ZimX

White Paper

8. Technology and Architecture

The ZimX platform is designed as regulated financial infrastructure. Architectural decisions prioritise regulatory compliance, auditability, safeguarding, and operational control over speed of deployment or speculative functionality.

Deployment Status

No smart contracts have been deployed to any public blockchain network at the time of writing. No testnet or mainnet issuance of ZiGX or ZIMX has occurred. No customer-facing infrastructure is live. All technical descriptions represent design intent, subject to audit completion and regulatory permission.

8.1 Blockchain Infrastructure

Selected Network

The ZimX protocol is designed to operate on Base, an Ethereum-compatible Layer 2 network.

Selection Rationale

Security: - Inherits Ethereum's security model through optimistic rollup architecture - Benefits from Ethereum's extensive security research and audit ecosystem - Settlement finality provided by Ethereum mainnet

Compatibility: - Full EVM compatibility enables use of established development tooling - Compatible with institutional custody solutions - Interoperable with existing compliance and monitoring infrastructure

Efficiency: - Reduced transaction costs compared to Ethereum mainnet - Higher throughput capacity supporting transaction volume requirements - Sub-second confirmation times for improved user experience

Institutional Credibility: - Supported by publicly-traded, regulated entity (Coinbase) - Growing ecosystem of institutional-grade applications - Track record of operational stability

Technical Specifications (Target)

- Block time: Approximately 2 seconds
- Transaction costs: Fraction of a cent per transaction
- Throughput target: 1,000+ transactions per second
- Consensus: Optimistic rollup with fraud proofs

Conditionality

Final network selection remains subject to audit outcomes, custody provider compatibility, and regulatory considerations. No irreversible deployment decisions have been taken.

8.2 Smart Contract Framework

Core Contracts (In Development)

ZIMX Token Contract: - ERC-20 standard implementation - Fixed total supply: 1,000,000,000 ZIMX - No mint, burn, or supply manipulation functions - Transfer restrictions during vesting periods - Governance voting mechanisms

ZiGX Token Contract: - Reserve-backed token with minting controls - Maximum supply cap: 1,000,000,000 ZiGX - Minting permitted only with verified reserve deposit - Multi-signature minting authorisation required - Reserve verification mechanisms

Treasury Contract: - Multi-signature control (minimum 3-of-5 requirement) - Time-locked transactions for major operations (48-72 hours) - Transparent approval logs - Emergency procedures with enhanced authorisation

Governance Contract: - Proposal submission system - Token-weighted voting mechanism - Execution time-locks after approval - Veto mechanisms for critical changes

Vesting Contract: - On-chain enforcement of vesting schedules - Cliff periods and linear release automation - No manual intervention capability - Transparent release calendar

Development Status

Core smart contracts have been professionally developed under contract by Boosty Labs. Development work includes protocol logic relating to token issuance, governance, and settlement mechanics.

Under contractual terms, all deliverables and associated intellectual property vest in Blackmass Enterprises Ltd.

Audit Gating

Deployment of any smart contracts is explicitly gated on: - Completion of independent third-party security audits - Internal remediation of any identified issues - Regulatory readiness and feedback - Custody onboarding and safeguarding arrangements

ZIMX-related contracts: Dual independent audit process ZiGX-related contracts: Triple audit process (reflecting higher regulatory sensitivity)

No deployment occurs prior to completion of relevant audit phases.

8.3 Security Architecture

Smart Contract Security

Development Process: - Formal security requirements documentation - Security-focused development practices - Internal code review before external audit - Comprehensive test coverage (unit, integration, stress testing)

Audit Programme: - Independent audits by established security firms - All findings addressed before deployment - Public disclosure of audit reports - Bug bounty programme for ongoing security (planned)

Design Principles: - Defensive programming throughout - Reentrancy guards on critical functions - Integer overflow/underflow protection - Role-based access control on privileged functions

Infrastructure Security (Intended)

Network Protection: - DDoS protection at multiple layers - Geographic distribution of infrastructure - Redundant systems and failovers - 24/7 monitoring and alerting

API Security: - Rate limiting and throttling - Authentication and authorisation controls - Encrypted communications (TLS 1.3+) - Input validation and sanitisation

Data Security: - Encryption at rest and in transit - Secure key management systems - Compliance with data protection regulations

Treasury Security

Multi-Signature Control: - Minimum 3-of-5 signers for major operations - Geographic and organisational distribution of signers - Hardware wallet signing devices - Transparent signing logs

Time-Lock Mechanisms: - Large transactions delayed 48-72 hours - Review window for community and regulators - Emergency override with enhanced authorisation - Transparent countdown visibility

Custody Security

Reserve assets are intended to be held with third-party institutional custodians, not by ZimX Finance. Custody arrangements

include: - Regulated institutional custody providers - Insurance coverage for custody risks - Regular security audits of custody practices - Multi-signature controls on reserve movements

8.4 Scalability and Performance

Design Targets

Transaction Throughput: - Target: 1,000+ transactions per second - Sufficient for projected initial adoption scenarios - Scalable through Layer 2 optimisations

Transaction Costs: - Target: Sub-cent transaction fees - Enables micro-transaction viability - Cost efficiency for high-volume, low-value remittances

Settlement Speed: - Target: Near-instant on-chain confirmation - Ethereum mainnet settlement for finality - User-facing confirmation within seconds

Reliability Targets

- Uptime target: 99.9%+
- Redundant infrastructure design
- Geographic distribution for resilience
- Disaster recovery procedures

8.5 Integration Capabilities

Wallet Integration (Intended)

- Mobile SDKs for iOS and Android development
- Web-based wallet interface
- USSD/SMS fallback for feature phones
- Multi-language support

Merchant Integration (Intended)

- API documentation for payment integration
- QR code payment acceptance
- Point-of-sale system connectivity
- E-commerce platform plugins

Partner Integration (Intended)

- Banking system connectivity
- Mobile money operator integration
- Payout partner interfaces
- Regulatory reporting feeds

All integrations are subject to partner agreements, regulatory permission, and technical readiness.

8.6 User-Centric Design Principles

Accessibility

Device Compatibility: - Mobile-first design (iOS, Android) - Web interface for desktop access - Feature phone support via USSD/SMS - Low-bandwidth optimisation

Language Support: - English (primary) - Shona (local) - Ndebele (local) - Additional languages for corridor expansion

Connectivity: - Offline transaction queuing - Automatic synchronisation when online - Low data consumption design - USSD fallback always available

Usability

Interface Design: - Clean, uncluttered layout - Clear information hierarchy - Consistent design language - Accessibility considerations (contrast, sizing)

User Experience: - Streamlined onboarding process - Minimal steps for common operations - Clear error messages and guidance - Help documentation accessible in-app

8.7 Regulatory and Compliance Technology

KYC/AML Technology (Intended)

Identity Verification: - Integration with established KYC providers - Document capture and verification - Biometric matching - Liveness detection

Risk Assessment: - Automated risk scoring algorithms - Transaction pattern analysis - Enhanced due diligence triggers - Sanctions list screening (OFAC, UN, EU)

Transaction Monitoring (Intended)

Real-Time Analysis: - All transactions analysed as they occur - Pattern matching for suspicious activity - Geographic anomaly detection - Volume and frequency analysis

Reporting: - Suspicious Activity Report generation capability - Regulatory reporting templates - Audit trail maintenance - Data retention compliance

Data Protection

Privacy by Design: - Minimal data collection principle - Purpose limitation for data use - Privacy impact assessments - User consent mechanisms

Compliance: - GDPR alignment for UK operations - Data protection compliance in operating jurisdictions - Encryption standards (AES-256 at rest, TLS 1.3+ in transit) - Clear data retention policies

8.8 Development and Operations

Technology Stack (Intended)

Backend: - Modern scalable architecture - Relational database for structured data - Caching layers for performance - Message queues for asynchronous processing

Frontend: - Cross-platform mobile development - Web application framework - Type-safe development practices - Modern build tools and optimisation

Infrastructure: - Cloud-native architecture - Container orchestration - Infrastructure as code - Multi-region deployment capability

Development Practices

- Git-based version control
- Code review requirements
- Continuous integration pipelines
- Automated testing at multiple levels
- Security scanning integration

8.9 Technical Scope Exclusions

The ZimX platform does not include: - Lending or credit products - Yield-bearing accounts - Algorithmic or partially-backed stablecoin mechanisms - Permissionless issuance or redemption - Retail trading functionality - Decentralised finance integrations

Any future expansion of technical scope would be subject to separate regulatory review and approval.

8.10 Development Roadmap (Conditional)

The following phases are dependent on regulatory permission, audit completion, and funding:

Phase 1: Foundation - Smart contract deployment (post-audit) - Mobile wallet minimum viable product - Basic merchant integration - Custody and reserve infrastructure

Phase 2: Enhancement - Enhanced wallet features - Expanded merchant tools - Analytics and reporting - Multi-corridor support

Phase 3: Integration - Banking partnership integrations - Utility payment systems - Government services connectivity

Phase 4: Maturity - National coverage expansion - Institutional adoption support - Regional expansion infrastructure

All phases are subject to regulatory feedback and operational dependencies. Timelines are not guaranteed.

The technical architecture combines security, compliance, and accessibility. All systems are designed for regulated operation. Deployment is gated on audit completion, custody readiness, and regulatory permission. No assumptions are made regarding timelines or approval.