



Finance

Technical Architecture

White Paper · 2026 Edition

Blockchain infrastructure, smart contracts, and security design.

BlackMass Enterprises Ltd
UK Company No. 16124799

Technical Architecture

The ZimX platform is built as regulated financial infrastructure. Every architectural decision prioritises compliance, auditability, and operational resilience. This document covers the blockchain layer, smart contract framework, security architecture, and platform design.

1. Blockchain Infrastructure

ZimX is currently designed for Base, an Ethereum-compatible Layer 2 network. Base was selected for four reasons.

Security. Base inherits Ethereum's security model through its rollup architecture, with settlement finality on Ethereum mainnet. Transactions benefit from one of the most established smart contract ecosystems in the industry.

Cost. Transaction fees are typically a fraction of a cent, making micro-transactions viable, critical for a corridor where many transfers are small, regular amounts supporting family expenses.

Speed. Current block times of approximately two seconds are designed to deliver near-instant on-chain confirmation. Users are expected to experience transfers completing in minutes rather than the days typical of legacy infrastructure. Actual performance depends on network conditions at the time of transaction.

Institutional compatibility. The network supports the institutional custody solutions, compliance tooling, and monitoring infrastructure that regulated financial services require.

Final network selection remains subject to audit outcomes and custody compatibility.

2. Smart Contract Framework

Core smart contracts have been professionally developed by Boosty Labs.

All deliverables and intellectual property vest in BlackMass Enterprises Ltd. The initial on-chain components include:

ZIMX Token Contract. Fixed total supply of 1,000,000,000. No minting or supply manipulation mechanisms. Designed for ecosystem utility, access entitlements, and fee tiering.

ZiGX Token Contract. Reserve-backed settlement token with minting controls. Maximum supply cap of 1,000,000,000. Minting occurs only against verified reserve deposits with multi-signature authorisation and full audit trail.

Treasury and control framework. Treasury operations are governed through role-based access control, multi-signature approvals, and time-lock procedures, with transparent logs and enhanced thresholds for sensitive actions.

Governance design. Governance functionality is introduced progressively and enforced through audited controls, subject to regulatory permission, security audit outcomes, and operational readiness.

Vesting Contract. On-chain enforcement of team vesting schedules (including cliff periods and linear release) with no manual override capability and full transparency.

Audit Programme

Deployment is gated on independent third-party security audits. ZIMX contracts undergo dual independent audit. ZiGX contracts undergo triple audit, reflecting the higher sensitivity of reserve-backed instruments. Primary audit partner: Hacken. All findings must be addressed before deployment. Audit reports will be publicly disclosed.

3. Security Architecture

Smart Contract Security

Development follows security-focused practices: formal requirements documentation, internal code review before external audit, and comprehensive test coverage. Design principles include defensive programming, reentrancy guards, overflow protection, and role-based access control on all privileged functions.

Treasury Security

Multi-signature controls require multiple signers for major operations, with geographic and organisational distribution using hardware wallet signing devices. Time-lock mechanisms provide a review window for large movements. Cold storage holds the vast majority of reserves; hot wallets maintain only operational liquidity.

Infrastructure Security

Planned infrastructure includes DDoS protection, geographic distribution for resilience, redundant systems, and continuous monitoring. API security encompasses rate limiting, authentication controls, modern encryption, and input validation. Data protection practices align with GDPR.

4. ZiRA™ Platform Architecture (Zimbabwe Resource Assistant)

ZiRA's architecture separates the AI-powered access and information layer from settlement infrastructure.

The design goal is that the experience on a £1,200 smartphone in London and a £15 feature phone in rural Masvingo is functionally equivalent. The frontend is cross-platform: native iOS and Android apps, a web interface, and USSD/SMS fallback for feature phones. The backend uses scalable cloud-native architecture with multi-region deployment for availability and disaster recovery.

Accessibility Design

Device support spans smartphones, desktop browsers, and feature phones. Language support: English, Shona, and Ndebele with expansion capability. Connectivity design includes offline transaction queuing, low data consumption, and always-available USSD fallback. The interface prioritises simplicity and clear hierarchy.

Integration Capabilities

The platform supports wallet integration through mobile SDKs, merchant integration through APIs and QR systems, and partner integration for banking, mobile money, and payout connectivity. All integrations are subject to partner agreements and regulatory permission.

5. Scope

The platform does not include lending, credit, yield-bearing accounts, algorithmic stablecoin mechanisms, permissionless issuance, retail trading, or DeFi integrations.

ZimX Finance is in development and not yet operational. This document is for informational purposes only and does not constitute an offer of securities, investment advice, or a guarantee of any outcome. All forward-looking statements are conditional on regulatory permission, audit completion, and operational readiness.