IBVM

Technical White Paper

A Bitcoin-Native Layer-2 Architecture

Version 3.0 | October 2025

Copyright © 2025 IBVM IP LLC. All Rights Reserved.

- **Intellectual Property Notice**: All intellectual property, patents, trademarks, and copyrights related to the IBVM protocol and technology are owned by IBVM IP LLC, a Delaware registered limited liability company. IBVM IP LLC grants perpetual licenses to:
  - IBVM Inc. as the operating entity of the IBVM technology
  - IBVM Foundation Inc. for governance of the IBVM network

IBVM™ is a trademark of IBVM IP LLC.

Abstract

IBVM is the first and only Bitcoin Layer-2 architected for institutional, government, and enterprise adoption—while maintaining full support for permissionless DeFi applications.

International Bitcoin Virtual Machine (IBVM) is a next-generation Layer-2 scaling solution built on Bitcoin, combining zero-knowledge rollups, UTXO parallelization, and a Bitcoin-adapted virtual machine. By anchoring to Bitcoin's immutable Proof-of-Work base layer, IBVM enables fast, low-cost smart contracts and decentralized applications on Bitcoin without custodians or trusted intermediaries.

This technical paper presents IBVM's architecture, demonstrating how the platform achieves 10,000+ TPS with ~1-second finality while maintaining full verifiability on Bitcoin Layer-1. IBVM's innovative 3-tier privacy model with enterprise-grade compliance integration provides: **full zero-knowledge privacy for DeFi, complete transparency for government applications, and selective disclosure for regulated financial institutions**—making it the only Bitcoin infrastructure suitable for Central Bank Digital Currencies (CBDCs), institutional finance, public sector operations, and permissionless applications simultaneously.

IBVM compresses millions of Layer-2 transactions into succinct cryptographic proofs periodically anchored in Bitcoin blocks, massively increasing **throughput while preserving Bitcoin's security and decentralization. Through its 3-tier privacy architecture, IBVM provides complete transaction transparency for government and institutional accountability, selective disclosure for regulated enterprises, and full privacy for permissionless applications—all on the same infrastructure. The platform transforms Bitcoin from "digital gold" into a high-performance, compliance-ready platform for government infrastructure,** institutional applications, and decentralized finance—all secured by Bitcoin's unparalleled network integrity.

Introduction

1.1 Bitcoin's Promise and Limitations: Bitcoin is the world's most secure and decentralized blockchain, but this robustness comes with trade-offs. Bitcoin's base layer handles only ~7-10 transactions per second and supports a simple scripting system without general smart contracts. These limitations have led to Bitcoin being seen as a "boring" blockchain technologically—primarily used as a store of value—while other networks like Ethereum have advanced with Layer-2 scalability and rich decentralized applications.

For Bitcoin to evolve into the foundation of a truly programmable financial system, innovative Layer-2 solutions are essential.

1.2 Existing Layer-2 Solutions and Gaps : Several approaches have emerged to extend Bitcoin's capabilities, each with shortcomings:

- **Lightning Network:** Enables instant Bitcoin payments via off-chain channels, but lacks general programmability and requires complex channel management.
- **Sidechains (e.g., Liquid, RSK):** Introduce smart contracts on Bitcoin-pegged chains but rely on federations or new consensus mechanisms, often requiring "wrapped BTC" and trust in custodians.
- **Recent Proposals:** Projects like Stacks use separate tokens and novel consensus (Proof-of-Transfer), while concepts like BitVM and Spider chain explore rollup or drivechain ideas.

Critical Gap: No solution has combined high throughput, trustless Bitcoin anchoring, and Turing-complete programmability in one package without significant compromises.

1.3 IBVM's Vision : International Bitcoin Virtual Machine (IBVM) fills this gap as the first Bitcoin-native Layer-2 that leverages zero-knowledge (ZK) rollup technology on Bitcoin, enabling full smart contract functionality secured by the Bitcoin mainnet.

Operating as a hybrid zk-Rollup and UTXO-based architecture, IBVM compresses large batches of Layer-2 transactions into succinct proofs (validity proofs) periodically posted to Bitcoin's blockchain. This approach retains Bitcoin's security and finality while vastly expanding throughput and functionality.

Crucially: IBVM requires no changes to Bitcoin's consensus rules and avoids centralized custodians. All funds remain as real BTC, and withdrawals settle directly on Bitcoin L1. Users gain the speed and capability of a modern smart contract platform without sacrificing Bitcoin's trust model.

1.4 Key Technical Achievements

Government & Institutional-Grade Infrastructure - A Bitcoin First
IBVM is the only Bitcoin Layer-2 architected from the ground up for institutional, government, and enterprise adoption while maintaining support for permissionless DeFi applications. The 3-tier privacy model serves Central Banks (CBDCs), regulated financial institutions, public sector operations, and privacy-focused DeFi—all on Bitcoin's security foundation.

Massive Scalability : IBVM targets ~10,000 transactions per second on L2 (over 1,000× improvement vs Bitcoin L1) with ~1-second block times, achieved through parallel transaction processing and rollup compression, all while anchoring to Bitcoin for security.

Trustless Two-Way Pe : Using Simplified Payment Verification (SPV) proofs and Bitcoin scripts, IBVM enables a non-custodial bridge for BTC. Users lock native BTC on L1 and receive equivalent representation on IBVM L2—all verified cryptographically without trusting federations or wrapped assets.

Bitcoin's Ethos, Extended : Every design choice in IBVM aligns with Bitcoin's ethos of decentralization, security, and permissionless access. IBVM enhances Bitcoin's capabilities while reinforcing its role as the bedrock of trust.

2. Technical Architecture Overview

IBVM's architecture fuses proven Layer-2 techniques with Bitcoin-specific innovations, purpose-built to achieve high scalability and expressiveness without sacrificing trustlessness.

2.1 Core Architectural Pillars :

1. Bitcoin-Native zk-Rollup A validity rollup using ZK-SNARK/STARK proofs anchored to Bitcoin for scalability and security

2. UTXO Partitioning for Parallel Processing A novel scheme to process transactions concurrently by sharding the UTXO space.

3. SPV-Assisted Bridging Integration of Simplified Payment Verification to enable trust-minimized BTC deposits and withdrawals between L1 and L2.

4. Bitcoin-EVM Virtual Machine A Bitcoin-adapted smart contract VM providing Ethereum-like capabilities on Bitcoin's foundation.

5. Multi-Tier Privacy Layer Flexible privacy model supporting zero-knowledge, transparent, and hybrid transaction modes.

Together, these components allow IBVM to process orders of magnitude more transactions than Bitcoin per second, enable complex contracts and dApps, and still settle every outcome on Bitcoin L1 with cryptographic integrity.

3. Zero-Knowledge Rollup Design

3.1 Fundamental Architecture

At the heart of IBVM is a zero-knowledge rollup protocol built specifically for Bitcoin's UTXO model. In a zk-Rollup, batches of Layer-2 transactions are executed off-chain, and a succinct zk-proof attesting to the validity of each batch is periodically posted on-chain.

IBVM implements this by:

1. **Batch Processing:** Taking thousands of L2 transactions
2. **Proof Generation:** Generating a proof using advanced zero-knowledge proving systems (STARKs or SNARKs) that all transactions followed protocol rules
3. **Bitcoin Anchoring:** Embedding the proof plus an updated state root into the Bitcoin blockchain (via OP_RETURN output or inscription)

Each proof serves as a verifiable checkpoint—anyone can independently verify the zk-proof against the posted state root to confirm that the new L2 state is valid without replaying all L2 transactions.

3.2 Massive Compression

This compression dramatically reduces on-chain footprint and fees. Potentially millions of Layer-2 transactions can be confirmed on Bitcoin with a single proof of only a few hundred bytes.

3.3 Bitcoin-Native Design

Unlike Ethereum-oriented rollups that rely on Ethereum smart contracts or separate validators for finality, IBVM uses Bitcoin itself as both the data availability layer and the final settlement layer.

Key Properties:

- All rollup state commitments and proofs are anchored to Bitcoin's mainnet ledger
- Inherits Bitcoin's Proof-of-Work security
- No wrapped BTC or custodial tokens required
- Value moved into IBVM remains real BTC
- Withdrawals return BTC directly to L1 addresses

Security Model: If L2 operators were ever dishonest, users retain the recourse of Bitcoin L1 to enforce correct outcomes. The integrity of L2 is enforced by mathematics (zk-proofs) and Bitcoin's consensus, not by trust in intermediaries.

3.4 Proof Systems

IBVM leverages state-of-the-art zero-knowledge proof systems:

ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)

- Fast verification on Bitcoin
- Require trusted setup (mitigated through multi-party computation ceremonies)
- Extremely compact proofs (~200-300 bytes)

ZK-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge)

- No trusted setup required
- Quantum-resistant
- Slightly larger proof sizes but still highly efficient
- Post-quantum security properties

The platform can utilize either system or hybrid approaches depending on the specific use case and security requirements.

4. Multi-Tier Privacy Architecture

4.1 Privacy Design Philosophy

IBVM recognizes that different users and applications have different privacy and compliance needs. A DeFi trader may want complete anonymity, while a regulated financial institution requires full auditability. IBVM's multi-tier privacy model accommodates both extremes and everything in between.

4.2 Three-Tier Transaction Model

IBVM offers three distinct privacy levels, allowing users and institutions to select the appropriate compliance and privacy balance for their specific requirements:

Tier 1: Zero-Knowledge Privacy (ZK Mode)

Designed for: Permissionless DeFi, Privacy-Focused Applications

Technical Implementation:

- Full zero-knowledge proofs for transaction amounts and participants
- Only proof of validity is visible on-chain
- Utilizes advanced ZK circuits for amount hiding and identity shielding
- Comparable to Zcash-style shielded transactions

Use Cases:

- Privacy-focused DeFi applications
- Individual users seeking financial privacy
- Cross-border transactions requiring confidentiality
- Applications where regulatory compliance is not required

Properties:

- ✅ Maximum privacy
- ✅ Zero information leakage
- ✅ Fungibility preservation
- ❌ Not suitable for regulated institutions

Tier 2: Full Transparency Mode

Designed for: Government Applications, Public Sector, Regulated Financial Institutions Requiring Full Auditability

Technical Implementation:

- All transaction details publicly visible
- Participant identities disclosed (wallet addresses or KYC-verified identities via zkMe)
- Transaction amounts in clear
- Full audit trail available on-chain

Use Cases:

- **Government applications and public sector procurement**
- **Regulated financial institutions (banks, payment processors)**
- **Central Bank Digital Currency (CBDC) infrastructure**
- **Public sector accounting and transparency requirements**
- Applications requiring complete regulatory compliance

Properties:

- ✅ Complete compliance with regulatory requirements
- ✅ Full audit capability for regulators and authorities
- ✅ Institutional-grade transparency
- ✅ Government-ready architecture
- ❌ No privacy for participants

Tier 3: Hybrid Mode (Selective Disclosure)

Designed for: Regulated Financial Institutions Requiring Both Compliance and Transaction Privacy

Technical Implementation:

- Identity revealed through KYC verification (zkMe integration)
- Transaction amounts encrypted/suppressed using homomorphic encryption
- Amounts can be selectively disclosed to authorized parties (regulators, auditors)
- Allows regulatory compliance while preserving competitive transaction privacy

Use Cases:

- **Regulated DeFi protocols and institutional DeFi**
- **Enterprise blockchain applications and B2B transactions**
- **Cross-institutional settlements (bank-to-bank, clearing houses)**
- **Insurance, securities, and trade finance**
- Compliance-conscious privacy applications

Properties :

- ✅ Full KYC/AML compliance
- ✅ Amount privacy from public and competitors
- ✅ Selective disclosure to regulators only
- ✅ Perfect balance between privacy and institutional compliance
- ✅ Meets regulatory requirements without sacrificing commercial confidentiality

4.3 ZK.ME Integration for Compliance

For Tier 2 and Tier 3 transactions requiring identity verification, IBVM integrates with zkMe, a decentralized KYC/compliance infrastructure.

zkMe Integration Architecture

Identity Verification Flow:

1. **User Onboarding :**

- User completes KYC process through zkMe
- Identity credentials issued as zero-knowledge proofs
- User maintains custody of identity data

2. **Transaction Authorization**

- User selects Tier 2 or Tier 3 mode
- zkMe credential attached to transaction
- Proof of KYC compliance verified without revealing underlying identity documents

3. **Regulatory Access**

- Regulators can verify KYC compliance through zkMe interface
- Selective disclosure allows showing identity to authorized parties only
- Maintains privacy from general public while satisfying compliance requirements

Technical Benefits:

- **Decentralized Identity:** No central KYC database
- **Privacy-Preserving:** KYC verification without exposing personal data on-chain
- **Regulatory Compatible:** Meets AML/KYC requirements for institutional adoption
- **Portable Credentials:** Same identity can be used across IBVM ecosystem

Compliance Features:

- AML screening integration
- Sanctions list checking
- Jurisdiction-based access controls
- Audit trail for regulatory reporting
- Real-time compliance monitoring

4.4 Privacy Layer Implementation

Protocol-Level Support :

The IBVM protocol natively supports all three tiers at the consensus level:
Transaction Structure:

```
{
  type: "zk" | "transparent" | "hybrid",
  proof: ZK_Proof,
  identity_credential: Optional<zkMe_Credential>,
  amount_commitment: Optional<Pedersen_Commitment>,
  metadata: Transaction_Metadata
}
```

Smart Contract Integration:
dApps can specify their privacy requirements:

- DeFi protocols can mandate Tier 1 (ZK) for privacy
- Institutional platforms can require Tier 2 (transparent)
- Hybrid applications can support multiple tiers

User Control:
Users choose privacy tier per transaction through wallet interface:

- Privacy toggle in IBVM wallet
- Clear explanation of privacy/compliance trade-offs
- Seamless switching between modes

4.5 Institutional and Government Compatibility

IBVM is architected specifically to support both permissionless DeFi and regulated institutional/government applications—a unique capability among Bitcoin Layer-2 solutions.

The multi-tier privacy model positions IBVM as the premier Bitcoin infrastructure for:

Identity Verification Flow:

Government Use Cases:

- **Public sector procurement** (Tier 2: full transparency for accountability)
- **Tax collection and revenue systems** (Tier 3: identity disclosed, amounts private until audit)
- **Central Bank Digital Currency (CBDC) infrastructure** (Tier 2 or 3 based on policy requirements)
- **Cross-border government settlements** with full compliance
- **Public records and land registries** on immutable Bitcoin security
- **Voting and governance systems** with transparent or private ballot options

Institutional Use Cases:

- **Bank-to-bank settlements** (Tier 3: KYC compliance with competitive privacy)
- **Securities tokenization** (Tier 2: full regulatory oversight and audit trails)
- **Trade finance and letters of credit** (Tier 3: selective disclosure to counterparties)
- **Insurance claims processing** (Tier 3: privacy with regulatory auditability)
- **Cross-institutional clearing and settlement** (Tier 2 or 3: compliance-first architecture)
- **Corporate treasury operations** on Bitcoin infrastructure

Regulatory Access

✅ **Meets existing financial regulations** without compromising Bitcoin's security model
✅ **Provides comprehensive audit trails** for compliance officers and regulators
✅ **Enables institutional participation** in the Bitcoin ecosystem for the first time
✅ **Bridges public blockchain benefits** with private sector compliance requirements
✅ **Future-proof architecture** adaptable to evolving regulatory frameworks globally

Competitive Differentiation:

Unlike other Bitcoin Layer-2 solutions that serve only permissionless use cases, IBVM's architecture makes it:

- **The only Bitcoin L2 ready for government deployment**
- **The only Bitcoin L2 with institutional-grade compliance built-in**
- **The only Bitcoin L2 supporting both privacy and transparency simultaneously**
- **The bridge between Bitcoin's decentralization and institutional requirements**

This positions IBVM to capture both the DeFi market AND the vastly larger institutional and government blockchain market—on Bitcoin's security foundation.

5. UTXO Partitioning for Parallel Processing

5.1 The UTXO Advantage

Bitcoin's use of UTXOs (unspent transaction outputs) is often seen as a hurdle for smart contracts, but IBVM turns it into an advantage through UTXO partitioning.

5.2 Parallel Processing Mechanism

In the UTXO model, transactions consume and create outputs. Critically, transactions touching distinct UTXOs can be processed in parallel without conflicts.

IBVM's Implementation:

1. **Partition Strategy:** The Layer-2 UTXO set is divided into multiple shards or groups
2. **Concurrent Validation:** Different sequencer nodes (or parallel threads) handle separate transaction subsets simultaneously
3. **Conflict Avoidance:** Transactions reference disjoint UTXOs, eliminating processing bottlenecks

5.3 Performance Gains By partitioning UTXOs, IBVM mitigates the traditional bottleneck of linear block assembly:

- Transactions in different UTXO partitions confirm in the same 1-second block
- No waiting for sequential processing
- **Demonstrated Performance**: Internal testing shows ~10,000 TPS (over 1,000× improvement over Bitcoin L1)

5.4 Dynamic Partition Management

Adaptive Partitioning:

- If one partition becomes congested, protocol adjusts partition boundaries
- UTXO reallocation balances load dynamically
- Ensures consistent performance across varying transaction patterns

Key Insight: IBVM transforms Bitcoin's UTXO model into a feature—enabling multi-threaded, parallel execution that exploits the inherently parallel nature of independent UTXOs.

6. Simplified Payment Verification (SPV) Integration

6.1 SPV Foundation

To seamlessly connect IBVM with the Bitcoin mainnet, the platform employs **Simplified Payment Verification** (SPV)techniques as described in Satoshi Nakamoto's original Bitcoin whitepaper.
SPV allows lightweight clients to verify that a transaction was included in the Bitcoin blockchain without downloading the full chain—by checking proof-of-work in block headers and Merkle proof of transaction inclusion.

6.2 Trustless BTC Deposits

Deposit Flow:

1. **User Action:** Send BTC to special lock address on Bitcoin L1 (multi-signature or script-controlled)
2. **Proof Generation:** User or relayer submits SPV proof of the deposit transaction (Merkle path in confirmed Bitcoin block)
3. **IBVM Verification:** IBVM nodes verify proof against Bitcoin's block header chain
4. **L2 Credit:** Once verified, IBVM credits equivalent BTC representation to user's L2 account

No Centralized Custodian Required: Any IBVM full node or user can validate the SPV proof to ensure deposit legitimacy.

6.3 Trust-Minimized Withdrawals

Withdrawal Flow:

1. **User Request:** Burn/lock BTC tokens on IBVM L2, requesting withdrawal to Bitcoin address
2. **State Validation:** Withdrawal corresponds to valid rollup state transition (proven by zk-proof anchored on Bitcoin)
3. **SPV Verification:** System requires SPV proof that latest rollup state (authorizing withdrawal) is recorded on Bitcoin L1
4. **BTC Release:** Bitcoin transaction released from lockbox to user's address

Fraud Prevention: Brief challenge window where anyone can present proof of invalid withdrawal. However, validity proofs should catch fraudulent transactions automatically.

6.4 Non-Custodial Two-Way Peg

By combining zk-proofs for state validity with SPV proofs for Bitcoin inclusion, IBVM achieves **a non-custodial two-way peg:**

- BTC moves in/out based on cryptographic verification
- No federation or oracle approval required
- Any Bitcoin full node or SPV client can audit and enforce the peg
- Security reduces to Bitcoin's own security model

Contrast with Federated Solutions: RSK's federation and similar approaches require trust in signing quorums. IBVM uses SPV so security depends only on Bitcoin blockchain integrity.

7. Bitcoin-EVM Virtual Machine

7.1 Smart Contract Layer

On top of the rollup and UTXO innovations, IBVM features a **Bitcoin-adapted virtual machine** bringing full smart contract capabilities to Bitcoin.

Bitcoin-EVM is closely aligned with Ethereum's EVM (Ethereum Virtual Machine) semantics but adapted for a Bitcoin environment.

7.2 Developer Experience

EVM Compatibility:

- Smart contracts written in Solidity or Vyper
- Familiar account model, gas fees for computation
- Compatible with Ethereum development tools (compilers, wallets, IDEs)
- State changes rolled up and committed to Bitcoin

Hybrid Architecture:

- EVM-style contracts for complex logic
- Bitcoin scripts for custody and bridging
- Seamless interoperation between layers

7.3 Key Attributes

Deterministic Execution

- Each contract call is deterministic and gas-metered
- Prevents infinite loops and DoS attacks
- Execution environment isolated and secure
- Network operations fueled by IBVM tokens (see Network Economics documentation)

Bitcoin Script Integration

- Interoperates with Bitcoin scripts for custody
- Example: EVM multisig wallet tied to actual Bitcoin script holding funds
- Ensures contract logic and Bitcoin script consistency

Gas Model

- Transactions metered by computational cost
- Network fees paid in IBVM tokens (native gas currency)
- Fee market prevents spam and resource abuse
- Efficient execution optimized for rollup batching
- Fee structure detailed in separate Network Economics documentation

7.4 Smart Contract Use Cases

DeFi Protocols:

- Decentralized exchanges (DEXs)
- Lending platforms with BTC collateral
- Stablecoins backed by Bitcoin
- Yield farming and liquidity mining

Digital Assets:

- NFT marketplaces on Bitcoin
- Token standards (BRC-20 style or new standards)
- Fractionalized real-world assets
- Gaming and metaverse applications

Cross-Chain Services:

- Bridges connecting Bitcoin to Ethereum/other chains
- Oracle networks for off-chain data
- Cross-chain messaging protocols

Enterprise Applications:

- Supply chain tracking with Bitcoin security
- Decentralized identity systems
- Automated compliance and regulatory reporting
- Trustless escrow and settlement systems

7.5 Technical Innovation

The Bitcoin-EVM makes IBVM a general-purpose smart contract platform anchored to Bitcoin. This capability, combined with rollup performance and trust guarantees, transforms what Bitcoin can do—from simple transfers to full-fledged decentralized applications, all on a Bitcoin-secured layer.

8. Comparative Analysis: IBVM vs Other Bitcoin Layer-2 Solutions

Feature	IBVM	Lightning	Liquid	RSK	Stacks	BitVM (Theoretical)
Throughput	10,000+ TPS	High (off-chain)	~100 TPS	~100 TPS	~40 TPS	TBD
Smart Contracts	Full EVM	No	Limited	EVM-compatible	Clarity	Theoretical
Security Model	Bitcoin L1 + ZK proofs	Channel parties	Federated	Federated	Proof-of-Transfer	Bitcoin scripts
Trust Requirement	Trustless (cryptographic)	Trustless channels	Federation trust	Federation trust	Separate consensus	Trustless (if viable)
BTC Custody	Non-custodial (SPV)	Channel locks	Federated multisig	Federated peg	No native BTC	Script-based
Finality	Bitcoin L1 + ZK ~1 second L2 / Bitcoin L1 final off-chain	Instant off-chain	~1 minute	~30 seconds	~10 minutes	TBD
New Token	Yes (network utility)	No	L-BTC (pegged)	RBTC (pegged)	STX (separate)	No
Privacy Options	3-tier model	Channel privacy	Confidential txs	Public	Public	Potentially

8.2 Key Differentiators

IBVM's Unique Position:

1. True Bitcoin Layer-2 with Validity Proofs: Combines rollup security (derived from mainchain) with sidechain flexibility (smart contracts, fast finality)
2. No Trust Compromises: Unlike sidechains/federations, IBVM doesn't require trusting new consensus or multisigs
3. Scale + Expressiveness: Far exceeds payment channels in functionality, while maintaining higher throughput than other smart contract L2s
4. Privacy Flexibility: Only solution offering institutional-grade compliance options alongside permissionless privacy
5. Bitcoin-Native: No wrapped assets or changes to Bitcoin protocol required

Contrast

- **Lightning**: Fast payments but no programmability
- **Liquid/RSK**: Smart contracts but federated trust model
- **Stacks**: Smart contracts but separate token/consensus
- **BitVM**: Theoretical, unproven at scale
- **IBVM**: Bitcoin security + Ethereum programmability + ZK scalability

9. Development Roadmap and Milestones

9.1 Historical Milestones (Achieved)

Q4 2023 - Project Inception

- SFoundational R&D: UTXO partitioning design
- ZK proof system evaluation for Bitcoin
- Bitcoin-EVM compatibility prototyping
- Initial architecture whitepaper

Q1 2024 - Development Kickoff

- Team expansion: blockchain engineers, cryptography experts
- First versions of zk-rollup engine
- IBVM virtual machine development
- SPV bridging architecture specification

Q2 2024 - Testnet Alpha

- Alpha testnet in controlled environment
- Basic L2 transactions validated via proofs on Bitcoin testnet
- IBVM Wallet and DApp Store prototypes
- Security audit engagement

Q3 2024 - Public Reveal

- Public litepaper and website launch
- Community building and developer outreach
- Partnership exploration (wallets, Lightning providers)
- Throughput optimization: 9,000 TPS achieved in testing
- EVM compatibility refinement

Q4 2024 - Testnet Beta

- Public beta testnet launch
- Developer and user access with test BTC/tokens
- Ecosystem partner alignment
- Community engagement and feedback collection

Q1 2025 - Final Testing Phase

- Network stabilization incorporating beta feedback
- Strategic funding secured
- IBVM Mobile Wallet launch (50,000+ downloads)
- IBVM DApp creator platform introduction
- Testnet participation rewards program

9.2 Upcoming Milestones

Q2-Q4 2025 - Mainnet Preparation

- Final security audits and penetration testing
- BTC-IBVM bridge activation on mainnet
- Core dApps deployment (DEX, lending protocols)
- Network parameter optimization
- Sequencer infrastructure deployment

Q4 2025 - Mainnet Launch

- Full mainnet deployment
- Privacy tier activation (ZK, Transparent, Hybrid modes)
- zkMe integration for compliance features
- Initial dApp ecosystem launch
- Performance monitoring and optimization

9.3 Post-Launch Development (2026+)

Q1-Q2 2026 - Decentralization Phase

- Community-run sequencer/prover nodes
- Distributed block production implementation
- Enhanced governance mechanisms
- Advanced monitoring and analytics tools

Q3-Q4 2026 - Protocol Enhancements

- Throughput optimization beyond 10k TPS
- Advanced ZK proof systems integration
- New Bitcoin upgrade compatibility (covenants, signature schemes)
- Cross-chain interoperability expansion

2027 and Beyond - Ecosystem Maturation

- Full ecosystem of dApps (DeFi, NFTs, gaming)
- Institutional adoption and enterprise partnerships
- Cross-chain hub development (Cosmos IBC, Polkadot)
- Privacy feature enhancements (fully homomorphic encryption research)
- Continued protocol optimization and research

9.4 Technical Research Priorities

Ongoing Research:

- Recursive proof systems for infinite scalability
- Post-quantum cryptography integration
- Advanced privacy primitives (fully shielded contracts)
- Data availability optimization
- Novel Bitcoin script utilization for L2 security

10. Security Model and Assumptions

10.1 Threat Model : IBVM's security architecture addresses the following threat vectors:

Layer-2 Threats:

- Malicious sequencers attempting invalid state transitions
- Data availability attacks (withholding transaction data)
- Censorship of user transactions
- Front-running and MEV (Maximal Extractable Value) exploitation

Bridge Threats:

- Fraudulent deposit claims
- Unauthorized withdrawals
- SPV proof manipulation
- Eclipse attacks on light clients

Smart Contract Threats:

- Contract vulnerabilities (reentrancy, overflow, etc.)
- Gas griefing attacks
- Cross-contract exploits
- Privacy mechanism bypasses

10.2 Security Guarantees

Mathematical Security (ZK Proofs):

- Computational soundness: Adversary cannot create false proofs without breaking cryptographic assumptions
- Zero-knowledge property: Proofs reveal no information beyond validity
- Succinctness: Proofs verify in logarithmic time

Bitcoin Anchoring:

- Ultimate finality from Bitcoin PoW
- State transitions invalid without Bitcoin-anchored proof
- Reorg protection through sufficient confirmations

Non-Custodial Design:

- No trusted third parties hold user funds
- Cryptographic enforcement of withdrawals
- Bitcoin L1 as ultimate arbiter of disputes

Privacy Security:

- Zero-knowledge mode: Information-theoretic privacy for shielded transactions
- Hybrid mode: Selective disclosure controlled by user
- No privacy leakage between tiers

10.3 Security Assumptions

Cryptographic Assumptions:

- Hardness of discrete logarithm problem (for elliptic curve cryptography)
- Security of hash functions (SHA-256, Keccak)
- Soundness of zk-SNARK/STARK proving systems
- Security of commitment schemes (Pedersen commitments)

Network Assumptions:

- Bitcoin network remains secure (51% attack resistant)
- Sufficient honest full nodes validate IBVM state
- Data availability (at least one honest party archives L2 data)

Economic Assumptions:

- Rational sequencer behavior (when staking implemented)
- Sufficient economic incentive for proof generation
- Market liquidity for bridge operations

10.4 Audit and Verification

Security Practices:

- Multiple independent security audits
- Formal verification of critical circuits
- Public bug bounty program
- Continuous monitoring and incident response
- Open-source codebase for community review

11. Performance Specifications

11.1 Throughput Metrics

Target Performance:

- **Transactions Per Second:** 10,000+ TPS (Layer-2)
- **Block Time:** ~1 second (L2 blocks)
- **Finality:** ~1 second soft finality, Bitcoin confirmation for hard finality
- **Proof Generation:** ~10-30 seconds per batch (depending on batch size)
- **Batch Size:** 10,000-100,000 transactions per proof

Scalability Characteristics:

- Linear scaling with UTXO partitions
- Sub-linear proof verification cost
- Logarithmic state commitment size

11.2 Cost Efficiency

Transaction Costs:

- L2 transaction fees are orders of magnitude lower than Bitcoin L1 due to proof amortization across thousands of transactions
- Cost distributed across entire batch, reducing per-transaction overhead
- Storage efficiency: ~300 bytes per proof on Bitcoin (vs. megabytes for raw transactions))

Computational Efficiency:

- Parallel UTXO processing reduces redundant computation
- Batch verification optimizes cryptographic operations
- Efficient state tree updates

11.3 Resource Requirements

Sequencer Node:

- **CPU:** 16+ cores for parallel processing
- **RAM:** 32GB+ for state management
- **Storage:** 1TB+ SSD for transaction history
- **Network:** 1Gbps+ for transaction propagation

Prover Node:

- **CPU:** 32+ cores or specialized acceleration (GPU/FPGA)
- **RAM:** 64GB+ for proof generation
- **Storage:** Minimal (proofs only)

Full Node:

- **CPU:** 4+ cores
- **RAM:** 8GB+
- **Storage:** 100GB+ (grows with usage)

Light Client:

- Minimal resources
- SPV-level verification
- Suitable for mobile devices

12. Team and Contributors

12.1 Core Team

Dr. John Sajadi - Co-Founder & Chief Architect

- Ph.D. in Computer Science and Blockchain
- Global blockchain architect
- Web3/DeFi thought leader
- Keynote speaker on decentralized technology
- Expert in distributed systems and cryptographic protocols

Albert Dadon AM - Chairman

- Chevalier De l'Ordre National Du Merite
- Order of Australia recipient
- Distinguished entrepreneur and investor
- Decades of experience in governance and strategic growth
- Global diplomacy and cultural leadership background

Alok Agrawal - Co-Founder & CTO

- Technical driving force of IBVM implementation
- Director at Quest Global Technologies
- Extensive enterprise blockchain experience
- Oversees engineering team and development pipeline
- Expert in blockchain protocol development

Romil Jain - Co-Founder & COO

- Deep expertise in blockchain architecture and smart contracts
- EVM systems specialist
- Director at Quest Global Technologies
- Leads Bitcoin-EVM hybrid design and optimization
- Expert in modular systems and cross-chain interoperability

12.2 Development Team

Quest Global Technologies Team:

- Blockchain protocol developers (rollup logic, cryptography)
- Front-end and mobile developers (wallet apps, DApp platform)
- Testing and QA engineers (performance and security testing)
- Award-winning development capabilities
- Proven track record in enterprise blockchain delivery

12.3 Advisory Board

Anthony Jaoui

- Former EY blockchain practice builder (Switzerland)
- Serial entrepreneur
- Institutional strategy and fintech expertise
- Enterprise partnerships and financial structuring advisor

Alexander Rees-Evans

- UNDP blockchain initiative advisory board member
- Author of "How to Launch a Token"
- Co-owner of Fundraisebot and Norm
- Web3 partnerships and go-to-market strategy
- Public listings and ETF expertise

Additional Advisors:

- Cryptography experts
- Bitcoin protocol specialists
- Financial industry insiders
- Academic researchers

12.4 Research Partnerships

IBVM collaborates with:

- Blockchain protocol developers (rollup logic, cryptography)
- Front-end and mobile developers (wallet apps, DApp platform)
- Testing and QA engineers (performance and security testing)
- Award-winning development capabilities
- Proven track record in enterprise blockchain delivery

13. Open Source and Community

13.1 Open Source Commitment

Intellectual Property Framework:

IBVM operates under a multi-entity structure designed to balance innovation protection with open-source principles:

- **IBVM IP LLC (Delaware):** Owns all intellectual property, patents, trademarks, and copyrights related to IBVM technology; responsible for development
- **IBVM Inc.:** Operates as the primary operating entity under perpetual license from IBVM IP LLC
- **IBVM Foundation Inc.:** Holds perpetual license from IBVM IP LLC for network governance

Code Availability:

- Core protocol: Open source (Apache 2.0 / MIT license)
- Smart contracts: Verified and public
- Client implementations: Multiple independent implementations encouraged
- Documentation: Comprehensive technical docs and tutorials

Open Source Philosophy:

While intellectual property is protected under IBVM IP LLC, the project is committed to open-source development principles. This structure allows:

- Protection of innovative breakthroughs (patents, trademarks)
- Free use and development by the community (open-source licensing)
- Prevention of patent trolling or hostile IP claims
- Long-term sustainability through proper IP management
- Clear separation between IP ownership/development (IBVM IP LLC) and operations (IBVM Inc. and Foundation governance)

Community Contributions:

- GitHub-based development
- Public issue tracking
- Community PR review process
- Developer grants for ecosystem tools
- Contributors retain rights to their contributions under project licensing terms

13.2 Developer Resources

Documentation:

- Technical specifications
- API documentation
- Integration guides
- Tutorial series and examples
- Architecture deep-dives

Developer Tools:

- SDKs for multiple languages (JavaScript, Python, Rust)
- Testing frameworks
- Local development environment
- Block explorer and analytics
- Smart contract templates

Support Channels:

- Developer Discord/Telegram
- Technical forums
- Office hours with core team
- Hackathon support

14. Future Research Directions

14.1 Scalability Enhancements

Recursive Proofs:
- Proof of proofs for unbounded scalability
- Constant verification time regardless of transaction volume
- Research collaboration with leading ZK teams

Advanced Parallelization:
- Cross-partition transactions
- Optimistic UTXO locking
- Predictive partition management

14.2 Privacy Innovations

Fully Shielded Contracts:
- Private smart contract execution
- Confidential state transitions
- Research into practical fully homomorphic encryption (FHE)

Cross-Tier Privacy:
- Privacy-preserving compliance proofs
- Selective disclosure protocols
- Anonymous credentials integration

14.3 Interoperability

Cross-Chain Architecture:
- IBC (Inter-Blockchain Communication) integration
- Trustless bridges to Ethereum and other L1s
- Atomic swaps with advanced cryptography

Bitcoin Integration:
- Covenant integration (if/when available on Bitcoin)
- Taproot utilization for improved scripts
- Lightning Network interoperability

14.4 Quantum Resistance

Post-Quantum Cryptography:
- STARK-based proofs (already quantum-resistant)
- Post-quantum signature schemes research
- Migration path for quantum threats

15. Conclusion

International Bitcoin Virtual Machine (IBVM) represents a fundamental advancement in Bitcoin's capabilities. By combining zero-knowledge rollups, UTXO parallelization, Bitcoin-EVM compatibility, and flexible privacy tiers, IBVM transforms Bitcoin from a simple value transfer network into a high-performance, privacy-flexible platform for decentralized applications.

15.1 Technical Achievements

- **Scalability**: 10,000+ TPS with ~1-second finality—over 1,000× improvement from Bitcoin L1
- **Security**: Cryptographic validity proofs anchored to Bitcoin's Proof-of-Work, ensuring trustless operation
- **Programmability**: Full EVM compatibility bringing Ethereum's developer ecosystem to Bitcoin
- **Privacy & Compliance:** Industry-first 3-tier model supporting permissionless privacy AND institutional/government compliance—the only Bitcoin L2 architected for both DeFi and regulated use cases
- **Trustlessness**: Non-custodial SPV-based bridge maintaining Bitcoin's trust model

15.2 Innovation Impact

IBVM bridges the gap between Bitcoin's security and Ethereum's programmability, while introducing novel privacy features that make it suitable for permissionless DeFi, regulated institutional applications, and government infrastructure.

Unique Market Position: IBVM is the **only Bitcoin Layer-2 that serves both markets simultaneously:**

- **Permissionless DeFi:** Privacy-focused applications using Tier 1 (ZK mode)
- **Institutional Finance:** Regulated entities using Tier 2 (transparent) or Tier 3 (hybrid)
- **Government Infrastructure**: Public sector applications using Tier 2 for accountability

This dual-market capability unlocks Bitcoin for institutional and government adoption—historically restricted to permissioned blockchains—while maintaining support for privacy-focused DeFi applications.

The platform requires no changes to Bitcoin's consensus, operates without trusted intermediaries, and maintains the philosophical principles that make Bitcoin the most trusted blockchain—while dramatically expanding what can be built on that foundation.

15.3 Vision Realized

By unlocking Bitcoin's full potential as programmable financial infrastructure, IBVM enables:

- **DeFi** without leaving Bitcoin's security
- **Privacy** when needed for individuals and private applications
- **Compliance** when required for institutions and government
- **Scale** for global adoption across all sectors
- **Innovation** on the world's most secure blockchain

Market Opportunity:

IBVM uniquely positions itself to capture:

1. **Permissionless DeFi Market:** Privacy-focused applications on Bitcoin
2. **Institutional Finance Market:** Banks, payment processors, asset managers using Bitcoin infrastructure
3. **Government & Public Sector Market:** CBDC, procurement, public records on Bitcoin security

This dual-market strategy—serving both DeFi and institutional/government sectors—makes IBVM the most versatile Bitcoin Layer-2 solution and positions it to capture the largest addressable market in the Bitcoin ecosystem.
IBVM represents the evolution of Bitcoin from "digital gold" to the foundation of a global, programmable, privacy-flexible, compliance-ready financial system—all while preserving and reinforcing the principles that make Bitcoin special.

Appendix A: Technical Specifications Summary

A.1 Performance Metrics

- **Throughput:** 10,000+ TPS (Layer-2)
- **Block Time:** ~1 second (L2)
- **Finality:** ~1 second soft, Bitcoin confirmation for hard
- **Proof Size:** ~200-300 bytes (SNARK) or ~100KB (STARK)
- **Batch Size:** 10,000-100,000 transactions

A.2 Privacy Tiers

- **Tier 1 (ZK):** Zero-knowledge proofs, full privacy
- **Tier 2 (Transparent):** Full disclosure, KYC-verified
- **Tier 3 (Hybrid):** Identity revealed, amounts private

A.3 Consensus Model

- **L1 Consensus:** Bitcoin Proof-of-Work (inherited)
- **L2 Consensus:** Validity proofs (zk-SNARKs/STARKs)
- **Finality:** Cryptographic finality on L2, probabilistic finality via Bitcoin

A.4 Bridge Mechanism

- **Deposits:** SPV-verified BTC locking
- **Withdrawals:** Proof-verified BTC unlocking
- **Security:** Non-custodial, cryptographically enforced

A.5 Virtual Machine

- **Type:** Bitcoin-EVM (EVM-compatible)
- **Languages:** Solidity, Vyper
- **Gas Model:** Computational metering
- **Interoperability:** Bitcoin script integration

Appendix B: Cryptographic Primitives

B.1 Zero-Knowledge Proofs

- **zk-SNARKs:** Groth16, PLONK variants
- **zk-STARKs:** FRI-based STARKs
- **Commitment Schemes:** Pedersen commitments, KZG commitments

B.2 Hash Functions

- **Bitcoin Compatibility:** SHA-256
- **EVM Compatibility:** Keccak-256
- **Merkle Trees:** SHA-256 based for Bitcoin anchoring

B.3 Signature Schemes

- **Bitcoin:** ECDSA (secp256k1)
- **EVM:** ECDSA (secp256k1)
- **Future:** Schnorr signatures, BLS signatures

B.4 Encryption

- **Privacy Layer:** ElGamal encryption, Homomorphic encryption (research)
- **Communication:** TLS 1.3 for node communication
- **Key Management:** HD wallets (BIP32/39/44)

Appendix C: Network Architecture

C.1 Node Types

1. **Sequencer Nodes:** Order transactions, produce L2 blocks
2. **Prover Nodes:** Generate zero-knowledge proofs
3. **Full Nodes:** Validate state, maintain full history
4. **Light Nodes:** SPV-level verification
5. **Archive Nodes:** Historical data preservation

C.2 Network Topology

- **Peer-to-peer:** Bitcoin-style gossip network
- **Transaction Propagation:** Optimized mempool
- **Proof Distribution:** Efficient proof relay
- **Data Availability:** Distributed storage layer

C.3 Communication Protocols

- **P2P Protocol:** Custom Bitcoin-compatible protocol
- **RPC:** JSON-RPC for client communication
- **Bridge Protocol:** SPV proof relay mechanism
- **Sequencer Coordination:** BFT-style consensus (future)

References

1. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System"
2. Buterin, V. (2014). "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform"
3. Ben-Sasson et al. (2014). "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture"
4. Groth, J. (2016). "On the Size of Pairing-based Non-interactive Arguments"
5. Bunz et al. (2020). "Transparent SNARKs from DARK Compilers"
6. Gabizon, A., Williamson, Z. J., & Ciobotaru, O. (2019). "PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge"
7. Bitcoin Core Development Team. (2023). "Bitcoin Protocol Documentation"
8. Ethereum Foundation. (2023). "Ethereum Virtual Machine (EVM) Specifications

Document Version: 3.0
Last Updated: October 2025
Copyright: © 2025 IBVM IP LLC. All Rights Reserved.
Contact: technical@ibvm.io
Website: https://ibvm.io

Legal Notice:

This technical white paper is protected by copyright and other intellectual property laws. IBVM™ and all related marks are trademarks of IBVM IP LLC. No part of this document may be reproduced, distributed, or transmitted in any form without prior written permission from IBVM IP LLC, except for non-commercial, educational purposes with proper attribution.

The technology, protocols, and innovations described herein are subject to intellectual property rights owned by IBVM IP LLC. IBVM Foundation Inc. and IBVM Inc. operate under perpetual licenses from IBVM IP LLC.

For licensing inquiries, please contact: licensing@ibvmfoundation.org

---

This is a living document. Technical specifications may be updated as the protocol evolves. For the latest version, please visit our GitHub repository or official website.