Incognito

A Wallet-to-Wallet Privacy Protocol for Ethereum

Incognito enables private transfers of the ERC-20 token INC by encrypting transaction details on Ethereum and all EVM-compatible chains. Private transfers are done entirely on Layer 1 via smart contracts with no off-chain dependencies, logs, mixers, relayers or Layer-2 solutions.

---

1. Introduction

Public blockchains expose transaction data, allowing tracing of participants and flows. This compromises privacy and security. *Incognito* addresses this by allowing users to securely hold and transfer INC without revealing recipient or amount data. It operates fully on-chain, with no off-chain infrastructure, intermediaries, or relayers. The total INC supply is capped at 10 million tokens.

---

2. Protocol Overview

Private Send: Transfers occur through a two-step encrypted contract interaction. Tokens are sent wallet-to-wallet in a way that is immediate, non-custodial, and unlinkable. Only the recipient can decrypt the transfer and access the funds.

Gasless ETH: Users swap INC for ETH without holding ETH, solving the cold wallet problem. Gas is paid in INC, and ETH comes from a shared, manually funded pool.

Optional Decryption: Users can reveal balances for public use. Decryption is voluntary, may be partial, and is irreversible.

ERC-20 and EVM Compatible: INC conforms to ERC-20 and deploys on all EVM chains.

Transfers are never pooled, delayed, or routed through intermediaries. Each transaction is direct and trustless.

---

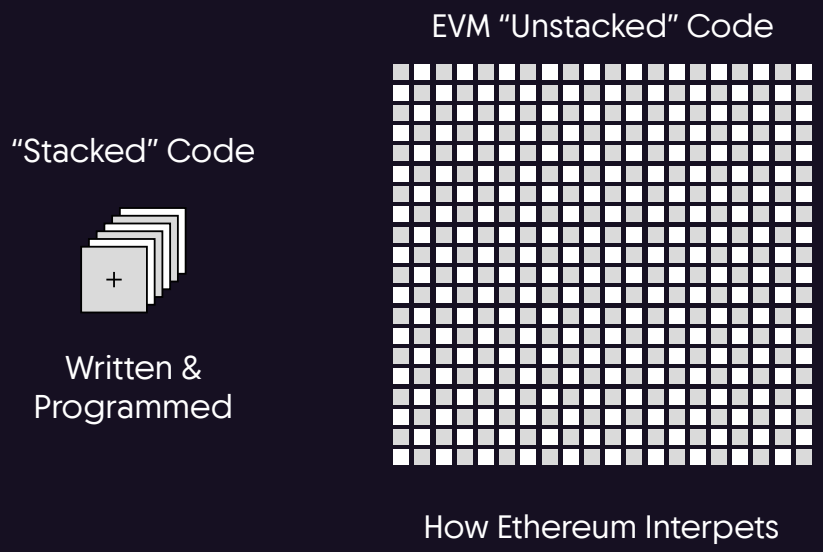
3. On-Chain Visibility

Only a limited set of interactions are visible on-chain:

- Wallets interacting with the Private Send contract (encrypted and indistinct).
- Public DEX trades (e.g. buying or selling INC on Uniswap).
- Gasless Swap calls, which surface a wallet requesting ETH.
- Optional decryptions, which reveal part or all of a private balance.

None of these events are linked to each other on-chain. Transaction paths cannot be reconstructed, and encrypted transfers do not reveal sender, recipient, or amount. The protocol emits no logs or metadata beyond what is necessary for base functionality.

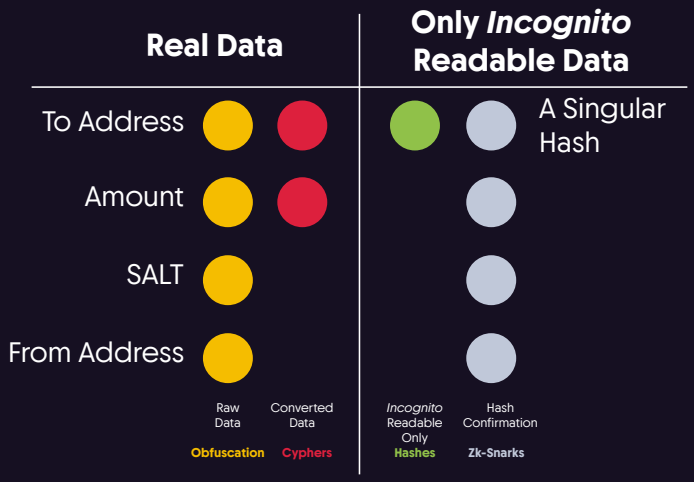
4. Technical Details



Irreversibility Principle
Ethereum compiles contracts into a flattened structure that is difficult to reverse-engineer. *Incognito* applies a combination of advanced techniques that prevent reconstruction of the original logic. This ensures that the privacy logic remains secure, private, and unalterable once deployed.

These methods were developed through years of refinement and were not available elsewhere. The result is a system where contract logic remains internal and unmodifiable once deployed, ensuring long-term consistency and operational integrity without external control. This principle of irreversibility is fundamental to *Incognito*'s privacy model.

Cyphers, Hashes, and SNARK-like Structure
Incognito processes real transaction data—recipient, amount, sender, and salt—through a custom cypher that is readable only by the privacy contracts. This cyphered output is then combined into a hash, with reversibility functioning in a SNARK-like manner. Only the recipient, using their private key, can decrypt the output and access the underlying values. This design enables one-way encryption with selective revealability.



"Privacy Barrier" or the point past where only the recipient's key can read data

The hashing system uses Ethereum's Keccak-256 algorithm for modeling and storage, extended with custom arithmetic, timestamps, byte-shifting, and decomposed metadata such as sender variables. These components are designed to fit within Ethereum's constrained contract size while preserving security and execution speed.

A minimal obfuscation layer is also applied—such as event suppression and modified calldata formatting — to reduce indexability by block explorers and limit passive data exposure. While not a core privacy mechanism, it increases the cost of surveillance. Even with direct observation, no party can recover the source values or reconstruct transfer paths without the recipient's private key.

5. Security and Governance

The Private Send protocol is fully autonomous. It has no admin keys, no fee mechanisms, no governance, and no operator access. Contracts are immutable, store no user data, and enforce privacy entirely on-chain through cryptographic design. The Gasless Swap contract operates separately from the privacy system. The ETH pool it uses is shared and non-custodial. The rate is manually set and typically less favorable than the open market. The pool is designed for minimal utility, yielding just enough ETH for a basic action—such as decrypting, sending, or using a DEX. It is not linked to prior activity or balance size. Anyone may contribute ETH. Contributions are permanent.

Incognito is a minimal, embedded privacy system for Ethereum and EVM chains—built without intermediaries and designed to function passively and autonomously within the Ethereum network.