IndoBit: A Zero-Knowledge Identity Protocol for the Indonesian Web3 Ecosystem

Version: 1.0.1 (last change on July 23, 2025)

Abstract

This paper proposes IndoBit, a decentralized identity verification protocol designed to enable privacy-preserving, zero-knowledge proofs (ZKPs) of key user traits (such as phone verification, age, or region) for Indonesian users in the Web3 ecosystem. IndoBit leverages zero-knowledge circuits to allow users to cryptographically prove attributes without exposing underlying data. The protocol uses IBIT, a native Solana token, to govern access, incentivize verifiers, and align incentives. IndoBit aims to become a foundational identity primitive for Indonesia's digital economy.

1. Introduction

In emerging markets like Indonesia, digital identity is fragmented and invasive: applications require excessive personal data (e.g., KTP upload, selfies), and data breaches are rampant. At the same time, Web3 adoption is growing, but lacks localized identity rails. IndoBit aims to fill this gap, offering an identity layer that's:

- Zero-knowledge and privacy-first
- Token-incentivized and decentralized
- Optimized for the Indonesian regulatory, UX, and infrastructure landscape
- The protocol enables users to prove facts like "I own an Indonesian phone number," "I'm over 18," or "I'm unique" - without exposing the raw data, using zkSNARKs and other cryptographic primitives.

2. Problem Statement

Current identity systems face the following issues:

- Privacy Risk: Centralized KYC exposes user PII
- Sybil Attacks: dApps are flooded with fake accounts and bots
- Regulatory Conflict: Developers cannot handle identity data without compliance overhead
- Lack of Local Relevance: No identity solutions reflect Indonesian infrastructure (phone, e-KTP, WhatsApp).

Zero-Knowledge Identity for Indonesia

3. System Design

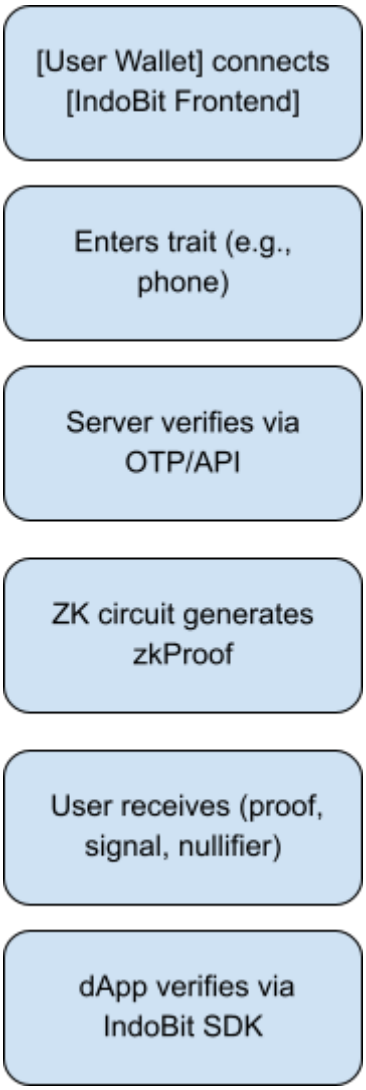
3.1. Identity Traits

IndoBit supports ZK proofs of specific identity "traits," not full documents. Initial supported traits:

- Phone Ownership
- Geolocation Region
- Age Bucket
- Email Ownership

Each trait has an associated ZK circuit.

3.2. Architecture Overview



3.3. Zero-Knowledge Circuits

Circuits are written in Circom or Noir, compiled to SNARKs using Groth16 or PLONK. Each circuit:

- Takes user input (e.g., phone hash, OTP code)
- Generates zkProof for public signal (e.g., "phone verified")
- Uses nullifier to prevent replays

4. Token Design (IBIT)

4.1. Utility

- Access Fee: Users burn or spend IBIT to generate proofs
- Staking: Trusted issuers (e.g., phone verification providers) stake IBIT
- Governance: IBIT holders vote on accepted trait types
    - Proof expiration
    - Circuit upgrades
    - Reward: Proof verifiers or evaluators may receive IBIT

4.2. Economics

- Proof cost: e.g., 1-5 IBIT per proof
- Staking requirement: e.g., 1,000 IBIT for a validator

5. Security & Privacy

- All proofs are zero-knowledge; no PII is stored or revealed
- Nullifiers prevent replay or double-claim
- No DID or wallet linkage is required
- Proofs can be verified without a centralized backend
- Future versions may implement zk-SBT (soulbound traits) that are unlinkable but revocable.

6. Use Cases

Use-case	Description
App Login	Users prove phone ownership, age, region

Age-restricted Access	Games/finance apps verify “over 18” status
Anti-bot Sybil Control	Require IndoBit proof to ensure uniqueness
Cross-dApp Identity Portability	One proof = reusable across services

7. Roadmap Summary

Phase	Goal	Traits	$IBIT Usage
1	ZK Phone Proof MVP	Phone	Pay per proof
2	Trait Expansion	Email, Region, Age	Stake, reward
3	Dev SDK + Proof Aggregation	All above	Verifier Incentive
4	DAO Governance	Community-elected	Full DAO voting

8. Risks

We’ve identified several risks associated with this project, such as:

1. Adoption Risk: Users or devs may not integrate the SDK.
2. UX Complexity: Poor onboarding for wallets or ZK usage.
3. Sybil Gaps: Unverified traits may be abused without staking.
4. Compliance Ambiguity: May conflict with e-KYC mandates.

9. Future Work

1. ZK biometric sketching (e.g., voice hash via WA)
2. Reputation proof aggregation across apps
3. Integration with e-KTP API or local banking rails
4. zkML to evaluate traits based on encrypted behavioral patterns

10. Conclusion

IndoBit offers a real, applicable use of zero-knowledge cryptography in a region lacking private identity tools. By focusing on Indonesia's infrastructure and usage patterns, it builds a localized, token-powered zkID layer that protects users, reduces compliance overhead, and gives developers a path toward Sybil-resistant user bases.