Simpl — Whitepaper

Simpl is a peer-to-peer crypto transfer platform that lets users send and receive digital assets using a verified phone number as a universal identifier. Simpl replaces long wallet addresses with a secure phone-to-wallet mapping layer, automatically routes transactions to the correct blockchain and wallet, and optionally holds funds in a smart-contract escrow until the recipient claims them. Simpl is designed for mainstream adoption: simple UX, strong privacy protections, and modular architecture that supports multiple chains and custodial or non-custodial wallets.

1. Problem

Wallet addresses are long, error-prone, and intimidating to non-technical users.

Cross-chain transfers require users to manage multiple wallets and addresses.

User errors are often irreversible; recovering funds is costly or impossible.

Onboarding friction prevents mainstream adoption.

2. Value Proposition

Send crypto as easily as sending an SMS.

Reduce transaction errors by mapping phone numbers to verified wallets.

Support both custodial and non-custodial users.

Offer fallback escrow and claim flows for unregistered recipients.

3. How Simpl Works

Verification & Linking: User verifies phone via OTP and links one or more wallets (e.g., MetaMask via WalletConnect, Bitcoin via xpub, or an in-app custodial wallet).

Mapping Layer: The backend stores phone → wallet mappings. Mappings are stored encrypted; only a hashed/obfuscated token is used in public references. Optionally anchor verification proofs or revocation metadata on a light on-chain registry (minimal on-chain footprint).

Send Flow: Sender inputs phone number and amount. System resolves recipient mapping and network, prompts user to sign the transaction using their chosen wallet. Transaction is broadcast to the chain.

Escrow (fallback): If recipient is unregistered or opts out, funds are held in an escrow smart contract. Recipient verifies phone and claims funds. Escrow contains timeout and dispute resistant logic.

Notification & Finality: Recipient receives notification and a transaction record. Block confirmations are surfaced, and a link to a block explorer is offered.

Sender app → Simpl API: send request (phone, token, amount)

Simpl API → Mapping service: resolve wallet + chain

Simpl API → Sender wallet: request signature

Sender wallet → Blockchain: broadcast TX or Escrow contract

Blockchain → Simpl monitoring: listen for confirmations

Simpl → Recipient: push notification / claim flow

4. Technical Architecture

Components

Mobile app (React Native / Flutter) — UI, WalletConnect client, local key handling for non-custodial mode.

Simpl Gateway (API) — Node.js/Go service that handles mapping lookups, routing decisions, fee estimation, and transaction orchestration.

Mapping Service — Encrypted datastore (Postgres or Mongo) holding phone hash → wallet tuples, salt, chain metadata, verification proofs. Access controlled by the API.

Blockchain Workers — Off-chain services that handle transaction construction, gas optimization, L2 routing, and confirmation monitoring.

Escrow Contracts — Solidity (or chain equivalent) contracts to hold unclaimed funds; include timeouts, multi-sig recovery, and a reclaim path.

Key Management — For custodial flows use HSM or KMS (AWS KMS, Azure Key Vault) with strict policies. For non-custodial flows rely on WalletConnect and user private keys.

Mapping design options

Off-chain encrypted mapping: Store phone hash + encrypted wallet. Simpl decrypts for routing (centralized but private).

Decentralized DID approach: Register a public DID or ENS name mapping to an on-chain pointer — better privacy tradeoffs but higher cost/complexity. Choose hybrid: off-chain for privacy, optional on-chain anchor for non-repudiation.

5. Escrow Smart Contract

Purpose: Safely store funds sent to unregistered numbers.

Mechanics: sender deposits funds to escrow contract with metadata (phone hash, expiry). Recipient registers phone and proves identity to Simpl; Simpl instructs contract release to recipient address. If recipient does not claim before expiry, sender can reclaim funds. Include dispute resolution and logs.

6. Security & Threat Model

Threats

Phone number hijack (SIM swap)

Compromised user private key

Mapping DB compromise

Front-running of on-chain settlement

Mitigations

Multi-factor verification for high-value operations (SMS + email + device binding).

Use ephemeral nonces + signatures for mapping updates.

Encrypt mapping with per-record salts; use strict access controls and audit logs.

Use relayer batching and gas estimation to minimize front-running vectors.

Escrow timeouts and multisig/guardian recovery for high-value accounts.

7. Roadmap

MVP (Q1): Phone verify, wallet link, ETH testnet send/receive, escrow demo.

Beta (Q2): Mainnet ETH, UI polish, analytics, 3k beta users.

Launch (Q3): Multi-chain support (BSC, Polygon), on/off ramps, 50k users.

Scale (Q4+): Partnerships, SDK for merchants, compliance expansions.

Legal Disclaimer

This document is for informational purposes and not an offer to sell securities. Simpl will consult legal counsel for token issuance, money-transmitter risk, and local licensing.