yes, No, Abstain\} \rightarrow \{Pass, Fail\},$$

where $Vote(p, H, v_H)$ aggregates the votes $v_H = \{v_h | h \in H\}$ and determines the outcome. This decision-making process is automated through smart contracts, ensuring impartial execution. Let

$$E : P \times \{Pass, Fail\} \rightarrow A \tag{17}$$

be the execution function, where $E(p, Pass)$ triggers actions $a \in A$ associated with the passed proposal p, and $E(p, Fail)$ takes no action. This automated execution eliminates the need for intermediaries and enforces decisions transparently. The DAO structure enables flexible and adaptable governance, fostering community participation and ensuring alignment with user interests. This decentralized model promotes trust, transparency, and long-term sustainability for the RWA ecosystem.

3.6 Identity management

Identity management is a crucial aspect of Real-World Asset (RWA) tokenization, particularly for ensuring compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. While the core functionality of our framework (tokenization, staking, Layer-2 scaling, governance) does not require on-chain storage of personally identifiable information (PII), a robust and flexible identity management solution is necessary for many RWA use cases. This section outlines different approaches to integrating identity management with our framework.

Our framework is designed to be agnostic to the specific identity management solution used, allowing for flexibility and adaptation to different regulatory requirements and user preferences. Several approaches are possible, each with its own trade-offs in terms of privacy, security, and decentralization:

1. **Self-Sovereign Identity (SSI)** offers an alternative approach, leveraging Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). With SSI, users maintain control over their own identity data, selectively disclosing it to relying parties (like the SPV or token issuer) only when necessary. DIDs, unique and globally resolvable identifiers independent of centralized authorities, are paired with VCs – digitally signed statements about a user's identity attributes, issued by trusted entities. While SSI enhances user privacy and control, and reduces reliance on centralized identity providers, it does require user adoption of DID/VC technology and can introduce some complexity in credential management.
2. **Permissioned Identity Systems** offer another approach, where a consortium of trusted entities, such as financial institutions or government agencies, manages user identities. Users would undergo KYC/AML verification with one of these entities, which would then issue a digital credential granting access to the RWA platform. While this approach benefits from leveraging existing KYC/AML infrastructure and potentially simplifies integration with traditional financial systems, it introduces greater centralization, potential single points of failure, and reliance on trusted third parties.
3. **Integration with Existing KYC/AML Providers** Our framework can integrate with existing KYC/AML service providers through oracles or APIs. A user wanting to interact with the platform (e.g., to purchase tokenized assets) would undergo verification with a chosen provider. Upon successful verification, the provider would issue a digitally signed attestation, which the user then submits to the relevant smart contract. The smart contract verifies the signature of the attestation, and grants access if it is valid. This approach leverages existing KYC/AML infrastructure and expertise, avoiding the need to build a new identity system from scratch. However, it does introduce a reliance on external providers and may raise privacy concerns if data is shared with multiple providers.

3.6.1 Integration with the framework

Regardless of the chosen identity management approach, integration with our framework typically involves a consistent sequence of steps. First, a user verifies their identity through one of the supported mechanisms before interacting with restricted platform features (e.g., purchasing security tokens or participating in governance). Upon successful verification, the user receives a digital credential (such as a VC, a signed attestation, or an entry in a permissioned system). When interacting with the platform, the user presents this credential to the relevant smart contract. The smart contract then verifies the credential's authenticity and validity, for instance, by checking the issuer's signature, verifying against a list of trusted issuers, or querying an oracle. Based on the verification result, the smart contract grants or denies access to the requested functionality.

As a concrete example, consider a user wishing to purchase tokenized shares of real estate. The user would first undergo KYC/AML verification with a trusted provider. Upon successful verification, the provider issues a digitally signed attestation of compliance. The user submits this attestation to the smart contract governing the token sale, which verifies the signature and, if valid, allows the purchase to proceed.

3.6.2 Privacy considerations

It's crucial to balance the need for regulatory compliance with user privacy. Our framework prioritizes minimizing the amount of sensitive data stored on-chain. Whenever possible, we advocate for approaches that use cryptographic proofs or attestations, rather than storing PII directly on the blockchain. The specific approach chosen will depend on the regulatory requirements and the preferences of the stakeholders involved.

3.7 Framework novelty and contributions

While the individual components of our framework – Ethereum staking, Optimistic Rollups, DAOs, and decentralized oracles – build upon existing technologies, their combination and application to Real-World Asset (RWA) tokenization, along with several key design choices, constitute the core novelty and contributions of this work.

Unlike many existing platforms that focus on a single aspect of tokenization, our framework provides a complete, integrated solution specifically designed for RWAs, simultaneously addressing the critical needs of scalability, security, decentralized governance, and reliable real-world data feeds (as discussed in Section 1).

A key innovation is the direct integration of ETH staking to secure the Layer-2 network (Section 3.2). This differs from many Layer-2 solutions that rely on separate, smaller validator sets. By leveraging Ethereum's existing, large, and decentralized validator set, we significantly enhance the security and censorship resistance of the RWA tokenization process. The economic incentives of ETH staking (rewards and slashing) directly apply to Layer-2 validators, aligning their interests with system integrity.

Furthermore, our framework places critical system parameters under the control of a Decentralized Autonomous Organization (DAO) (Section 3.5). This includes parameters governing the reward mechanism (α and β in Section 3.2), slashing conditions, oracle selection criteria, and aspects of the Layer-2 implementation. This DAO governance provides flexibility and adaptability lacking in more centralized or static platforms.

The framework supports a hybrid token standard (ERC-20 for fungible assets, ERC-721 for non-fungible assets, as described in Section 3.1), enabling representation of diverse assets within the same unified platform. Section 3.1 also introduces a regulatory mapping function:

$$R : J \times A \rightarrow C \tag{18}$$

where $R(j, a)$ determines the token classification $c \in C$ (e.g., security, utility token) for asset a in jurisdiction j.

These novel aspects, working in concert, are designed to overcome the limitations of existing approaches and provide a more robust, scalable, secure, and adaptable platform for RWA tokenization (Table 7).

4 Security

Given the critical nature of security in ensuring the integrity of the tokenization process, the following section details the specific security measures integrated into our proposed framework.

4.1 Security of the framework

Ensuring the security of our proposed framework is paramount for maintaining the integrity and robustness of the RWA platform. We adopt a multi-layered security approach, addressing potential vulnerabilities at various levels: smart contract level, oracle integration, Layer-2 operation, key management and access control, and governance.

Smart contract security Smart contracts form the core of our platform's functionality. To mitigate the risk of vulnerabilities (denoted by V_c) within the smart contracts SC, we employ rigorous auditing, formal verification, and bug bounty programs. Auditing by independent security experts aims to identify and rectify potential vulnerabilities before deployment. Formal verification techniques, denoted as $Verify(SC)$, provide mathematical assurances of the contract's correctness by proving adherence to specified properties. For instance, we can formally verify that a token transfer function correctly updates balances and prevents double-spending. This approach, while not eliminating all potential vulnerabilities, significantly reduces the risk of common smart contract bugs. Furthermore, a bug bounty program, incentivizing external security researchers R to discover and report vulnerabilities $Bounty(R, V_c)$, complements our internal security efforts. This incentivizes external security researchers to identify and report vulnerabilities, complementing our internal security efforts and providing a form of crowdsourced security auditing.

Oracle security The decentralized nature of our oracle solution, Chainlink, significantly reduces the inherent risks associated with centralized oracles. Employing multiple independent oracle networks enhances redundancy, minimizing the probability of data manipulation $P(M_O)$ or outages $P(O_O)$. Formally,

$$P(M_O \cup O_O)_{decentralized} < P(M_O \cup O_O)_{centralized}. \tag{19}$$

This inequality is based on the fundamental principle that independent failures are less likely than correlated failures. The more independent oracles we have, the lower the probability that a majority will be compromised or unavailable simultaneously. Data signing and reputation systems further bolster the integrity and trustworthiness of data feeds by increasing the cost of manipulation and discouraging malicious behavior.

Layer-2 security While inheriting the security of the underlying Ethereum blockchain ($Sec_{L2} \approx Sec_{L1}$), Optimistic Rollups introduce a potential vulnerability during the dispute period T_D. We mitigate this risk through robust fraud detection mechanisms D_f and the staking mechanism, which incentivizes honest validator behavior. The staking mechanism introduces a penalty function $Penalty(V_m, M)$ for malicious validator behavior M by validator V_m. This disincentivizes fraud and reduces the probability of fraudulent transactions being finalized $P(F_t)$.

Table 7 Security Measures and Mitigated Vulnerabilities

Security Layer	Measure	Mitigated Vulnerability/Threat
Smart Contracts	Auditing, Formal Verification (Subsection 2.3), Bug Bounties	Smart contract vulnerabilities (V_c)
Oracle Integration	Decentralized Oracles (Chainlink), Data Signing, Reputation Systems	Data Manipulation ($P(M_O)$), Outages ($P(O_O)$) (Subsection 3.4)
Layer-2 Operation	Fraud Detection (D_f), Staking Mechanism ($Penalty(V_m, M)$)	Fraudulent Transactions ($P(F_t)$), Dispute Period Vulnerability (Subsection 3.3)
Key Management	Multi-Signature ($MultiSig$), HSMs, Access Control (AC)	Unauthorized Access ($P(UA)$)
DoS Resistance	Rate Limiting (RL), Decentralized Validator Network	Denial-of-Service Attacks
Governance	Secure Voting, Quorum Requirements (Q)	Governance Attacks (Subsection 3.5)

Key management and access control Secure key management is crucial for protecting sensitive data. We employ multi-signature schemes ($MultiSig$) and Hardware Security Modules (HSMs) to enhance the security of key operations. Strict access control policies (AC), based on role-based access control (RBAC) principles, limit access to critical system components only to authorized personnel, thereby minimizing the risk of unauthorized access $P(UA)$.

Denial-of-service (DoS) resistance The platform is designed with DoS resistance in mind. Rate limiting (RL) and other mitigation techniques are employed to prevent disruptions caused by malicious actors. The decentralized nature of the validator network also contributes to inherent DoS resilience by distributing the points of potential attack.

Governance security The DAO governance model, secured by secure voting mechanisms and quorum requirements Q, prevents malicious control of the platform. The voting power $VP(h)$ of each holder h is proportional to their token holdings, promoting democratic decision-making and hindering manipulation by a single entity. The quorum requirement ensures that decisions are made with sufficient participation from the token holder community.

This multi-layered security approach, incorporating diverse techniques at each level, strengthens the platform's resilience and promotes trust in the RWA ecosystem. Continuous monitoring and vulnerability assessments allow us to adapt to the evolving threat landscape and maintain a proactive security posture.

4.2 Potential vulnerabilities

While our framework incorporates robust security measures, it's crucial to acknowledge potential vulnerabilities and propose mitigation strategies.

4.2.1 Smart contract vulnerabilities

Let C represent the set of all possible smart contracts deployed on our platform. Despite employing rigorous auditing and formal verification techniques, the possibility of a smart contract $c \in C$ containing an unforeseen vulnerability v cannot be entirely eliminated. We can express this as

$$P(v|c) > 0, \tag{20}$$

where $P(v|c)$ denotes the probability of a vulnerability v existing in a given contract c. To mitigate the risk associated with such vulnerabilities, we adopt a multi-pronged approach. First, a bug bounty program is introduced, incentivizing a set of external security experts E to identify vulnerabilities. This can be represented as a function

$$B : E \times V \to R, \tag{21}$$

where $B(e, v)$ is the reward offered to expert $e \in E$ for discovering vulnerability $v \in V$. Second, formal verification methods are employed, aiming to mathematically prove the correctness of the contract logic. This can be formalized as

$$\forall c \in C, \exists p \in P \tag{22}$$

such that $M \models p(c)$, where P is the set of properties a contract must satisfy, M is a formal model, and $p(c)$ represents the application of property p to contract c. Third, upgradable smart contracts are implemented, allowing for post-deployment patching of identified vulnerabilities. This can be represented as a function

$$U : C \times V \to C', \tag{23}$$

where $U(c, v)$ transforms a vulnerable contract c into a patched contract $c' \in C'$. Finally, an insurance fund I is established to compensate users in the event of an exploit. The fund's payout can be represented as a function

$$F : V \times L \to R, \tag{24}$$

where $F(v, l)$ is the compensation provided for losses $l \in L$ resulting from the exploitation of vulnerability v. This multilayered strategy aims to minimize the impact of potential smart contract vulnerabilities and maintain the overall security of the platform.

4.2.2 Oracle manipulation

Let D be the set of data sources used by our oracle mechanism and O be the set of oracle nodes. While decentralized oracle networks mitigate certain risks, the potential for manipulation persists. Let M represent the event of oracle manipulation. We aim to minimize $P(M)$, the probability of manipulation. To achieve this, we employ several strategies. Firstly, we utilize multiple independent data sources $|D| > 1$ for each data feed f. This redundancy can be represented as

$$f = d_1, d_2, ..., d_n, \tag{25}$$

where $d_i \in D$ and $n > 1$. The independence of these sources reduces the likelihood of a single point of failure or malicious influence. Secondly, on-chain data validation mechanisms are implemented. Let

$$V : D \to 0, 1 \tag{26}$$

be a validation function, where $V(d) = 1$ if data from source d passes validation and 0 otherwise. This validation helps detect anomalies and filter potentially manipulated data. Thirdly, a reputation system

$$R : O \to \mathbb{R} \tag{27}$$

is employed to track the performance and reliability of each oracle node $o \in O$. A higher reputation score $R(o)$ indicates higher trustworthiness. Finally, we leverage established decentralized oracle networks like Chainlink, which distribute trust across multiple nodes and further reduce $P(M)$. This multi-layered approach, combining data redundancy, validation, reputation tracking, and decentralization, enhances the security and reliability of our oracle mechanism, minimizing the risk of manipulation.

4.3 Layer-2 attacks

Optimistic Rollups, while offering scalability benefits, introduce specific security considerations. Let V be the set of validators on the Layer-2 network. A malicious validator $v_m \in V$ could attempt to censor transactions or submit fraudulent state roots S_f. To mitigate this, we impose a staking requirement S_r, where each validator $v \in V$ must stake a minimum amount of ETH. This staking requirement disincentivizes malicious behavior by introducing a financial penalty for misconduct. Formally, let $M(v)$ represent the malicious behavior of validator v, and $P(M(v)|S_r)$ be the probability of malicious behavior given the staking requirement. We aim to minimize $P(M(v)|S_r)$ by setting a sufficiently high S_r. Furthermore, a fraud proof mechanism allows any user $u \in U$ to challenge a potentially fraudulent state root S_f within a challenge period T. This can be represented as

$$C : U \times S_f \times T \to \{0, 1\}, \tag{28}$$

where $C(u, S_f, T) = 1$ if the challenge is successful. Additionally, validator rotation is implemented to limit the impact of a compromised node. Let

$$R : V \times T \to V' \tag{29}$$

be the rotation function, where $R(V, T)$ updates the set of validators after time T.

Another potential attack vector involves data withholding, where validators fail to publish data required for transaction processing. Let D be the set of transaction data. A data withholding attack can be represented as

$$W : V \times D \to \{0, 1\}, \tag{30}$$

where $W(v, d) = 1$ if validator v withholds data $d \in D$. To mitigate this, we employ data availability committees $A \subset V$, where a subset of validators is responsible for ensuring data availability. We can also introduce redundant data storage, where $d \in D$ is stored on multiple nodes, further reducing the probability of data loss. This combined approach mitigates the risks associated with malicious validators and data withholding attacks, enhancing the security and reliability of our Layer-2 solution.

4.3.1 Bribery attacks

ribery attacks represent a significant economic attack vector against Optimistic Rollups. In such an attack, an attacker incentivizes one or more validators to include fraudulent transactions or state updates by offering a financial reward, or bribe, that exceeds the expected rewards from honest validation. A successful bribe could lead to the finalization of fraudulent transactions, resulting in financial loss or system manipulation.

Our framework mitigates bribery attacks through several mechanisms. First, high staking requirements and substantial slashing penalties, as defined in Section 3.2, increase the economic cost for both the attacker and any colluding validator. Let $E_s(v)$ be the amount of ETH staked by validator v, and let $Slash(v, M(v))$ represent the slashing penalty for malicious behavior $M(v)$. For a bribe to be successful, the attacker's offered bribe, $B(v)$, must exceed the validator's expected rewards from honest behavior plus the expected loss from slashing:

$$B(v) > R(v) + P(\text{detection}) \cdot Slash(v, M(v)) \tag{31}$$

where $P(\text{detection})$ is the probability of the malicious behavior being detected and successfully challenged. Because $Slash(v, M(v))$ is a function of $E_s(v)$ (a significant portion or even all of the staked ETH), a large $E_s(v)$ significantly raises the cost of bribery.

Second, by leveraging ETH staking, we inherit a large and decentralized validator set, V. The cost of bribing a sufficient number of validators to control the outcome becomes prohibitively expensive as the size and diversity of V increase. Let $V_c \subset V$ be the set of validators the attacker needs to bribe to control the outcome. The total bribe cost, B_{total}, can be represented as:

$$B_{total} = \sum_{v \in V_c} B(v) \tag{32}$$

As the cardinality of V ($|V|$) increases, the required size of V_c also generally increases, driving up B_{total}.

Third, reputation systems (Section 3.4) further deter bribery. Validators with high reputation scores have more to lose (future rewards and delegation) by participating in an attack.

Fourth, the challenge-response mechanisms (fraud proofs, Section 3.3) provide a crucial defense. Even if bribed validators submit fraudulent state updates, other participants can challenge them, leading to transaction reversal and validator slashing.

Finally, monitoring systems (Section 4.1) detect unusual validator behavior (e.g., sudden changes in voting patterns or consistent submission of challenged batches), increasing P(detection) and thus the expected cost of bribery.

Economic modeling and game theory can analyze the effectiveness of these mitigations, informing parameter choices (e.g., minimum staking requirement S_r, slashing penalty percentage) to make bribery attacks economically infeasible.

4.4 Metering module security

While blockchain immutability ensures data integrity on-chain, it does not address the security of the data source. In our framework, the metering modules (e.g., in appliances) are the primary data source. A compromised metering module, denoted as M_c, could inject false data, d_f, into the system, which, if undetected, would be immutably stored, undermining system integrity. Let D_I represent the set of all data intended for the blockchain, and D_A be the set of all data actually added to the blockchain. Ideally, $D_I = D_A$. However, a compromised module introduces the risk that $D_A = D_I \cup \{d_f\} - \{d_t\}$, where d_t is valid data omitted by the compromised module. Therefore, metering module security is paramount.

Metering module security requires several key elements. Tamper resistance prevents physical attacks. Secure boot ensures only authorized firmware executes, typically using cryptographic signatures and a hardware-rooted chain of trust. Secure firmware updates, authenticated and integrity-checked, are essential to address vulnerabilities. The module must authenticate itself to the network (e.g., a smart meter) before submitting data, preventing unauthorized devices from injecting false data. Authentication might use cryptographic keys or certificates. Authorization ensures the module only submits data it's permitted to submit (e.g., energy consumption for its specific appliance). Data encryption (e.g., using TLS/SSL) protects data confidentiality and integrity during transmission. Key management, including secure storage and handling of cryptographic keys, is crucial. Intrusion detection mechanisms can also be implemented to detect and report anomalies.

To mitigate the risk of compromised modules, our framework advocates for several strategies. Hardware Security Modules (HSMs), dedicated tamper-resistant hardware, can protect cryptographic keys and perform sensitive operations. Trusted Execution Environments (TEEs), like ARM TrustZone or Intel SGX, provide an isolated execution environment for security-critical code (key management, data signing), reducing the attack surface. Cryptographic signatures are essential; the module digitally signs all submitted data using a private key. The smart contract verifies this signature, confirming data origin and integrity (See Section 4.1). The corresponding public key would be registered with the smart contract. Let $S(d, k_{priv})$ be the signature of data d using private key k_{priv}, and $V(d, s, k_{pub})$ be a verification function that returns true if signature s is valid for data d and public key k_{pub}, and false otherwise. The smart contract's verification can be represented as:

$$V(d, S(d, k_{priv}), k_{pub}) = \begin{cases} \text{true}, & \text{if } d \text{ is authentic and untampered} \\ \text{false}, & \text{otherwise} \end{cases} \tag{33}$$

Regular security audits of both hardware and software are crucial. Anomaly detection algorithms can identify unusual data patterns, potentially indicating a compromise. Redundancy, using multiple independent sensors, can improve reliability and help detect discrepancies. Finally, device attestation allows a device to prove its identity and the integrity of its software/firmware to a remote party, ensuring only legitimate modules connect and submit data.

4.5 Security implications

The security of our proposed framework is intrinsically linked to the security implications of our chosen Layer-2 solution, Optimistic Rollups, and our oracle mechanism, Chainlink. While both offer significant advantages, they also introduce specific security considerations that must be addressed.

4.5.1 Optimistic rollups security implications

The security of Optimistic Rollups hinges on two key aspects: fraud proof mechanisms and data availability. Let S_R represent a state root published on Layer-1. A fraud proof mechanism allows any honest participant $p \in P$ (where P is the set of all participants) to challenge the validity of S_R by submitting a fraud proof F_p within a challenge period T. We can represent this challenge process as a function

$$C : P \times S_R \times F_p \times T \to 0, 1, \tag{34}$$

where $C(p, S_R, F_p, T) = 1$ indicates a successful challenge. While effective, this mechanism introduces a delay Δt in transaction finality, where $\Delta t \leq T$. This delay, though generally acceptable for RWA transactions, could impact time-sensitive applications. The effectiveness of this mechanism also relies on the assumption that $\exists p \in P$ such that p is honest and capable of constructing F_p within T.

Data availability poses another challenge. While transaction data D is submitted to Layer-1, immediate accessibility for all participants cannot be guaranteed. Let $A(p, d, t)$ be a function representing the accessibility of data $d \in D$ to participant p at time t. A data availability issue arises when

$$\exists p \in P, \quad \exists d \in D, \quad \exists t \in [0, T] \tag{35}$$

such that $A(p, d, t) = 0$. This lack of access can hinder independent transaction verification and potentially enable censorship by malicious validators. Mitigating this requires robust data availability solutions, such as data availability committees or redundant data storage, effectively ensuring $A(p, d, t) = 1$ for all $p \in P$, $d \in D$, and $t > T_{DA}$, where T_{DA} is a short delay for data availability. Therefore, the security and practicality of Optimistic Rollups depend on the careful design and implementation of these mechanisms, balancing security with the timeliness of transaction processing.

4.5.2 Chainlink oracle security implications

Chainlink, while offering a decentralized oracle solution, presents certain security considerations. Decentralization, while enhancing security, can introduce latency. Let L_C be the latency of Chainlink and L_O be the latency of a centralized oracle. Generally, $L_C > L_O$, although the difference is often minimal. For time-sensitive applications, where a maximum acceptable latency L_{max} is defined, this difference could be a limiting factor if $L_C > L_{max}$.

Data source reliability is crucial. Let $D = d_1, d_2, ..., d_n$ be the set of data sources used by Chainlink. The reliability of the oracle data O_D depends on the reliability of each $d_i \in D$. Let $R(d_i)$ represent the reliability of data source d_i. A compromised data source d_c with $R(d_c) \approx 0$ can negatively impact the integrity of O_D. Robust data validation mechanisms, represented by a validation function

$$V : D \rightarrow 0, 1, \tag{36}$$

and the use of multiple independent data sources ($n > 1$) are crucial for mitigating this risk.

Finally, Chainlink's interaction with the Layer-2 network relies on smart contracts S_C. Vulnerabilities in S_C, represented by a vulnerability function $Vul(S_C)$, can compromise the oracle mechanism. Formally, if $Vul(S_C) = 1$ (vulnerability present), then the security of the oracle mechanism is compromised. Rigorous auditing and adherence to security best practices are therefore essential to minimize $P(Vul(S_C))$, the probability of a vulnerability existing in the smart contracts. Thus, careful consideration of these factors—latency, data source reliability, and smart contract security—is paramount for ensuring the overall security and reliability of the Chainlink oracle mechanism within our framework.

Addressing these security implications is crucial for building a robust and trustworthy RWA tokenization platform. We employ a multi-layered approach to security, combining the inherent strengths of Optimistic Rollups and Chainlink with additional security measures, such as fraud detection mechanisms, data validation checks, and robust key management practices. This comprehensive security strategy aims to mitigate the risks associated with our chosen Layer-2 solution and oracle mechanism while maximizing their benefits for scalability and efficient data integration.

5 Case study

5.1 Introduction

The energy sector is undergoing a significant transformation with the widespread adoption of smart meters. These devices generate vast quantities of granular data on electricity consumption, providing unprecedented insights into energy usage patterns. This data, while inherently valuable, faces challenges related to secure and efficient management, accessibility, and trust. Integrating smart meter data with blockchain technology presents a compelling solution to these challenges. Blockchain's inherent properties of transparency, traceability, and immutability enable the creation of a secure and auditable record of energy consumption. Furthermore, smart contracts can automate various processes, including billing, settlement, and even complex energy trading mechanisms, based on this trusted data stream.

This case study demonstrates the practical application of our proposed framework for Real-World Asset (RWA) tokenization, using smart meter data as a representative RWA. Our objectives are to validate the feasibility of integrating the framework's key components (tokenization, ETH staking for Layer-2 security, DAO governance, and oracle integration) in a real-world scenario; to evaluate the framework's effectiveness in addressing scalability, security, and decentralized governance challenges for high-frequency, low-value data; and to provide simulation-based empirical evidence supporting the paper's claims regarding performance and viability. Smart metering is chosen as the focal point because smart meter data is a tangible and quantifiable real-world asset (electricity consumption), the high-frequency nature of the readings aligns with Layer-2 scalability requirements, the low individual value of each reading benefits from Layer-2's reduced transaction costs, and the data offers a foundation for various blockchain applications beyond billing, including energy trading, carbon emission tracking, and demand-side management.

5.2 Experimental setup

5.2.1 Simulation environment

The experimental evaluation of our framework is conducted within a simulated environment implemented using Python and Jupyter Lab. This choice provides a flexible and controlled setting for experimentation, allowing for precise manipulation of system parameters and observation of their effects. The use of simulation is preferred over a real-world deployment at this stage due to considerations of cost-effectiveness, time constraints, and the need for complete control over the experimental conditions. A real-world deployment would introduce complexities and uncontrolled variables that are not essential for the core validation objectives of this case study.

The simulation environment faithfully emulates the core functionalities of the proposed framework. It incorporates a Layer-2 Optimistic Rollup, including transaction batching, state root calculation, and a basic fraud proof mechanism. ETH staking and slashing are modeled, with validators depositing ETH as collateral and facing penalties for submitting fraudulent blocks. A Decentralized Autonomous Organization (DAO) is simulated, enabling token holders to vote on proposals using various mechanisms (simple majority, quadratic, time-locked). Oracle integration is represented by a network of nodes retrieving, aggregating, and signing data from multiple independent sources, with dynamic reputation updates. Finally, smart meter behavior is modeled, generating realistic electricity consumption readings based on a pre-defined appliance profile.

It is important to acknowledge that while the simulation strives for realism, it necessarily simplifies certain aspects of a full-scale, real-world deployment. For instance, the fraud-proof mechanism is a simplified representation, and factors such as network latency are not explicitly modeled. However, the level of detail in the simulation is sufficient to evaluate the key performance characteristics and validate the core design principles of the framework.

5.2.2 Parameters

The simulation utilizes a range of parameters to represent the various components of the framework. These parameter values are, whenever possible, derived from realistic values observed in existing systems and informed by relevant literature. Table 8 presents a summary of the key parameters used in the simulation.

5.2.3 Data generation

Smart meter data The generation of realistic smart meter readings is a crucial aspect of the simulation. We employ an `ApplianceProfile` class, implemented in Python, to model the power consumption behavior of a refrigerator. This profile defines a set of distinct operational states (e.g., *idle*, *compressor_on*, *defrost*), each characterized by a specific power consumption level (in Watts) and a duration (in seconds). Transitions between these states

Table 8 Simulation Parameters

Category	Parameter Name	Value(s) and Rationale
Layer-1	`L1_BLOCK_TIME`	12 seconds. Approximate block time of Ethereum.
Layer-1	`L1_GAS_LIMIT`	30,000,000. A representative gas limit for Ethereum.
Layer-2	`L2_BLOCK_TIME`	2 seconds. Faster block time on Layer-2 to enhance throughput.
Layer-2	`DISPUTE_PERIOD`	604,800 seconds (7 days). Time window for challenging potentially fraudulent state roots.
Layer-2	`BATCH_SIZES`	[1, 10, 50, 100, 200]. Range of batch sizes used for scalability analysis.
Validator	`STAKING_REQUIREMENT`	32 ETH. Minimum ETH stake required to become a validator, consistent with Ethereum 2.0 specifications.
Validator	`NUM_VALIDATORS`	100/50. Number of validators in the simulations (the code demonstrates variations).
Oracle	`NUM_ORACLES`	10. Number of oracle nodes.
Oracle	`NUM_DATA_SOURCES`	5. Number of independent data sources per oracle.
Oracle	`ORACLE_REPUTATION_DECREASE`	5. Reputation decrease for incorrect oracle reports.
Oracle	`ORACLE_REPUTATION_INCREASE`	1. Reputation increase for correct oracle reports.

are governed by probabilities, creating a time-varying and realistic consumption pattern. The `Meter` class utilizes this `ApplianceProfile` to generate readings at 5-second intervals, simulating the data stream produced by a real smart meter. A simplified code snippet illustrating these classes is provided below:

```
class ApplianceProfile:
    def __init__(self, states, transitions):
        # ... (Implementation as provided in the code) ...

class Meter:
    def __init__(self, meter_id, private_key):
        # ... (Implementation as provided in the code) ...
    def generate_reading(self, model="random", **kwargs):
        # ... (Implementation as provided in the code) ...
```

Oracle data The simulation of oracle data involves multiple independent data sources. Each source provides a value for a given data point (e.g., the current electricity price), with added random noise to represent real-world measurement imperfections and potential biases. Oracle nodes, represented by the `OracleNode` class, retrieve data from these sources. They then aggregate the retrieved data; in this simulation, a simple average is used for aggregation. Finally, each oracle node signs the aggregated result using a simplified signing mechanism. The `OracleNode` class also maintains a reputation score for each oracle, which is updated dynamically based on the honesty of its reports, relative to the consensus value.

Layer-2 transactions Layer-2 transactions are simulated using the `Transaction` class. Each transaction represents a transfer of value, which in the context of this case study could represent a payment for electricity consumption. These individual transactions are then grouped into batches of varying sizes using the `simulate_layer2_transactions` function. This batching is a core mechanism of the Optimistic Rollup, allowing for increased transaction throughput.

5.3 Results and implications

5.3.1 Layer-2 scalability

A primary objective of this case study is to evaluate the scalability of our Layer-2 solution. We measure the transaction throughput (TPS) as a function of the batch size, a key parameter in Optimistic Rollups. The simulation results, directly extracted from the code's output, are presented below:

```
--- Layer-2 Scalability Simulation ---
Batch size: 1, Number of batches: 1000, TPS: 0.50
Batch size: 10, Number of batches: 100, TPS: 5.00
Batch size: 50, Number of batches: 20, TPS: 25.00
Batch size: 100, Number of batches: 10, TPS: 50.00
Batch size: 200, Number of batches: 5, TPS: 100.00
```

Analysis The data unequivocally demonstrate a substantial increase in TPS as the batch size increases. This relationship is a direct consequence of the batching mechanism in Optimistic Rollups. By grouping multiple transactions into a single batch, the fixed overhead associated with submitting a state root to Layer-1 is amortized across a larger number of transactions, leading to a significant improvement in overall throughput.

Comparison with layer-1 The observed TPS values achieved on Layer-2 are considerably higher than what could be achieved directly on Layer-1, given the inherent limitations of Ethereum's block time and gas limit. This underscores the effectiveness of our Layer-2 solution in addressing the scalability bottleneck.

Real-world implications These findings confirm the scalability advantages of employing a Layer-2 approach for managing high-frequency data streams, such as those generated by smart meters. The selection of an optimal batch size in a real-world deployment will necessitate a trade-off between maximizing throughput and minimizing transaction latency. However, the simulation demonstrates that high TPS can be realized with reasonably sized batches, making the system suitable for real-world applications.

5.3.2 Staking and security

The simulation incorporates a simplified fraud-proof mechanism to illustrate the security aspects of the framework. A malicious validator is deliberately introduced, and a fraudulent block containing an invalid transaction is submitted. Other validators have a 10% probability of detecting and challenging this fraudulent block. A successful challenge results in the slashing of the malicious validator's stake by 50%. An example of a successful challenge, as output by the simulation code, is shown below:

```
--- Staking and Security Simulation ---
Validator validator_33 successfully challenged block ...
Fraudulent block detected and challenged!
Validator validator_0 was slashed. Remaining stake: ...
```

Analysis The staking and slashing mechanisms are fundamental to the economic security of the Layer-2 network. The requirement for validators to stake ETH, coupled with the risk of losing a significant portion of that stake upon detection of malicious behavior, serves as a strong deterrent against attempts to compromise the system's integrity.

Real-World Implications The parameters governing staking requirements and slashing penalties are crucial design choices. In a real-world deployment, these parameters would require careful calibration to ensure a sufficient level of security without imposing overly punitive measures that might discourage honest validator participation.

5.3.3 DAO governance

The simulation demonstrates the operation of the DAO governance mechanism. Token holders are simulated, and they vote on proposals using different voting mechanisms: simple majority, quadratic voting, and time-locked voting. Examples of the simulation output for these voting scenarios are presented below:

```
--- DAO Governance Simulation ---
--- Simple Voting ---
Proposal 'Increase the dispute period to 14 days.' passed with ...
--- Quadratic Voting ---
Proposal 'Adjust the oracle reward mechanism.' passed with ...
```

Analysis The simulation highlights that different voting mechanisms can lead to different outcomes, even with the same set of voters and proposals. This reflects the varying ways in which voting power is distributed under each mechanism. Quadratic voting, for instance, tends to mitigate the influence of large token holders compared to simple majority voting, promoting a more balanced distribution of decision-making power.

Real-world implications The selection of a voting mechanism is a critical design decision for the DAO. It directly impacts the balance of power within the governance system and the ability of the community to effectively guide the platform's evolution. The chosen mechanism must strike a balance between efficiency and inclusivity.

5.3.4 Oracle integration

The simulation tracks the reputation of oracle nodes over time. Oracle nodes that consistently provide accurate data, close to the consensus value derived from multiple independent sources, see their reputation scores increase. Conversely, nodes that submit inaccurate or delayed data, simulated by adding noise, experience a decrease in their reputation. The simulation output, showing the final aggregated data from the oracles at each time step, is as follows:

```
--- Oracle Simulation (Enhanced) ---
Time: 1, Final aggregated data: ...
Time: 2, Final aggregated data: ...
...
```

Analysis The reputation system serves as a crucial incentive mechanism, encouraging oracle nodes to provide accurate and reliable data. It also provides a metric for users and smart contracts to assess the trustworthiness of the data being supplied.

Real-World Implications The parameters controlling the rate of reputation increase and decrease must be carefully tuned in a real-world deployment. The system should be responsive to changes in oracle behavior, penalizing malicious or unreliable nodes, but not overly sensitive to minor, unavoidable fluctuations in data accuracy.

5.4 Discussion

5.4.1 Advantages and limitations

The case study presented in Section 5 provides valuable insights into the advantages and limitations of our proposed framework.

Advantages The simulation results demonstrably support several key advantages. The Layer-2 solution, using Optimistic Rollups, achieves significantly higher transaction throughput (TPS) than Layer-1, crucial for handling high-frequency smart meter data. ETH staking and a simplified fraud-proof mechanism provide robust economic security, with slashing disincentivizing malicious validator behavior. The DAO simulation showcases the feasibility of community-driven governance, allowing token holder participation. The oracle simulation, with its reputation system, incentivizes honest data provision, contributing to data reliability. Finally, batching transactions on Layer-2 substantially reduces transaction costs compared to Layer-1 processing, enhancing cost-effectiveness.

Limitations Despite the encouraging simulation results, it is crucial to acknowledge certain limitations inherent in the current study and the framework's design. The simulation environment, while designed to be comprehensive, necessarily simplifies certain aspects of a real-world deployment. Factors such as network latency between nodes, the full complexities of validator interactions and consensus mechanisms, and the intricacies of a production-ready fraud-proof implementation are not modeled in complete detail. Furthermore, the security of the system, particularly the Layer-2 component built upon Optimistic Rollups, relies on the core assumptions of that design. A critical assumption is the continuous availability of at least one honest participant within the network who is capable of, and incentivized to, challenge any potentially fraudulent state roots within the defined dispute period. Finally, while the framework employs multiple independent oracle nodes to mitigate the risk of oracle centralization and data manipulation, this approach does not entirely eliminate the vulnerability. A sufficiently sophisticated attack that simultaneously targets multiple oracle nodes, or a systemic vulnerability that affects all oracle nodes, could still compromise the integrity of the data provided to the system.

5.4.2 Comparison with other approaches

Our proposed framework for RWA tokenization exhibits several distinct advantages when compared to alternative approaches currently available. First, in comparison to RWA tokenization platforms built directly on Layer-1 blockchains, our framework offers dramatically improved scalability. Layer-1 blockchains are inherently limited in their transaction throughput due to their block time and block size constraints. This limitation makes them unsuitable for applications involving high-frequency data streams, such as those generated by smart meters. Our framework overcomes this fundamental limitation through the use of off-chain transaction processing on Layer-2, enabling significantly higher transaction rates. Second, when contrasted with other Layer-2 scaling solutions, our framework's direct integration of ETH staking provides a superior degree of security and censorship resistance. Many existing Layer-2 solutions rely on separate, smaller validator sets or alternative consensus mechanisms, which can be more vulnerable to attacks or centralization. By leveraging the existing, large, and decentralized validator set of Ethereum, our framework inherits the robust security properties of the Ethereum mainnet. Finally, compared to traditional, centralized energy data management systems, our blockchain-based framework offers a fundamentally different approach. Centralized systems often lack transparency and auditability, and they may be less efficient due to manual processes and a reliance on intermediaries. Our framework, in contrast, provides inherent transparency, immutability, and automation through the use of blockchain technology and smart contracts, resulting in a more secure, efficient, and trustworthy solution for managing and utilizing energy data.

5.4.3 Future work

Building upon the findings of this study, several promising avenues for future research and development can be identified. Further research should enhance the fraud-proof mechanisms within the Layer-2 solution, potentially involving more sophisticated cryptographic techniques and alternative challenge-response protocols to improve efficiency and security. Developing more advanced economic models is also crucial for analyzing validator and oracle node incentives, including fine-grained analysis of staking rewards, slashing penalties, and reputation mechanisms to ensure long-term economic sustainability and security. This analysis should explicitly include evaluating the economic security and robustness of the DAO governance itself against potential manipulation, moving beyond the foundational mechanisms presented. While extending the current simulation environment to model more complex attack scenarios (such as coordinated oracle attacks or validator collusion) offers valuable insights into resilience, demonstrating real-world feasibility necessitates empirical validation.

Consequently, a crucial next phase involves a structured progression towards deployment, forming a roadmap for empirical validation. Initially, deploying the core framework components onto an Ethereum testnet will allow for functional validation of component interoperability, initial performance benchmarking against simulated results (e.g., TPS, latency), and testing of security mechanisms under controlled conditions. Following successful testnet validation, a targeted pilot program focused on a specific RWA category (e.g., tokenized equipment leases or specific financial instruments) is envisioned. This pilot would involve partnering with relevant stakeholders, integrating necessary off-chain processes like identity verification (KYC/AML), validating the end-to-end tokenization and management lifecycle with limited real-world value, assessing operational practicalities and costs, and gathering crucial user feedback to rigorously assess the framework's practicality.

Findings from these empirical stages will inform iterative refinements. Concurrently, exploring alternative Layer-2 scaling solutions, such as zk-Rollups (including zkEVMs), and different decentralized oracle networks remains important to evaluate their performance and security characteristics within the RWA tokenization context through comparative analysis. Furthermore, extending the simulation capabilities to explicitly model and quantitatively assess the practical resilience of the decentralized governance structure against specific attack vectors, such as Sybil attacks or whale dominance, particularly when employing alternative mechanisms like quadratic voting (briefly mentioned but not modelled herein), is necessary. Addressing the practical challenges of real-world data integration, including acquisition, cleansing, standardization, and privacy preservation, will also be essential. Achieving broader market integration and liquidity also requires addressing the current Ethereum-centric design; therefore, future work must actively investigate and evaluate secure and efficient cross-chain interoperability solutions. This involves exploring mechanisms such as established protocols (e.g., CCIP, IBC), bridging technologies, and token wrapping strategies to enable seamless interaction and asset movement between this framework and other relevant blockchain ecosystems. Finally, the development of user-friendly interfaces, including dashboards for data visualization, asset management tools, and intuitive DAO participation interfaces, is vital for facilitating wider adoption and realizing the framework's full potential.

5.5 Cost analysis & quantitative comparison

This section assesses the costs associated with developing, deploying, and operating the proposed framework. While a precise financial forecast depends heavily on specific implementation choices, prevailing market conditions (e.g., ETH price, L1 gas fees), and the scale of deployment, we first outline the primary cost categories and then present a quantitative comparison based on simulation results to illustrate the economic advantages of the proposed Layer-2 approach.

To provide a concrete illustration of the potential cost savings, we conducted a simulation comparing representative RWA transactions on Ethereum Layer-1 against our proposed Layer-2 solution (based on Optimistic Rollups). The simulation utilized Web3.py with a local Ganache instance, representing a low L1 gas price environment (~2 Gwei), and incorporated a simplified L2 cost model including operational gas, fixed fees, and amortized L1 data costs dependent on batch size. Table 9 summarizes the average costs derived from these simulations, assuming an ETH price of $2000 USD and a $0.1 USD fee for Oracle services where applicable.

The simulation results presented in Table 9 highlight several key economic aspects of the proposed framework. Firstly, the Layer-2 operational gas (L2 OpGas), representing the computational effort on the L2 network, is substantially lower than the equivalent L1 gas consumption across all transaction types, reflecting the inherent efficiency gains of off-chain computation. Secondly, the crucial role of batch size (BS) in Optimistic Rollups is evident. Increasing the batch size from 10 to 50 significantly reduces the average cost per L2 transaction. This occurs because the relatively fixed cost of submitting the L2 batch data and state root to L1 is amortized over a larger number of transactions, directly validating the scalability advantage of the rollup approach.

It is important to contextualize the direct L1 vs. L2 cost comparison within the simulation's low L1 gas price environment (~2 Gwei). Under these specific conditions, the L2 cost savings are less dramatic, and for smaller batch sizes, the combined cost of L2 fees and L1 data amortization can approach or even slightly exceed the minimal L1 cost. However, this simulation clearly demonstrates the *mechanism*

Table 9 Layer-1 vs. Layer-2 RWA Transaction Cost Comparison

Transaction Type	Platform	Avg. Gas	Avg. Cost (ETH)	Avg. Cost (USD)	Oracle Cost (USD)	Notes
RWA Issue (ERC-721)	Layer-1	74274	0.00002108	0.0422	N/A	L1 GasPrice: ≈ 2.00 Gwei
RWA Issue (ERC-721)	L2 (Sim.)	7427	0.00002009	0.0402	N/A	BS=10, L2 OpGas
RWA Issue (ERC-721)	L2 (Sim.)	7427	0.00001353	0.0271	N/A	BS=50, L2 OpGas
RWA Transfer (ERC-20)	Layer-1	52172	0.00001135	0.0227	N/A	L1 GasPrice: ≈ 2.00 Gwei
RWA Transfer (ERC-20)	L2 (Sim.)	5217	0.00001964	0.0393	N/A	BS=10, L2 OpGas
RWA Transfer (ERC-20)	L2 (Sim.)	5217	0.00001308	0.0262	N/A	BS=50, L2 OpGas
Yield Dist. (N=3)	Layer-1	139544	0.00001367	0.0273	N/A	L1 GasPrice: ≈ 2.00 Gwei
Yield Dist. (N=3)	L2 (Sim.)	13954	0.00002139	0.0428	N/A	BS=10, L2 OpGas
Yield Dist. (N=3)	L2 (Sim.)	13954	0.00001483	0.0297	N/A	BS=50, L2 OpGas
Governance Vote	Layer-1	73894	0.00000555	0.0111	N/A	L1 GasPrice: ≈ 2.00 Gwei
Governance Vote	L2 (Sim.)	7389	0.00002008	0.0402	N/A	BS=10, L2 OpGas
Governance Vote	L2 (Sim.)	7389	0.00001352	0.0270	N/A	BS=50, L2 OpGas
Oracle Update	Layer-1	48228	0.00000317	0.0063	0.1000	L1 GasPrice: ≈ 2.00 Gwei
Oracle Update	L2 (Sim.)	4823	0.00001956	0.0391	0.1000	BS=10, L2 OpGas
Oracle Update	L2 (Sim.)	4823	0.00001300	0.0260	0.1000	BS=50, L2 OpGas

Notes: L2 (Sim.) = Layer-2 Simulated costs. BS = Batch Size. L2 OpGas = Simulated operational gas on L2 (≈ 10% of L1 gas in this model). L1 Gas Price obtained from Ganache (~2.00 Gwei). ETH price assumed $2000 USD. Oracle Cost is an assumed service fee, independent of on-chain gas. N/A = Not Applicable by which L2 achieves cost savings. In real-world Ethereum mainnet scenarios, where L1 gas prices are often significantly higher (e.g., 10x, 50x, or more), the absolute L1 transaction costs would increase proportionally. In contrast, the dominant cost factor for L2 becomes the amortized L1 data cost, which scales much more favorably than full L1 execution. Therefore, under realistic network conditions, the cost advantage of the Layer-2 solution is expected to be substantial, potentially reducing transaction fees by orders of magnitude compared to Layer-1.

Furthermore, the simulation underscores the significance of Oracle costs for specific RWA operations. As seen in the "Oracle Update" transaction, the assumed $0.1 USD Oracle service fee constitutes the vast majority of the total cost in this low-gas simulation, dwarfing the on-chain gas expenses. This highlights that for RWA use cases heavily reliant on frequent external data feeds, optimizing Oracle usage and considering associated service fees is a critical component of the overall economic viability, independent of the chosen blockchain layer.

Beyond these transaction-specific costs derived from the simulation, the overall financial picture involves several other key categories detailed below.

5.5.1 Development costs

The creation of a robust and secure RWA tokenization platform, such as the one presented in this study, necessitates several significant upfront development costs. The most substantial of these costs is typically the skilled labor required to design, implement, and thoroughly test the system. This involves assembling a specialized team possessing expertise in various domains, including software engineering, smart contract development, security auditing, and project management. Specifically, a deep understanding of blockchain technology, cryptography, and distributed systems is essential for building a secure and reliable platform. Beyond labor costs, there are also potential software-related expenses. While a significant portion of the development process can leverage readily available open-source software and libraries, specialized development tools, comprehensive testing frameworks, or licensing fees for certain proprietary software components may be required. Finally, hardware costs can contribute to the overall development expenses. The development and testing phases may require dedicated hardware resources, including high-performance workstations for running simulations and conducting computationally intensive tasks. In addition, depending on the security requirements, specialized hardware security modules (HSMs) may be necessary to protect sensitive cryptographic keys and ensure the integrity of critical operations.

5.5.2 Deployment costs

Transitioning the framework from a development environment to a live, production setting entails several deployment costs associated with infrastructure provisioning and initial system configuration. A primary cost is the deployment of the necessary smart contracts to the Ethereum mainnet (Layer-1). This process incurs gas costs, which are directly proportional to the computational complexity of the smart contracts and the prevailing gas prices on the Ethereum network at the time of deployment. Furthermore, while the core transaction processing is offloaded to the Layer-2 network for scalability, there are potential server costs associated with running supporting infrastructure. This infrastructure may include relayers, which are responsible for facilitating secure communication and data transfer between the Layer-1 and Layer-2 networks. Additionally, data availability services may be required to ensure that transaction data remains accessible even in the event of Layer-2 unavailability. Finally, servers may be needed to host user interfaces and provide access points for interacting with the platform. In addition to these infrastructure-related costs, network bandwidth costs will be incurred due to the ongoing data transmission between the Layer-1 network, the Layer-2 network, and the integrated oracle networks. These costs will depend on the volume of data transmitted and the pricing structure of the network providers.

5.5.3 Operational costs

Maintaining the platform and processing transactions incurs ongoing operational costs. As highlighted by the simulation (Table 9), Layer-2 transaction fees are a primary component. These fees, while significantly lower per transaction than on Layer-1 due to rollup efficiencies (especially with larger batch sizes), still constitute a recurring expense influenced by L2 network activity and the cost of L1 data submission. Another key operational cost involves accessing external data via decentralized oracle networks (like Chainlink), which typically charge service fees based on usage and data requirements. Validator incentives for securing the Layer-2 network, usually funded from transaction fees, also represent an operational outflow necessary for system integrity. Finally, operating the DAO involves minor costs related to executing proposals on-chain and managing the treasury.

5.5.4 Legal and compliance costs

The operation of an RWA tokenization platform, particularly one dealing with assets like electricity consumption data, may be subject to a range of legal and regulatory requirements. The specific nature and extent of these requirements, and therefore the associated costs, will vary significantly depending on the nature of the tokenized assets and the jurisdictions in which the platform operates. Several key areas of legal and compliance costs can be anticipated. Firstly, compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations is often mandatory. This typically necessitates verifying the identities of users interacting with the platform, which may involve integrating with and paying for services provided by third-party KYC/AML verification providers. Secondly, adherence to data privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the United States, is crucial. Meeting these requirements may necessitate substantial investments in data security infrastructure, privacy-enhancing technologies, and ongoing compliance efforts. Finally, depending on the specific regulatory landscape and the classification of the tokenized assets, there may be costs associated with reporting to relevant regulatory authorities. This could involve preparing and submitting regular reports, undergoing audits, and maintaining ongoing communication with regulators.

5.5.5 Comparison with traditional systems

Compared to traditional, centralized systems for managing real-world assets and related data, the proposed blockchain-based framework offers the potential for substantial cost reductions. The automation enabled by smart contracts, the reduced reliance on intermediaries, and the increased efficiency of Layer-2 transaction processing, as quantitatively indicated by the simulation results, can lead to significant operational cost savings, particularly under high L1 gas fee conditions. Furthermore, the inherent transparency and auditability of blockchain technology can reduce costs associated with fraud prevention and dispute resolution.

5.5.6 Factors influencing costs

The overall costs associated with developing, deploying, and operating the proposed RWA tokenization framework are subject to several influential factors. The scale of deployment plays a crucial role. A larger number of users, smart meters, and other connected devices directly translates to higher transaction volumes on the Layer-2 network, increased data storage requirements, and potentially greater costs associated with KYC/AML verification if applicable. The frequency of transactions is another significant factor. Higher transaction frequencies, such as more frequent smart meter readings, lead to a greater number of transactions processed on the Layer-2 network, thus increasing Layer-2 transaction fees. Similarly, higher data update frequencies from oracles can result in increased oracle data costs. The regulatory landscape is a major determinant of costs. The specific regulatory requirements imposed by relevant jurisdictions, including KYC/AML, data privacy, and reporting obligations, can significantly impact the legal and compliance costs incurred by the platform. The choice of underlying technologies also has cost implications. Different Layer-2 scaling solutions (e.g., Optimistic Rollups, zk-Rollups) and different decentralized oracle networks (e.g., Chainlink, other providers) have varying cost structures, affecting both the initial deployment costs and the ongoing operational expenses. Finally, market volatility, particularly fluctuations in the price of ETH and gas prices on the Ethereum network, can impact various cost components. These include the costs of deploying smart contracts, the economic incentives for validators (rewards and slashing), and the fees associated with Layer-2 transactions.

6 Conclusion

This paper presented a novel blockchain-based framework for the tokenization and management of Real-World Assets (RWAs). Our key contributions include: (1) the design and implementation of a modular and adaptable framework that supports diverse asset classes; (2) the integration of decentralized governance mechanisms to empower stakeholders and promote transparency; and (3) the incorporation of a Layer-2 scaling solution to address scalability challenges.

Our experimental evaluation demonstrated the feasibility and efficiency of the proposed framework. We successfully tokenized both fungible and non-fungible assets, simulated user interactions with the staking and governance mechanisms, and demonstrated the functionality of the Optimistic Rollup scaling solution. The results showed that our framework can achieve high throughput and low latency while maintaining robust security and transparency.

Our analysis of the potential impact of the framework on the RWA market revealed significant opportunities for democratizing access to investment opportunities, enhancing liquidity, reducing transaction costs, and improving regulatory compliance. While challenges remain, such as addressing interoperability and fostering wider adoption, we believe our framework provides a solid foundation for transforming the RWA landscape. By directly addressing the scalability limitations of Ethereum through Layer-2 integration, and enhancing security through a novel combination of ETH staking and a DAO-governed approach, our research provides a concrete foundation for building a more efficient, transparent, and accessible RWA ecosystem. For example, The integration of Layer-2 solutions such as Optimistic Rollups can lead to a tenfold or greater improvement in transaction throughput, and the DAO governance can be used to adjust key parameters such as the threshold. However, we acknowledge that scalability remains an ongoing challenge for blockchain-based systems in general. Our framework directly addresses this challenge through the integration of Layer-2 scaling, specifically Optimistic Rollups. By processing transactions off-chain and submitting only compressed batches to the Ethereum mainnet, we achieve significant improvements in transaction throughput and reductions in gas costs, as demonstrated in our experimental results (Section 5.2). Furthermore, we employ specific optimizations within our Optimistic Rollup implementation, such as grouping similar RWA transactions to maximize compression efficiency and leveraging time-delayed batching, taking advantage of RWA's relatively longer settlement times compared with traditional cryptocurrencies.

Future work will focus on refining the framework's security features, exploring alternative scaling solutions, developing user-friendly interfaces to facilitate broader adoption and addressing adoption challenges. Specifically, we plan to investigate alternative Layer-2 solutions like zk-Rollups and state channels, and to perform a comparative analysis to determine their suitability for different RWA use cases. In the longer term, we will explore more radical scalability solutions such as sharding, which involves partitioning the blockchain network into smaller shards to enable parallel processing. Ongoing research into data availability solutions (e.g., data availability sampling, EIP-4844) will also be crucial for achieving further scalability improvements. We also anticipate that improving hardware capability will be helpful. In particular, the emergence of zkEVMs presents a compelling alternative to Optimistic Rollups, offering potential advantages in terms of security and finality. A comparative analysis of different Layer-2 solutions, including zkEVMs, within the context of RWA tokenization is a key area for future investigation. Furthermore, exploring the integration of our framework with hybrid blockchain solutions, which combine the benefits of public and private blockchains, could be valuable for addressing regulatory compliance and data privacy concerns in specific RWA use cases. Finally, investigating interoperability with other blockchain platforms is crucial. The development of robust interoperability protocols, such as Cosmos's Inter-Blockchain Communication (IBC) protocol and Chainlink's Cross-Chain Interoperability Protocol (CCIP), is opening up new possibilities for cross-chain asset transfers and data sharing. Integrating our framework with these protocols would enable seamless interaction with other blockchain ecosystems, expanding the reach and utility of tokenized RWAs. We are confident that our research will contribute to the ongoing development of a more efficient, transparent, and accessible RWA ecosystem.

Author Contributions Xiaofei Zhao, as the lead author, spearheaded the conceptualization of this novel framework for secure and scalable real-world asset tokenization, guiding its methodological development with a focus on integrating Ethereum staking and Layer-2 solutions. His oversight extended to the design of the hybrid token standard and the robust due diligence process. Jieqiong Ding played a crucial role in refining the hybrid token standard and extensively researched existing tokenization platforms, contributing significantly to the investigation of oracle manipulation vulnerabilities and the documentation of the due diligence process. Yunqi Su's expertise was vital in analyzing Ethereum staking mechanisms and Layer-2 scaling, particularly Optimistic Rollups, while also contributing to the security analysis concerning smart contracts. Hua Wang focused on assessing the framework's real-world applicability and the regulatory context of asset tokenization, offering valuable insights into practical implementation challenges. Fanglin Guo supported the research effort through literature reviews on existing tokenization approaches and contributed to the design of the decentralized oracle network and discussions surrounding the governance model. As student authors, Qianggang Zhang aided in implementing smart contracts for tokenization and staking, alongside contributing to the experimental setup for the case study, while Minyang Mu assisted in the implementation and testing of the DAO governance smart contracts, further contributing to the literature review on blockchain security.

Funding Not Applicable.

Data Availability The data and code used in this study are publicly available and can be accessed at the following GitHub repository: https://github.com/xifezhao/eth-rwa-tokenization

Declarations

Competing Interests The authors declare no competing interests.

References

1. Mottaghi SF, Steininger BI, Yanagawa N (2024) Real estate insights: The current state and the new future of tokenization in real estate. J Property Invest Finance 42(6):614–620. https://doi.org/10.1108/JPIF-07-2024-0087
2. Gong H (2024) In: Gong H (ed) Tokenised Real-World Assets (RWA) and Decentralised Physical Infrastructure Networks (DePIN), pp 175–197. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0491-5_6
3. Bamakan SMH, Nezhadsistani N, Bodaghi O, Qu Q (2022) Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. Sci Reports 12(1):2178. https://doi.org/10.1038/s41598-022-05920-6
4. Ferrezuelo RD (2023) Risk assessment of digital assets insurance applications in cryptocurrencies and nfts
5. Chen Y (2018) Blockchain tokens and the potential democratization of entrepreneurship and innovation. Business Horizons 61(4):567–575. https://doi.org/10.1016/j.bushor.2018.03.006
6. Lee JY (2019) A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. Business Horizons 62(6):773–784. https://doi.org/10.1016/j.bushor.2019.08.003
7. Baum A (2021) Tokenization–the future of real estate investment. The J Portfolio Manage 47(10):41–61
8. Mazzorana-Kremer F (2019) Blockchain-based equity and stos: Towards a liquid market for sme financing? Theoret Econ Lett 9(5):1534–1552. https://doi.org/10.4236/tel.2019.95099
9. Alamsyah A, Muhammad IF (2024) Unraveling the crypto market: A journey into decentralized finance transaction network. Digital Business 4(1):100074. https://doi.org/10.1016/j.digbus.2024.100074

10. Jameaba M-S (2024) Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Sector and Beyond. [Online; accessed 3. Jan. 2025]. https://doi.org/10.2139/ssrn.4808469 . https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4808469
11. Christodoulou I, Rizomyliotis I, Konstantoulaki K, Nazarian A, Binh D (2024) Transforming the remittance industry: harnessing the power of blockchain technology. J Enterprise Inf Manage 37(5):1551–1577. https://doi.org/10.1108/JEIM-03-2023-0112
12. Welfare A (2019) Commercializing Blockchain: Strategic Applications in the Real World. John Wiley & Sons, ???
13. He Z, Li Z, Yang S, Qiao A, Zhang X, Luo X, Chen T (2024) Large language models for blockchain security: A systematic literature review. ArXiv e-prints. https://doi.org/10.48550/arXiv.2403.14280
14. Cao X, Zhang J, Wu X, Liu B (2022) A survey on security in consensus and smart contracts. Peer-to-Peer Netw Appl 15(2):1008–1028. https://doi.org/10.1007/s12083-021-01268-2
15. Series OBP (2020) The tokenisation of assets and potential implications for financial markets. The Secretary General of the OECD 107
16. Cappai M (2023) The role of private and public regulation in the case study of crypto-assets: The italian move towards participatory regulation. Comput Law Secur Rev 49:105831. https://doi.org/10.1016/j.clsr.2023.105831
17. Baltais M, Sondore E, Putniņša TJ, Karlsen JR (2024) Economic impact potential of real-world asset tokenization. UTS Business School, University of Technology Sydney, Report, 2024–06
18. Edelman R (2022) The Truth About Crypto: A Practical, Easy-to-Understand Guide to Bitcoin, Blockchain, NFTs, and Other Digital Assets. Simon and Schuster, ???
19. Sguanci C, Spatafora R, Vergani AM (2021) Layer 2 blockchain scaling: a survey. ArXiv e-prints https://doi.org/10.48550/arXiv.2107.10881
20. Mandal M, Chishti MS, Banerjee A. Investigating layer-2 scalability solutions for blockchain applications. In: 2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), pp 710–717. https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys60770.2023.00101
21. Michelson K, Sridharan A, Cabuk UC, Reesor E, Stolman B, Mailen D, Bunfield D, Smith J, Snow P (2022) Accumulate: An identity-based blockchain protocol with cross-chain support, human-readable addresses, and key management capabilities. ArXiv e-prints. https://doi.org/10.48550/arXiv.2204.06878
22. Grandjean D, Heimbach L, Wattenhofer R (2024) Ethereum proof-of-stake consensus layer: Participation and decentralization. In: Budurushi J, Kulyk O, Allen S, Diamandis T, Klages-Mundt A, Bracciali A, Goodell G, Matsuo S (eds) Financial Cryptography and Data Security. FC 2024 International Workshops, pp 253–280. Springer
23. Takei Y, Shudo K. Effective ethereum staking in cryptocurrency exchanges. In: 2024 IEEE International Conference on Blockchain (Blockchain), pp 332–339. https://doi.org/10.1109/Blockchain62396.2024.00050
24. Cong LW, He Z, Tang K (2022) The Tokenomics of Staking. [Online; accessed 4. Jan. 2025]. https://doi.org/10.2139/ssrn.4059460 . https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=4059460
25. McCorry P, Buckland C, Yee B, Song D (2021) Sok: Validating bridges as a scaling solution for blockchains. Cryptol ePrint Archive
26. Fekete DL, Kiss A (2023). Toward Building Smart Contract-Based Higher Education Systems Using Zero-Knowledge Ethereum Virtual Machine. https://doi.org/10.3390/electronics12030664
27. Kim SK, Ma Z, Murali S, Mason J, Miller A, Bailey M (2018) Measuring Ethereum Network Peers. Ass Comput Mach. https://doi.org/10.1145/3278532.3278542
28. Zhang L, Lee B, Ye Y, Qiao Y. Ethereum transaction performance evaluation using test-nets. In: Schwardmann U, Boehme C, B Heras D, Cardellini V, Jeannot E, Salis A, Schifanella C, Manumachu RR, Schwamborn D, Ricci L, Sangyoon O, Gruber T, Antonelli L, Scott SL (eds) Euro-Par 2019: Parallel Processing Workshops, pp 179–190. Springer
29. Aspris A, Dyhrberg AH, Putniņš TJ, Foley S (2022) Digital Assets and Markets: A Transaction-Cost analysis of market architectures. [Online; accessed 3. Jan. 2025]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4301258
30. Wijesekara PA, Gunawardena S (2023) A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges. https://doi.org/10.3390/network3030017
31. Esmat A, Vos M, Ghiassi-Farrokhfal Y, Palensky P, Epema D (2021) A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. Appl Energy 282:116123. https://doi.org/10.1016/j.apenergy.2020.116123
32. Ahmed H (2024) Security tokens, ecosystems and financial inclusion: Islamic perspectives. Int J Islamic Middle Eastern Finance Manage 17(4):730–745. https://doi.org/10.1108/IMEFM-04-2024-0195
33. Pasdar A, Lee YC, Dong Z (2023) Connect api with blockchain: A survey on blockchain oracle implementation. ACM Comput Surv 55(10):208. https://doi.org/10.1145/3567582
34. Ciriello RF (2021) Tokenized index funds: A blockchain-based concept and a multidisciplinary research framework. Int J Inf Manage 61:102400. https://doi.org/10.1016/j.ijinfomgt.2021.102400
35. Sunyaev A, Kannengießer N, Beck R, Treiblmaier H, Lacity M, Kranz J, Fridgen G, Spankowski U, Luckow A (2021) Token economy. Business Inf Syst Eng 63(4):457–478. https://doi.org/10.1007/s12599-021-00684-1
36. Androulaki E, Camenisch J, Caro AD, Dubovitskaya M, Elkhiyaoui K, Tackmann B (2020) Privacy-preserving auditable token payments in a permissioned blockchain system. Ass Comput Mach. https://doi.org/10.1145/3419614.3423259.
37. Heines R, Dick C, Pohle C, Jung R (2021) The tokenization of everything: Towards a framework for understanding the potentials of tokenized assets. PACIS 40
38. Ahmadi S (2020) A Tokenization System for the Kurdish Language. ACL Anthology, 114–127
39. Monrat AA, Schelén O, Andersson K (2019) A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access 7:117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094
40. Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with iot. challenges and opportunities. Future Gener Comput Syst 88:173–190. https://doi.org/10.1016/j.future.2018.05.046
41. Zheng Z, Xie S, Dai H-N, Chen W, Chen X, Weng J, Imran M (2020) An overview on smart contracts: Challenges, advances and platforms. Future Gener Comput Syst 105:475–491. https://doi.org/10.1016/j.future.2019.12.019
42. Sayeed S, Marco-Gisbert H, Caira T (2020) Smart contract: Attacks and protections. IEEE Access 8:24416–24427. https://doi.org/10.1109/ACCESS.2020.2970495
43. Fang Y, Han S, Huang C, Wu R (2019) Tap: A static analysis model for php vulnerabilities based on token and deep learning technology. PLOS ONE 14(11):0225196. https://doi.org/10.1371/journal.pone.0225196
44. Chod J, Trichakis N, Yang SA (2022) Platform tokenization: Financing, governance, and moral hazard. Manage Sci

45. Belchior R, Vasconcelos A, Guerreiro S, Correia M (2021) A survey on blockchain interoperability: Past, present, and future trends. ACM Comput Surv 54(8):168. https://doi.org/10.1145/3471140
46. Beniiche A (2020) A study of blockchain oracles. ArXiv e-prints https://doi.org/10.48550/arXiv.2004.07140
47. Choo S, Kim W (2023) A study on the evaluation of tokenizer performance in natural language processing. Appl Artif Intell 37(1):2175112. https://doi.org/10.1080/08839514.2023.2175112

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Xiaofei Zhao is currently an Associate Professor at Lanzhou Petrochemical University of Vocational Technology and a Ph.D. candidate at Lanzhou Jiaotong University. Her research interests include the design and application of emerging digital technologies, with a focus on improving the efficiency and reliability of modern information systems.

Jieqiong Ding leads Public Warning Services at the Gansu Meteorological Service Centre and holds a master's degree from Zhejiang Sci-Tech University. Her research explores meteorological data mining, the impact of climate on economic development, and related security issues, aiming to improve public safety and economic resilience through data-driven insights. She focuses on developing and implementing data-driven strategies for effective public warning dissemination and emergency response.

Yunqi Su is a faculty member at the School of Information Engineering, Lanzhou Petrochemical University of Vocational Technology, holding a Master's degree in Computer Science and Technology from the University of Southampton. His research focuses on digital strategy and information systems, particularly cloud computing strategies, data security in information systems.

Hua Wang is the Big Data Business Lead and Security Manager at State Grid Gansu Electric Power Company, holding a Master's degree in Computer Science from Lanzhou University of Technology. She leads the development and implementation of big data strategies and solutions, with a particular focus on data security and risk mitigation. She oversees multiple teams dedicated to leveraging power grid operational data to enhance system security, operational efficiency, and the reliability of grid management.

Fanglin Guo is the Big Data Business Lead and Laboratory Director at State Grid Gansu Electric Power Company, holding a Master's degree in Computer Science from Lanzhou Jiaotong University. She leads the development and implementation of big data strategies and solutions, directing multiple laboratories focused on leveraging power grid operational data for improved efficiency, reliability, and grid management.

Qianggang Zhang is an undergraduate student in IoT Engineering Technology at the School of Information Engineering, Lanzhou Petrochemical University of Vocational Technology. He contributed significantly to the development, implementation, and experimental validation of the blockchain framework presented in this paper.

Mingyang Mu is an student in Network Technology at the School of Information Engineering, Lanzhou Petrochemical University of Vocational Technology. He contributed significantly to the development, implementation, and experimental validation of the smart contract described in this paper.

Authors and Affiliations

Xiaofei Zhao[1,2] · **Jieqiong Ding**[3] · **Yunqi Su**[1] · **Hua Wang**[4] · **Fanglin Guo**[4] · **Qianggang Zhang**[1] · **Mingyang Mu**[1]

✉ Xiaofei Zhao
xifizhao@gmail.com

Jieqiong Ding
dgjeqiong@gmail.com

Yunqi Su
suyunqi@lzpuvt.edu.cn

Hua Wang
whscdx1126@outlook.com

Fanglin Guo
fglnguo@gmail.com

Qianggang Zhang
3361211871@qq.com

Mingyang Mu
1543807310@qq.com

[1] School of Information Engineering, Lanzhou Petrochemical University of Vocational Technology, No. 1, Shandan Street Xigu District, Lanzhou 730060, Gansu, China

[2] School of Automation, Lanzhou Jiaotong University, No. 88, Anning West Road Anning District, Lanzhou 730070, Gansu, China

[3] Public Information Office, Gansu Province Meteorological Service Center, No.2070 Donggang East Road Chengguan District, Lanzhou 730030, Gansu, China

[4] Digital Business Division, State Grid Gansu Electric Power Company, No. 629, Xijin East Road Qilihe District, Lanzhou 730050, Gansu, China