
LitVM
Litecoin's Virtual Machine
LitVM Litepaper V1.2
www.litvm.com

Contents

Abstract

LitVM is Litecoin's first trustless EVM rollup, designed to unlock the full spectrum of Web3 functionality for the Litecoin community. Officially endorsed by the Litecoin Foundation, LitVM transforms Litecoin from a payment-focused network into a fully programmable Web3 ecosystem.

Built using Arbitrum Nitro and powered by BitcoinOS technology, LitVM delivers a decentralized, EVM-compatible smart contract layer on Litecoin—enabling Web3 functionality such as yield markets, DeFi, real-world asset (RWA) tokenization, and AI-driven applications while inheriting Litecoin's battle-tested proof-of-work security.

LitVM follows the mantra of "Hard Money Web3"—bringing the principles of hard money (scarcity, security, and decentralization) to programmable blockchain applications. Enabling trustless bridging of native Litecoin and Litecoin-native assets via BitcoinOS's ZK technology, LitVM empowers these decentralized assets (alongside EVM-native assets) with lightning-fast EVM smart contract capabilities.

By fostering interoperability with Ethereum while anchoring security to Litecoin, LitVM aims to redefine Litecoin's role in the modern Web3 landscape.

1. Introduction

1.1 Background: The Evolution of Litecoin

Litecoin (LTC), launched in 2011 by Charlie Lee, was created as a faster, more efficient complement to Bitcoin, often described as the "silver to Bitcoin's gold." Built on a Scrypt-based proof-of-work (PoW) consensus mechanism, Litecoin offers a 2.5-minute block time—four times faster than Bitcoin's—enabling rapid transaction confirmations and low fees, typically under $0.01. These attributes have made Litecoin a preferred choice for everyday payments, microtransactions, and merchant adoption, with integrations in payment processors like Travala and BitPay (where it tops the rankings as the most used cryptocurrency by transaction volume). Over its 14-year history, Litecoin has maintained a

prominent position in the cryptocurrency rankings, with a market cap exceeding $20 billion at its peak, over 370 million lifetime transactions processed, and hundreds of thousands of daily active addresses.

Litecoin's development has prioritized simplicity, security, and decentralization, aligning with Bitcoin's core principles. Key milestones include its early adoption of Segregated Witness (SegWit) in 2017, which improved transaction malleability and enabled future scaling solutions, and the introduction of MimbleWimble Extension Blocks (MWEB) in 2022, which added optional privacy for shielded transactions. This has solidified Litecoin's reputation as an innovator when it comes to features later adopted by Bitcoin, reinforcing its role as a complementary network.

However, the rise of smart contract platforms like Ethereum, which supports DeFi, NFT infrastructure, and a wide array of decentralized applications (dApps), has exposed limitations in Litecoin's Layer-1 (L1) design. Lacking native smart contract functionality, Litecoin has been unable to support complex Web3 use cases, restricting its participation in high-growth sectors. While Litecoin's focus on payment efficiency remains a strength, the absence of a scalable Layer-2 (L2) rollup has hindered its ability to compete in the rapidly evolving Web3 ecosystem, where programmability and interoperability are paramount.

Furthermore, while the Bitcoin ecosystem has witnessed the birth of numerous L2s to provide extended functionality to the Bitcoin mainchain, Litecoin has significantly lagged behind. This undermines the previous work Litecoin has done to forge its position as Bitcoin's innovative counterpart for new upgrades and functionality, and threatens its continued relevance in the modern blockchain landscape.

1.2 The Need for a Litecoin Rollup

Layer-2 solutions have become a cornerstone of blockchain scalability, enabling blockchains to process transactions off-chain while preserving the security and decentralization of the mainnet (Layer-1). Technologies like zero-knowledge rollups (zkRollups) and optimistic rollups batch thousands of transactions into compact proofs, reducing congestion, lowering fees, and supporting complex computations. For Litecoin, an L2 solution is critical to address its current limitations and unlock new opportunities:

Enhance Scalability: Litecoin's L1 processes approximately 50 transactions per second (TPS), insufficient for Web3 applications requiring high throughput. A rollup can scale to thousands of TPS, supporting and unlocking new use cases for LTC and Litecoin-native assets like LTC-20 tokens, Ordinals, and Runes.

Enable Smart Contracts: By introducing Ethereum Virtual Machine (EVM) compatibility, a rollup allows developers to deploy smart contracts for yield markets, DeFi protocols, RWA platforms, AI applications, NFT marketplaces, gaming dApps, and more, expanding Litecoin's utility far beyond payments.

Foster Innovation: A rollup attracts developers to build tailored applications, leveraging Litecoin's low-cost transactions and privacy focus to create novel use cases, such as tokenized real-world assets (RWAs), institutional-grade yield strategies, and AI-integrated consumer applications.

Strengthen Interoperability: A trustless rollup can bridge Litecoin with Ethereum's ecosystem while aligning with Bitcoin's decentralized ethos, enabling cross-chain asset transfers and collaborative dApps.

Without a robust rollup, Litecoin risks being sidelined in the Web3 era, where scalability and programmability drive adoption. LitVM addresses these needs by providing a trustless EVM rollup that preserves Litecoin's core strengths while integrating advanced Web3 capabilities.

1.3 LitVM's Vision

LitVM is Litecoin's first trustless EVM rollup, designed to propel Litecoin into the forefront of the Web3 era. By combining Litecoin's fast, low-cost transactions with Ethereum's programmability and Bitcoin's philosophical alignment, LitVM unlocks a wide range of use cases, including yield markets, RWAs, AI applications, DeFi, and more.

LitVM leverages a hybrid rollup architecture—combining the speed of optimistic rollups with the cryptographic security of zero-knowledge proofs—to process transactions off-chain while anchoring their validity to both Litecoin and Ethereum. This dual-settlement approach provides flexibility, enhanced security, and resilience as LitVM progressively migrates to full Litecoin-native settlement.

The vision of LitVM is to create a vibrant, community-driven ecosystem where:

- **Litecoin Users** can access advanced Web3 services, such as earning yield on LTC through DeFi protocols, participating in tokenized real-world assets, or engaging with AI-powered applications, all with sub-cent fees.
- **Developers** can build scalable dApps using familiar Ethereum tools (e.g., Solidity, Hardhat, Foundry, MetaMask), integrating Litecoin-native assets and cross-chain data.

- **The Broader Crypto Ecosystem** benefits from trustless interoperability, enabling seamless asset transfers between Litecoin, Ethereum, and potentially Bitcoin via BitcoinOS infrastructure.
- **Bitcoin's Principles** are upheld through a decentralized, trust-minimized design, supporting programmable BTC and fostering collaboration between Litecoin and Bitcoin communities.

LitVM aims to redefine Litecoin's role as a Hard Money Web3 hub, cementing its position as the "silver" that complements Bitcoin's "gold" in the modern Web3 era, while tapping into Ethereum's programmable infrastructure. By empowering the Litecoin community with tools for innovation and interoperability, LitVM seeks to drive long-term adoption and growth of the broader Litecoin ecosystem.

1.4 Market Context and Opportunity

The Web3 market, valued at $4.62 billion in 2025 (in terms of revenue generated by Web3-related services, applications, and infrastructure), is projected to reach $99.75 billion by 2034, driven by a compound annual growth rate (CAGR) of 41.18%. Layer-2 solutions are pivotal to this growth, addressing the scalability and cost challenges of Layer-1 blockchains. Rollup technologies have emerged as the most robust L2 approach, offering high throughput (up to thousands of TPS), low fees (sub-cent), and robust security through cryptographic proofs. These platforms have fueled the expansion of DeFi, with a total value locked (TVL) exceeding $100 billion, and NFTs, with over $20 billion in trading volume in 2024, alongside emerging sectors like RWAs, AI, and gaming.

Litecoin, with its $5+ billion market cap, hundreds of thousands of daily active addresses, and over 370 million lifetime transactions, holds a unique position in the cryptocurrency landscape. Its 2.5-minute block times and sub-$0.01 fees make it ideal for payments, processing over 1 million daily transactions at peak. However, its lack of smart contract functionality has excluded it from DeFi and other burgeoning Web3 sectors, limiting its growth potential. In contrast, Ethereum’s ecosystem, hosting $300+ billion in assets and 10,000+ monthly active developers, dominates Web3, while Bitcoin’s $2 trillion+ market cap underscores its role as a secure store-of-value layer.

LitVM seizes this opportunity by providing an EVM-compatible rollup that focuses on the Litecoin ecosystem, integrating Litecoin-native assets (LTC, LTC-20, Runes, Ordinals) with Ethereum's developer ecosystem. By catering to Litecoin's loyal community and Ethereum's vast developer base, LitVM can capture market share in high-growth sectors.

Key market opportunities include:

- **Yield Markets:** Enabling Litecoin users to participate in DeFi protocols, institutional-grade yield strategies, and other yield-generating opportunities, with potential TVL growth to billions.
- **Real-World Assets (RWAs):** Facilitating tokenized assets (e.g., commodities like silver and gold, real estate, and physical collectibles) with L1-secured infrastructure and programmable smart contracts.
- **AI Ecosystem:** Supporting Litecoin-powered AI agents, AI-enhanced Web3 applications, and future-proofing in the age of artificial intelligence.
- **Advanced Payments:** Building on Litecoin's payment infrastructure with programmable payment rails and stablecoin support.
- **NFTs and Ordinals:** Supporting Litecoin-native NFT/Ordinals marketplaces and infrastructure, leveraging Litecoin's cultural relevance and low fees.
- **Gaming and SocialFi:** Offering scalable infrastructure for on-chain games and decentralized social platforms.

LitVM's competitive advantages include:

- **Hybrid Rollup Architecture:** Combining Arbitrum Nitro's battle-tested optimistic rollup with Succinct's zkVM validity proofs delivers the best of both worlds—fast execution with cryptographic security guarantees.
- **Trustless Bridging:** BitcoinOS's Grail Bridge enables non-custodial LTC transfers using ZK proofs, requiring only one honest validator (1/n security) rather than honest majority consensus.
- **Decentralized Sequencing:** Espresso's shared sequencer distributes block ordering across a permissionless node network, eliminating single points of failure and censorship risks.
- **Phased Settlement Migration:** LitVM's roadmap culminates in full Litecoin-native settlement, making it a true Litecoin L2 while initially leveraging Ethereum's security and liquidity.
- **Community Focus:** Allocating 51% of $LITVM tokens to the community, ecosystem funds, and grants fosters adoption and incentivizes development.
- **Litecoin-Native Assets:** Support for LTC-20 tokens, Runes, and Ordinals (in addition to LTC) enables unique use cases, such as Litecoin-based collectibles and tokenized assets.
- **Official Endorsement:** LitVM is officially endorsed by the Litecoin Foundation, with support from Charlie Lee and David Schwartz.

By positioning Litecoin as a scalable, programmable Web3 hub, LitVM aims to increase LTC's utility, attract global developers, and drive adoption across retail and institutional markets.

---

2. LitVM Overview

2.1 Core Purpose

LitVM is Litecoin's first trustless EVM rollup, designed to unlock the full potential of the Litecoin ecosystem by enabling secure, scalable, and cost-efficient Web3 applications. By leveraging a hybrid rollup architecture that combines optimistic execution with zero-knowledge validity proofs, LitVM processes thousands of transactions off-chain while anchoring their validity to both Litecoin and Ethereum blockchains.

The platform's primary objectives are:

1. **Create More Demand for LTC:** Drive adoption and utility for Litecoin as a base layer asset through yield opportunities, DeFi participation, and expanded use cases.
2. **Unlock Hard Money Web3:** Solve the trustless hard money issue in Web3 for retail, funds, institutions, treasuries, and governments by bringing the principles of hard money to programmable blockchain applications.
3. **Foster a Utility-Driven Future:** Connect Litecoin to the broader Web3 ecosystem, enabling cross-chain interoperability and new application categories.
4. **Enable Yield Generation:** Provide sustainable earning mechanisms for the Litecoin community through DeFi protocols and institutional-grade yield strategies.
5. **Create a Vibrant Ecosystem:** Build a vibrant Litecoin-powered ecosystem with primary focus on yield markets, RWAs, and AI applications.

LitVM addresses Litecoin's historical limitations—such as the lack of native smart contract support—while preserving its strengths as a fast, low-cost, and widely adopted payment network. By creating a scalable environment for decentralized applications and infrastructure, LitVM positions Litecoin as a central hub in the Web3 ecosystem, complementing Bitcoin's role as a secure settlement layer and Ethereum's programmable infrastructure.

2.2 Target Audience

LitVM is engineered to serve a diverse set of stakeholders, each with unique needs and opportunities within the Litecoin and broader crypto ecosystems.

For Litecoin Holders:

- Access yield opportunities without giving up custody of LTC
- Participate in DeFi protocols using trustlessly bridged Litecoin
- Engage with Litecoin-native assets (LTC, Ordinals, Runes, LTC-20s) in a programmable environment

For Developers:

- Unlock a large and active target market of Litecoin holders
- Deploy EVM-compatible smart contracts using familiar tools (Solidity, Hardhat, Foundry)
- Build on Litecoin's 14+ years of proof-of-work security
- Leverage ZK technology for scalable, low-cost applications

For Enterprises:

- Tokenize real-world assets with L1-secured infrastructure
- Access institutional-grade yield strategies
- Build compliant, scalable blockchain solutions

For the Broader Crypto Ecosystem:

- Ethereum developers and users benefit from LitVM's new market and ability to integrate Ethereum-based assets with LitVM's low-cost environment
- Bitcoin maximalists and developers align with LitVM's trustless, decentralized design, which respects Bitcoin's principles while extending functionality via Litecoin

2.3 Interoperability Goals

LitVM is architected to bridge Litecoin with Ethereum while aligning philosophically with Bitcoin's principles, creating a unified and decentralized Web3 ecosystem. Its interoperability goals are underpinned by advanced bridging mechanisms, modular infrastructure, and strategic ecosystem partnerships.

Seamless Asset Transfers:

- LitVM employs trustless bridging via BitcoinOS's Grail Bridge, enabling user-driven asset transfers from Litecoin using ZK proofs without centralized intermediaries
- The Arbitrum Bridge enables seamless transfers of ETH and ERC-20 tokens from Ethereum
- LTC and other Litecoin-native assets can be used in EVM protocols and dApps, while Ethereum-based assets can operate within LitVM's low-cost environment

Support for Cross-Chain dApps:

- LitVM's EVM compatibility allows developers to build dApps that interact with assets and data from both Litecoin and Ethereum ecosystems
- Oracles and SDKs provide access to multi-chain data, enabling dApps like cross-chain DeFi platforms, RWA marketplaces, or AI-integrated applications

Alignment with Bitcoin's Principles:

- LitVM respects Bitcoin's focus on decentralization and immutability, avoiding reliance on centralized bridges or custodians
- Its ZK-based architecture ensures trust-minimized interactions, appealing to Bitcoin's security-conscious community
- By enabling programmable Bitcoin (trustlessly bridged BTC via BitcoinOS infrastructure), LitVM allows BTC to participate in Litecoin-based DeFi and application ecosystems without altering Bitcoin's (or Litecoin's) L1

---

3. Technical Architecture

LitVM's technical architecture is designed to deliver a scalable, secure, and interoperable Layer-2 solution for Litecoin, leveraging a hybrid rollup architecture that combines the best of optimistic and zero-knowledge rollup technologies. By integrating BitcoinOS for trustless Litecoin bridging, Arbitrum Nitro for EVM-compatible execution, Succinct's zkVM for validity proofs, and Espresso for decentralized sequencing, LitVM creates a robust platform that supports Litecoin-native assets and enables cross-chain dApps.

3.1 Hybrid Rollup Architecture

LitVM is built as a hybrid rollup that combines the advantages of both optimistic and zero-knowledge rollup architectures:

Optimistic Execution (Arbitrum Nitro):

- Transactions are executed optimistically for fast processing
- Arbitrum's fraud proof mechanism provides security guarantees
- Users experience immediate transaction confirmations

Zero-Knowledge Validity Proofs (Succinct SP1 zkVM):

- Validity proofs are generated for all chain execution
- Proofs provide cryptographic guarantees of execution correctness
- Fast finality in minutes rather than the 7-day challenge period of pure optimistic rollups

This hybrid approach delivers:

- **Scalability:** Thousands of transactions per second with sub-cent fees
- **Security:** Mathematical guarantees through ZK proofs plus fraud-proof fallback
- **Speed:** Immediate optimistic confirmations with rapid ZK-verified finality
- **Cost Efficiency:** Proof costs as low as $0.01-0.02 per transaction

3.2 BitcoinOS Integration

BitcoinOS (BOS) is a smart contract operating system originally developed for Bitcoin, and adapted for Litecoin to enable trustless bridging and programmability. Successfully demonstrated on Bitcoin in July 2024 (block 853626), BOS leverages advanced ZK cryptography to execute complex computations off-chain while anchoring results to the L1.

Core BitcoinOS Components:

BitSNARK Verification: BitSNARK is the ZK verification protocol at the core of BitcoinOS, enabling verification of zero-knowledge proofs directly on UTXO blockchains:

- Small proof size of approximately 300 bytes
- Up to 40 bridge transactions per block
- No protocol changes required on Litecoin
- Fraud-proof security with deterministic challenges
- 1/n security model—only one honest verifier needed

Grail Bridge: The Grail Bridge enables trustless LTC movement between Litecoin mainchain and LitVM:

Deposit Flow:

1. User locks LTC in a Taproot address on Litecoin mainchain
2. BitcoinOS generates a ZK-SNARK proof verifying the locked funds
3. zkLTC is minted on LitVM at 1:1 ratio

Withdrawal Flow:

1. User burns zkLTC on LitVM
2. Proof is verified on Litecoin mainchain
3. LTC is released from the locked address

Security Properties:

- **Non-Custodial:** No third party ever holds user funds
- **1/n Security:** Only one honest validator needed for security
- **ZK Verification:** Proofs are mathematically verifiable
- **No Protocol Changes:** Works with existing Litecoin infrastructure

Litecoin-Specific Optimizations:

- Faster 2.5-minute block times enable quicker deposit confirmations
- Scrypt-based consensus provides broad, decentralized mining ecosystem
- MWEB integration planned for optional privacy features

Figure 1: *Litecoin-LitVM bridge architecture*

3.3 Arbitrum Orbit and Nitro

LitVM is built as an Arbitrum Orbit chain using the Nitro tech stack. Arbitrum Orbit enables permissionless deployment of customizable chains with:

- **EVM Equivalence:** Full compatibility with Ethereum smart contracts, tooling, and developer experience
- **Fraud Proofs:** Interactive fraud proof mechanism for transaction validity
- **Advanced Compression:** Efficient data batching for lower costs
- **Custom Gas Token:** zkLTC as the native gas token instead of ETH

Why Arbitrum Orbit:

- Battle-tested technology powering billions in TVL
- Active ecosystem of developers and tooling
- Continuous upgrades from Offchain Labs
- Flexibility to customize gas tokens, governance, and more

Nitro Architecture: Arbitrum Nitro provides the core execution environment:

- High-performance EVM-compatible execution
- Efficient state management
- Optimized transaction batching
- Seamless integration with Ethereum tooling

3.4 Succinct zkVM

LitVM enhances the Arbitrum Nitro rollup with Succinct's SP1 zkVM to generate validity proofs for all chain execution, creating a hybrid rollup architecture:

- **SP1 zkVM:** General-purpose zero-knowledge virtual machine that can prove execution of any Rust program
- **Validity Proofs:** Cryptographic proofs that verify correct state transitions
- **Fast Finality:** Proofs can be verified in minutes rather than the 7-day challenge period of pure optimistic rollups
- **Cost Efficiency:** Proof costs as low as $0.01-0.02 per transaction

This hybrid approach combines:

- The immediate execution speed of optimistic rollups
- The cryptographic security guarantees of ZK rollups

3.5 Espresso Shared Sequencer

LitVM utilizes Espresso's shared sequencer for decentralized block ordering:

- **Decentralized Sequencing:** Block proposals distributed across a permissionless node network
- **Censorship Resistance:** No single entity controls transaction ordering
- **Cross-Chain Composability:** Shared sequencing enables atomic operations across chains
- **Network Security:** Multiple independent sequencers provide redundancy

Unlike most rollups that rely on centrally operated sequencers, Espresso distributes sequencing across a geographically diverse set of professional and community-run nodes, eliminating single points of failure and censorship risks.

3.6 Dual Bridge Architecture

LitVM features two bridging systems to connect both the Litecoin and Ethereum ecosystems:

BitcoinOS Grail Bridge (Litecoin ↔ LitVM):

Feature	Description
Source Chain	Litecoin
Asset Type	LTC → zkLTC
Trust Model	ZK proofs (1/n honest verifier)
Custodian	None (non-custodial)
Primary Use	Onboard Litecoin users

Arbitrum Bridge (Ethereum ↔ LitVM):

Feature	Description
Source Chain	Ethereum / EVM
Asset Type	ETH, ERC-20s
Trust Model	Optimistic + ZK hybrid

Custodian	Bridge contracts
Primary Use	Onboard Ethereum users

The Arbitrum Bridge supports:

- ETH
- USDC, USDT, and other stablecoins
- ERC-20 tokens
- Other Ethereum-native assets

This dual-bridge architecture provides LitVM with access to both Litecoin's user base and Ethereum's deep liquidity.

3.7 EVM Compatibility

LitVM's full compatibility with the Ethereum Virtual Machine (EVM) ensures a seamless development experience:

Familiar Development Environment:

- Write smart contracts in Solidity, Vyper, or other EVM-compatible languages
- Use established tools: Hardhat, Foundry, Remix, Truffle
- Interact via Ethers.js, Web3.js, and standard libraries
- Connect with MetaMask, Rabby, and other EVM wallets

Portability:

- Existing EVM-native dApps can be deployed on LitVM with minimal modifications
- Standard token standards supported: ERC-20, ERC-721, ERC-1155

Ecosystem Integration:

- Full interoperability with Ethereum-based protocols, oracles, and DeFi platforms
- Access to Ethereum's vast developer ecosystem and tooling

3.8 Phased Mainnet Rollout

LitVM's mainnet will be deployed in three phases, progressively migrating settlement from Ethereum to Litecoin:

Phase 1: Ethereum Settlement + Dual Bridges

- Fully operational Arbitrum Orbit rollup settling on Ethereum
- Nitro's optimistic architecture with Succinct zkVM validity proofs
- BitcoinOS Grail Bridge deployed for trustless LTC bridging
- Arbitrum Bridge available for ETH and ERC-20 assets
- Espresso shared sequencer for decentralized block ordering
- zkLTC as gas token and primary base asset

Phase 2: Litecoin Proof Anchoring

- All finalized chain batches anchored to Litecoin blockchain
- Validity proofs inscribed using standard extended transactions
- No Litecoin protocol changes required
- Creates tamper-resistant audit trail secured by Litecoin's PoW
- Independent verification possible via Litecoin nodes

Phase 3: Litecoin Native Settlement

- Migration of settlement from Ethereum to Litecoin
- LitVM becomes a fully native Litecoin rollup
- Litecoin as the canonical settlement and finality layer
- Complete sovereignty under Litecoin's 14+ years of PoW security

This phased approach ensures:

- Immediate security guarantees via Ethereum in Phase 1
- Progressive decentralization toward Litecoin
- Uninterrupted operation throughout migration
- Preserved EVM compatibility and zkVM security

3.9 Asset Support

LitVM supports a diverse array of assets, catering to both the Litecoin and Ethereum ecosystems:

Litecoin-Native Assets:

Asset Type	Description	Status
LTC	Native Litecoin (as zkLTC)	✅ Supported
Ordinals	NFT-like inscriptions	🔜 Planned
Runes	Fungible token protocol	🔜 Planned
LTC-20	Token standard	🔜 Planned
Charms	BitcoinOS native tokens	🔜 Planned

Ethereum-Native Assets:

- ETH
- USDC, USDT, and other stablecoins
- ERC-20 tokens
- ERC-721 NFTs
- ERC-1155 multi-tokens

Native BTC (Planned): LitVM plans to support native BTC, bridged from Bitcoin's L1 using BitcoinOS's Grail Bridge. BTC on LitVM will enable Bitcoin users to participate in Litecoin-based DeFi, RWA, and broader dApp ecosystems without altering Bitcoin's L1 or relying on centralized custodians.

3.10 Scalability and Performance

LitVM is engineered for high scalability and performance:

Metric	LitVM	Litecoin L1	Ethereum L1
Throughput	Thousands TPS	~56 TPS	~15 TPS
Transaction Fees	Sub-cent	Sub-cent	$1-$100
Finality	Minutes (ZK)	2.5 min	12+ min

Key Optimizations:

- **Recursive zkSNARKs:** Enable proof aggregation across multiple batches
- **Efficient Batching:** Up to 10,000 transactions per rollup block
- **Parallel Proof Generation:** Minimizes bottlenecks for high-throughput dApps
- **Data Compression:** Optimized for L1 data requirements

3.11 Security Guarantees

LitVM inherits security from multiple layers:

1. **Litecoin Mainchain:** 14+ years of uninterrupted PoW security with hashrate comfortably exceeding 2 PH/s
2. **Ethereum Settlement (Phase 1):** World's most decentralized smart contract platform
3. **ZK Proofs:** Mathematical guarantees of execution correctness via Succinct SP1
4. **Espresso Sequencing:** Decentralized block production prevents censorship
5. **BitcoinOS Grail:** Non-custodial bridging with 1/n security
6. **Arbitrum Bridge:** Battle-tested rollup bridge infrastructure

Additional Safeguards:

- **Audited Contracts:** Smart contracts, bridges, and ZK circuits undergo rigorous third-party audits
- **Bug Bounties:** Incentive programs for white-hat security researchers
- **Fail-Safe Mechanisms:** Forced inclusion via L1 ensures liveness; emergency withdrawal protocols protect user funds

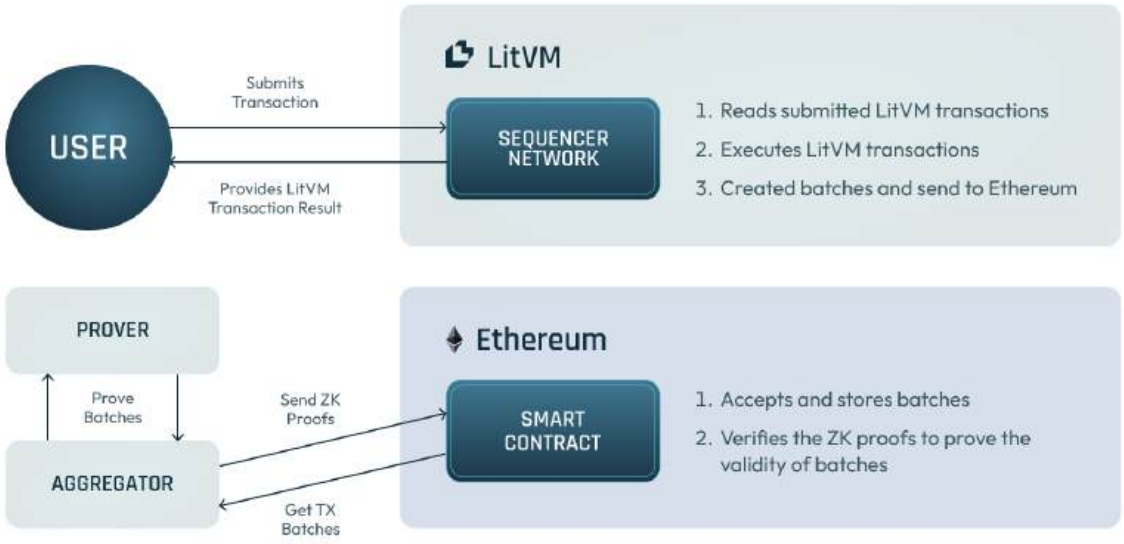


Figure 2: *Ethereum-side transaction processing & finalization*

---

4. Tokenomics

LitVM operates with a dual-token model designed to align incentives across the ecosystem while maintaining the principles of hard money.

4.1 Dual-Token Model

Token	Primary Function	Backing	Supply
zkLTC	Gas & Base Asset	1:1 with LTC	Elastic (based on bridged LTC)
$LITVM	Governance & Utility	Protocol value	Fixed

Benefits of Separation:

1. **Hard Money Preservation:** Gas fees paid in LTC-backed asset maintains Litecoin's monetary properties
2. **Clear Incentives:** Governance token aligns long-term stakeholders

3. **Sustainable Economics:** Revenue sharing creates value beyond speculation
4. **Flexible Tokenomics:** Each token optimized for its specific role

4.2 zkLTC: The Gas Token

zkLTC is a fully-collateralized representation of Litecoin (LTC) on LitVM, serving as the native gas token for all transactions and the primary base asset for DeFi protocols.

Key Properties:

Property	Description
1:1 Backing	Every zkLTC backed by LTC locked on Litecoin mainchain
Trustless	Bridging uses ZK proofs—no custodians or multisig
Gas Token	Used to pay transaction fees on LitVM
Base Asset	Primary liquidity pair for DeFi protocols
Redeemable	Can always be bridged back to native LTC

zkLTC Use Cases:

- Transaction fees (gas)
- DeFi collateral
- Trading pair base asset
- Yield strategies
- Cross-chain transfers

Why zkLTC Instead of Wrapped LTC?

Aspect	Wrapped LTC (Traditional)	zkLTC (BitcoinOS)

Custody	Third-party custodian	Non-custodial
Trust	Trust the custodian	Trust math (ZK proofs)
Verification	Off-chain attestation	On-chain proof
Counterparty Risk	High	Minimal
Redemption	Depends on custodian	Guaranteed via protocol

4.3 LITVM: Governance and Utility Token

LITVM is the native governance and utility token of the LitVM ecosystem, designed to coordinate activity between the economic, governance, and strategic layers of the network.

Token Utility:

1. Governance LITVM powers the Litecoin DAO, giving token holders rights to:

- Vote on protocol parameters and upgrades
- Propose and approve ecosystem grants
- Participate in strategic funding decisions
- Shape the future direction of LitVM

2. Revenue Sharing LitVM is one of the few Layer-2 platforms explicitly designed to share protocol revenue with its community:

- Sequencers order and batch transactions on LitVM
- A percentage of sequencer fees flows to LITVM holders and/or stakers
- Unlike chains where fees go entirely to operators, LitVM distributes value back

3. Ecosystem Access

- Priority access to new protocol launches
- Participation in Litecoin DAO initiatives
- Eligibility for ecosystem incentive programs

4.4 Revenue Model

LitVM's revenue model creates sustainable value through protocol fees:

- **Sequencer Fees:** Transaction ordering and batching generates recurring revenue
- **Institutional Yield Infrastructure:** Institutional-grade strategy vaults (e.g. DNA Fund) charge management and performance fees, with portions redirected to LITVM holders/stakers
- **Protocol Fees:** Various ecosystem activities generate fees distributed to stakeholders

This model transforms core infrastructure usage into tangible, recurring revenue that flows directly to community members—not relying on inflationary rewards or speculation.

4.5 Community Allocation

51% Community Allocation: Over half of all tokens are reserved for the community, prioritizing current Litecoin holders and welcoming new ecosystem participants.

Community allocation includes:

- Grants fund for innovative projects
- Usage incentives for Litecoin users
- Staking and liquidity incentives
- Governance rewards for active participation
- Dedicated Ordinals/Runes fund

---

5. Governance

5.1 The Litecoin DAO

LitVM's governance model has been designed to ensure decentralized, democratic decision-making processes tailored to the Litecoin community's founding principles. The $LITVM token serves as the vehicle for participation, incentive modeling, and stewardship.

Governance Rights:

- Vote on protocol parameters and upgrades
- Propose ecosystem initiatives

- Approve grant allocations
- Participate in strategic decisions

Governance Incentives: Active participants who vote, propose, and engage in community dialogue are eligible for rewards, encouraging ongoing engagement.

5.2 Treasury Board

LitVM's governance is anchored by the LitVM Treasury Board, a body tasked with overseeing the allocation of the 51% community token supply reserved for ecosystem development.

Treasury Board Composition (5 Seats):

1. Aztec Amaya (LitVM Co-founder)
2. Roc Zacharias (LitVM Co-founder)
3. David Schwartz (Litecoin Foundation, Director of Partnerships)
4. Community Majority Opinion Seat
5. Additional Member (TBA)

5.3 Proposal Process

LitVM employs an iterative, multi-step approach to ensure thorough vetting and genuine community input:

1. **Initial Proposal:** Community members submit proposals for consideration
2. **Temperature Check:** Token holders vote on whether the proposal merits further development
3. **Detailed Proposal:** Approved proposals return with comprehensive implementation details
4. **Treasury Board Vote:** Final determination on implementation

This governance model is intended to be a living, breathing framework that adapts based on feedback, performance, and emerging opportunities as Web3 technologies advance.

---

6. Use Cases

LitVM combines Litecoin's fast, low-cost transactions with Ethereum's smart contract capabilities, enabling diverse Web3 applications. Its trustless bridges and hybrid rollup

architecture create a versatile platform for developers and users, with primary focus on yield markets, real-world assets, and AI applications.

6.1 Yield Markets (Primary)

LitVM is unlocking a spectrum of on-chain, off-chain, and cross-chain yield opportunities for the Litecoin community.

DeFi Ecosystem:

- High-performance DEXs for decentralized trading
- LTC serving as primary base asset for DEX pairings
- Standard LP and farming incentives

Lending Markets:

- Decentralized lending platforms seeking LTC deposits
- LTC-backed loans with algorithmic rates
- Borrowing against LTC holdings without selling

Institutional-Grade Strategies: In partnership with DNA Fund, LitVM offers innovative yield strategies:

- Estimated 7-11% APR on spot LTC holdings
- Yields accumulated in LTC
- Available to both retail and institutional investors
- Actively managed products for high-net-worth individuals and funds

Staking and Governance Rewards:

- Potential $LITVM staking for governance participation
- Additional rewards for active involvement
- Protocol airdrops to LTC and $LITVM stakers/holders

6.2 Real-World Assets (Primary)

LitVM's technical architecture uniquely positions it as a prime hub for tokenized RWAs:

L1-Secured Infrastructure:

- BitcoinOS infrastructure enables creation of L1-secured RWAs

- Programmable timelocks for enhanced asset security
- Smart contracts managing fractional ownership

Supported Asset Types:

- **Commodities:** Silver, gold, and other precious metals with audited reserves
- **Real Estate:** Tokenized property with fractional shares
- **Financial Instruments:** Programmable bonds and structured products
- **Consumer-Driven:** Physical collectibles, royalties etc.

Key Benefits:

- Democratized investment access
- DeFi-ready infrastructure
- Cross-chain market access
- Institutional and retail appeal

6.3 AI Ecosystem (Primary)

LitVM positions Litecoin at the intersection of hard money and artificial intelligence:

Litecoin-Powered AI Agents:

- Autonomous agents operating with LTC
- AI-driven trading and portfolio management
- Automated DeFi strategies

AI-Enhanced Web3 Applications:

- User-friendly interfaces powered by AI
- Intelligent dApp interactions
- Simplified Web3 onboarding

Future-Proofing:

- Infrastructure ready for AI evolution
- DeFi AI agents for automated strategies
- Integration with emerging AI technologies

6.4 Advanced Payments Infrastructure

Building on Litecoin's payment heritage:

- **Programmable Payments:** Smart contract-enabled payment rails
- **Stablecoin Support:** Integration with major stablecoins (USDC, USDT)
- **Cross-Border Payments:** Low-cost international transfers
- **Merchant Solutions:** Enterprise-grade payment infrastructure

6.5 NFTs and Litecoin Ordinals

LitVM integrates Litecoin's Ordinals with EVM smart contracts:

NFT Infrastructure:

- Marketplaces for trading Litecoin Ordinals
- EVM contracts managing ownership and royalties
- Cross-chain NFT listings

Digital Collectibles:

- Art and collectibles minted as Ordinals on Litecoin mainchain
- Ported to LitVM for programmable features
- Fractional ownership capabilities

Creator Economy:

- Royalty management via smart contracts
- Creator tools and platforms
- Community-driven collections

6.6 Gaming and Metaverse

LitVM's high throughput and low fees support blockchain gaming:

Play-to-Earn:

- Rewards in LTC or LTC-20 tokens
- Low-latency transactions via zkRollups
- Transparent game mechanics

Metaverse Economies:

- Digital assets (land, items) as Ordinals or NFTs
- Smart contract ownership management
- 3D integration capabilities

Gaming Infrastructure:

- On-chain randomness for fair mechanics
- Scalable infrastructure for high-frequency interactions
- Cross-chain gaming assets

6.7 Decentralized Identity and Governance

Decentralized Identity (DID):

- Verifiable credentials stored on-chain
- Zero-knowledge proofs for privacy
- Interoperability with Ethereum DIDs

On-Chain Governance:

- LTC-20 or $LITVM tokens for voting
- Low fees encouraging participation
- Transparent, community-driven decision-making

---

7. Developer Onboarding

To propel the Litecoin ecosystem to the forefront of Web3, cultivating a thriving developer community is essential. As an EVM-compatible chain, LitVM leverages the extensive Ethereum ecosystem, enabling seamless migration for developers from Ethereum and other EVM-based platforms.

EVM Compatibility: A Seamless Transition

Established Tooling:

- **Solidity:** Standard smart contract language with OpenZeppelin libraries
- **Hardhat/Foundry:** Frameworks for testing, deploying, and debugging
- **Ethers.js/Web3.js:** Libraries for blockchain and wallet interactions

- **Remix/Truffle:** IDEs for rapid prototyping

Code Portability:

- Ethereum smart contracts deploy on LitVM with minimal changes
- Standard ERC token standards fully supported

Wallet Support:

- MetaMask, Rabby, Coinbase Wallet, Trust Wallet
- Any WalletConnect-compatible wallet

Developer Resources

Documentation:

- Comprehensive guides for setting up LitVM environments
- Tutorials for deploying via Hardhat or Foundry
- Integration guides for Grail Bridge and cross-chain features

Templates and Examples:

- Pre-built contract templates for common use cases
- Step-by-step guides for DeFi, NFT, and governance dApps
- Open-source audited contracts optimized for LitVM

SDK and APIs:

- Access to Litecoin state and cross-chain features
- Bridge integration libraries
- Oracle integrations

Community Building and Incentives

Hackathons:

- Regular events with prizes and token rewards
- Focus on Litecoin-based DeFi, RWAs, and AI applications

Grants Program:

- Funding for high-impact dApps

- Priority for yield infrastructure, RWA platforms, and AI applications

Ambassador Program:

- Rewards for tutorials, workshops, and mentoring
- Community recognition and support

Bug Bounties:

- Incentives for identifying vulnerabilities
- Security-focused community engagement

Deployment Guides

LitVM supports multiple deployment methods:

Foundry:

bash

```
Shell
forge create --rpc-url $LITVM_RPC_URL \
  --private-key $PRIVATE_KEY \
  src/Contract.sol:Contract
```

Hardhat:

bash

```
Shell
npx hardhat run scripts/deploy.js --network litvm_testnet
```

Remix:

- Browser-based deployment via Injected Provider
- Connect MetaMask to LitVM network

8. Ecosystem Benefits

8.1 For the Litecoin Community

Access to Web3: LitVM bridges the gap between Litecoin's payment focus and modern Web3 capabilities:

- Trade LTC on DEXs and participate in DeFi
- Access yield opportunities without giving up custody
- Engage with Litecoin Ordinals in programmable environments
- Participate in RWA markets and AI applications

Cost Efficiency:

- Sub-cent transaction fees
- Accessible DeFi for retail users
- Economical NFT trading and gaming

Community Growth:

- Attracts developers building on LitVM
- New users from DeFi, NFT, and gaming sectors
- Community-driven governance empowers participation

8.2 For EVM Developers

New Market Access:

- Millions of Litecoin users as potential dApp users
- Deploy existing contracts with minimal modification
- Fresh market beyond competitive Ethereum L2 landscape

Cross-Chain Opportunities:

- Build dApps spanning Litecoin and Ethereum
- Access Litecoin's payment capabilities
- Create novel cross-chain applications

Scalability:

- Thousands of TPS at sub-cent costs
- Fast finality for time-sensitive applications
- Familiar tools and development experience

8.3 For Bitcoin and the Broader Crypto Ecosystem

Philosophical Alignment:

- Trust-minimized, decentralized design
- No centralized sequencers or custodial bridges
- Respects Bitcoin's core principles

Interoperability:

- Bridges Litecoin with Ethereum ecosystem
- Future BTC integration via BitcoinOS
- Reduces ecosystem fragmentation

Innovation Hub:

- Testing ground for cross-chain collaboration
- Novel applications spanning multiple ecosystems
- Potential inspiration for Bitcoin L2 solutions

---

9. Strategic Partners

LitVM is built through collaboration with leading blockchain infrastructure providers:

Litecoin Foundation

The non-profit organization dedicated to advancing Litecoin adoption and development. LitVM is officially endorsed by the Litecoin Foundation.

- Official endorsement and community alignment
- Ecosystem collaboration
- Governance participation via David Schwartz

BitcoinOS

The operating system bringing programmability to UTXO blockchains. First to verify a ZK proof on Bitcoin mainnet (July 2024, block 853626).

- Grail Bridge trustless bridging infrastructure
- BitSNARK ZK verification protocol
- Cross-chain interoperability capabilities
- zkLTC minting and redemption

Arbitrum (Offchain Labs)

Provides the core rollup technology powering LitVM.

- Arbitrum Nitro execution layer
- EVM equivalence and smart contract support
- Interactive fraud proof mechanism
- Battle-tested security (billions in TVL)

Caldera

Leading infrastructure provider for deploying and managing Arbitrum Orbit chains.

- Chain deployment and management
- RPC infrastructure
- Network monitoring and reliability

Succinct

Develops SP1, a general-purpose zero-knowledge virtual machine.

- SP1 zkVM integration
- Validity proof generation
- Fast finality capabilities
- Cost-efficient proving

Espresso Systems

Provides shared sequencer infrastructure for decentralized transaction ordering.

- Shared sequencer mechanism
- Decentralized block ordering
- Cross-chain composability
- Censorship resistance

Lunar Digital Assets

The venture studio incubating LitVM.

- Full-stack blockchain venture studio
- Marketing and community building
- Strategic partnerships
- Ecosystem development

---

10. Roadmap

Timeline Overview

Milestone	Target
Testnet Launch	Q1 2026
Token Generation Event (TGE)	Following Testnet
Mainnet Activation	Post-TGE

Phased Rollout

Phase 1: Testnet and Initial Launch

- Deploy fully operational Arbitrum Orbit rollup
- Launch BitcoinOS Grail Bridge for trustless LTC bridging
- Enable Arbitrum Bridge for ETH/ERC-20 assets
- Activate Espresso shared sequencer

- Establish zkLTC as gas token

Phase 2: Litecoin Proof Anchoring

- Anchor finalized chain batches to Litecoin blockchain
- Inscribe validity proofs to Litecoin
- Create independent verification via Litecoin nodes

Phase 3: Litecoin Native Settlement

- Migrate settlement from Ethereum to Litecoin
- Establish Litecoin as canonical settlement layer
- Complete sovereignty under Litecoin's PoW security

Ecosystem Development

- Launch yield market infrastructure
- Deploy RWA tokenization platforms
- Integrate AI application frameworks
- Expand Ordinals/Runes support
- Grow developer ecosystem via grants and hackathons

---

11. Conclusion

LitVM represents a pivotal evolution for Litecoin, redefining its role as a scalable, programmable, and interoperable hub in the modern Web3 era. By harnessing a hybrid rollup architecture that combines Arbitrum Nitro's battle-tested execution with Succinct's zkVM validity proofs, LitVM overcomes Litecoin's historical L1 limitations, enabling a vibrant ecosystem of yield markets, real-world assets, AI applications, and diverse Web3 use cases.

Its EVM compatibility empowers developers to build sophisticated dApps using familiar tools, seamlessly connecting Litecoin with the Ethereum ecosystem. LitVM's phased settlement model begins with Ethereum's security guarantees while progressively migrating to full Litecoin-native settlement, ensuring unparalleled security, flexibility, and sovereignty. Advanced technologies—including BitcoinOS's trustless Grail Bridge, Espresso's decentralized sequencing, and Succinct's cost-efficient proving—underpin LitVM's

high-throughput architecture, capable of processing thousands of transactions per second at sub-cent fees.

LitVM's vision extends beyond technical innovation to foster a cohesive and inclusive crypto ecosystem. By bridging Litecoin with Ethereum, aligning philosophically with Bitcoin's decentralized ethos, and providing trustless infrastructure for hard money, LitVM reduces friction between blockchain communities and promotes collaboration. Its support for Litecoin-native assets and cross-chain capabilities unlocks novel use cases—from institutional-grade yield strategies to tokenized real estate and AI-powered applications—driving demand for LTC and expanding its utility.

Central to LitVM's mission is its commitment to community-driven growth. By allocating 51% of its token supply to the Litecoin community, ecosystem funds, and developer grants, LitVM incentivizes adoption and innovation. The governance model, anchored by the Treasury Board and Litecoin DAO, ensures democratic participation in the platform's evolution. A comprehensive developer ecosystem—featuring familiar EVM tooling, open-source contracts, and robust documentation—empowers global developers to build on LitVM.

As the Web3 market surges toward a projected $99.75 billion by 2034, LitVM positions Litecoin to capture significant market share in high-growth sectors like yield markets, RWAs, and AI. By cementing Litecoin as "Hard Money Web3"—the silver that complements Bitcoin's gold in the modern Web3 landscape—LitVM not only extends Litecoin's utility but creates a unified platform bridging retail, institutional, and developer communities.

The success of LitVM will amplify Litecoin's relevance, drive LTC adoption, and inspire further innovation across the crypto landscape, paving the way for a decentralized, inclusive, and interconnected future built on the principles of hard money.

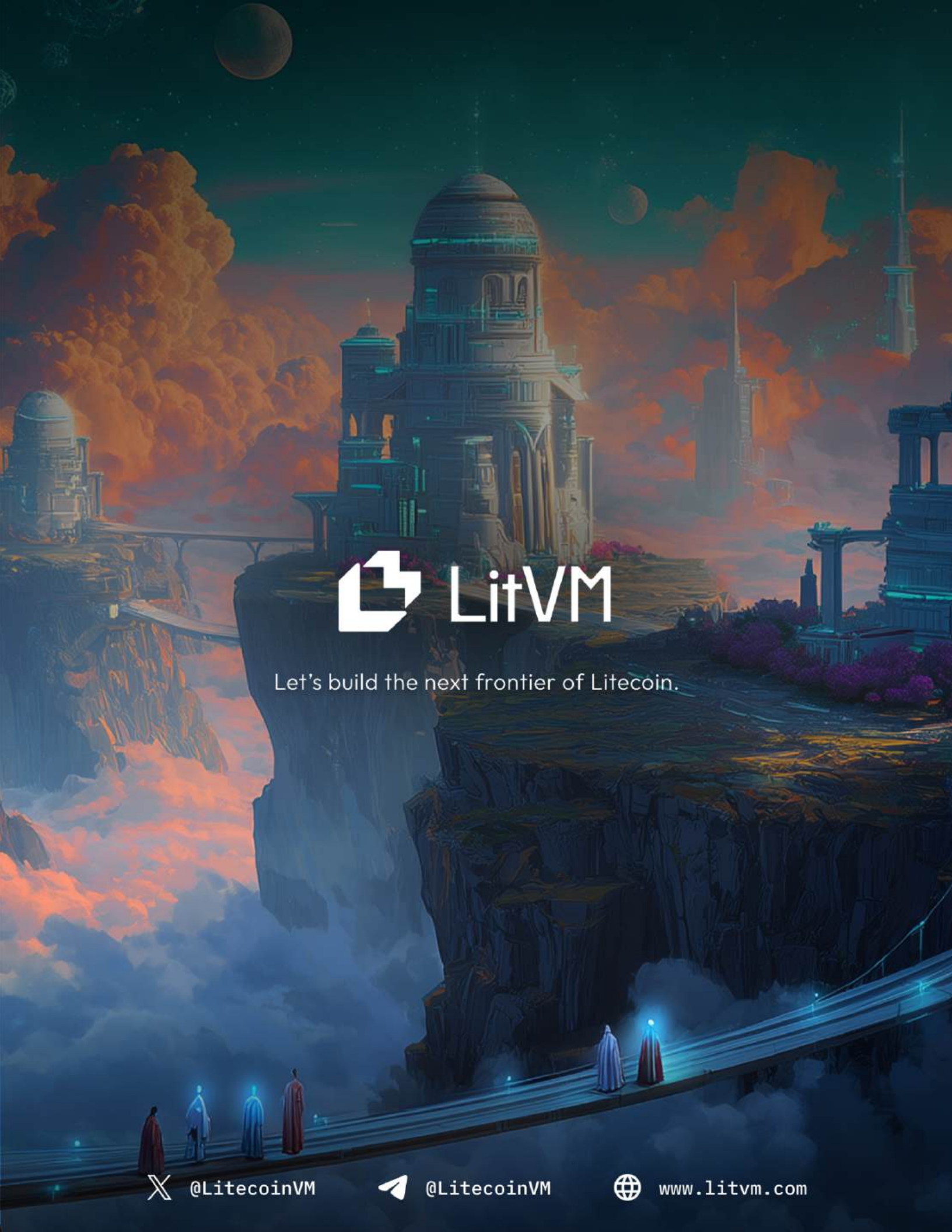
References

1. BitcoinOS Documentation: https://docs.bitcoinos.build/
2. Arbitrum Documentation: https://docs.arbitrum.io/
3. Succinct Documentation: https://docs.succinct.xyz/
4. Espresso Systems: https://docs.espressosys.com/
5. Litecoin Documentation: https://litecoin.info/
6. Precedence Research - Web 3.0 Market: https://www.precedenceresearch.com/web-3-0-market
7. LitVM Documentation: https://docs.litvm.com/
8. LitVM Official: https://litvm.com/

LitVM is Litecoin's Virtual Machine, enabling smart contract capabilities and Web3 applications for Litecoin. Officially endorsed by the Litecoin Foundation, LitVM is committed to fostering a 'Hard Money Web3' ecosystem, including Litecoin yield opportunities, real-world assets, AI and more.

Official Channels:

- Website: https://litvm.com
- Twitter: @LitecoinVM
- Telegram: t.me/litecoinvm


LitVM
Let's build the next frontier of Litecoin.
@LitecoinVM
@LitecoinVM
www.litvm.com