INCOGNITO

Be Invisible

Start moving privately without leaving the chain

Whitepaper v1.0

incognito-evm.com

incognito_evm

incognito_evm

INCOGNITO

Incognito EVM Whitepaper

PRIVACY INFRASTRUCTURE FOR ETHEREUM

Version: 1.0

Date: January 2026

STATUS (AS OF JANUARY 9, 2026

Incognito EVM is in advanced development. The core protocol and privacy architecture are feature-complete, with the user-facing dApp in final "Coming Soon" preparation. Full Ethereum Mainnet activation and public access are targeted for Q1 2026, subject to final testing and security reviews.

TL;DR

Incognito EVM restores privacy to Ethereum through zero-knowledge, on-chain value transfers for $INC, hiding transaction amounts, breaking sender–recipient links, and preserving full self-custody.

Privacy as infrastructure, not an afterthought.

WHO INCOGNITO EVM IS FOR

Incognito EVM is designed for privacy-conscious Ethereum users, DAOs managing sensitive treasury activity, and institutions that require financial discretion without sacrificing on-chain verification, composability, or self-custody.

TABLE OF CONTENTS

Executive Summary

RESTORING PRIVACY TO ETHEREUM

Ethereum was designed to be trustless, not private.

Every transaction, every balance, and every interaction on Ethereum is permanently visible. Wallet activity can be tracked, behavioural patterns can be profiled, and users are exposed to bots, scrapers, surveillance, and targeted attacks simply by participating in the network. Transparency, while foundational to trustless verification, has quietly become one of Ethereum's most significant constraints.

For individuals, this results in the loss of financial discretion.

For DAOs and treasuries, it exposes operational strategy.

For institutions, it makes privacy-sensitive activity impractical on-chain.

As on-chain activity scales toward institutional adoption, privacy is becoming a prerequisite rather than a feature.

INCOGNITO EVM EXISTS TO CLOSE THIS GAP

Incognito is a privacy-focused infrastructure protocol built directly on Ethereum, designed to enable private, unlinkable value transfer without removing users from the Ethereum ecosystem. Rather than relying on mixers, custodial systems, or off-chain settlement, Incognito applies zero-knowledge cryptography to preserve privacy while maintaining on-chain verification, composability, and security.

At the core of the protocol is $INC, an ERC-20 token that powers Incognito's privacy execution layer. Using zero-knowledge proofs, users

Executive Summary

will be able to send value, deposit, withdraw, and interact with privacy-enabled features while concealing transaction amounts and breaking observable links between senders and receivers. Proofs are generated client-side and verified on-chain, ensuring that privacy guarantees are cryptographic rather than procedural.

Incognito is fully EVM-compatible and will operate on Ethereum Mainnet. Smart contracts verify privacy proofs directly on-chain, while auxiliary components such as gasless execution are handled through a relayer to improve usability without introducing custodial risk. Encrypted secrets are stored in decentralized storage, ensuring that sensitive data remains unreadable to third parties.

Unlike legacy privacy solutions that sacrifice composability or require trusted intermediaries, Incognito is designed to integrate with Ethereum as it exists today. Users retain custody of their assets at all times. Funds are held in a non-custodial shielded pool, with no centralized control of value and no withdrawal delays imposed by the protocol.

Security and resilience are central to Incognito's design. The protocol employs audited smart contracts, industry-standard security libraries, and a controlled upgrade model with role-based access and time-locks to allow responsible evolution while mitigating systemic risk. Privacy is enforced mathematically, not through obfuscation or policy.

With a fixed supply of 1,000,000,000 INC, the protocol's economic model is designed to support sustainable usage, ecosystem incentives, and long-term alignment between users and the network. Privacy-enabled actions,

Executive Summary

protocol services, and future governance mechanisms are all anchored to the $INC token.

Incognito does not attempt to make Ethereum invisible.

It makes value transfer unlinkable.

By restoring discretion to on-chain activity, Incognito unlocks a new class of use cases, from private treasury management and user protection to institutional participation, without compromising Ethereum's core principles.

Privacy is not a niche feature.

It is foundational infrastructure.

INCOGNITO BRINGS IT BACK TO ETHEREUM

1. The Privacy Gap on Ethereum

Ethereum's transparent ledger enables global verification and composability, but it also permanently exposes transaction amounts, wallet balances, sender–recipient relationships, and behavioural patterns to analytics firms, bots, scammers, and surveillance entities.

This creates fundamental constraints:

- Individuals lose default financial privacy
- DAOs expose treasury movements and internal strategy
- Institutions cannot transact without leaking sensitive information
- Sophisticated users become targets through behavioural analysis

Existing privacy solutions fall short. Classic mixers rely on pooled liquidity and introduce timing risks. Off-chain systems add trust assumptions. Many newer privacy rollups require bridging and sacrifice native Ethereum composability.

Incognito EVM addresses this gap by providing **native, on-chain unlinkability of value transfers, without leaving Ethereum Mainnet.**

2. Design Principles

Incognito EVM is built around the following principles:

1. **PRIVACY AS A CORE PRIMITIVE**
   Enforced mathematically via zero-knowledge proofs.

2. **PRIVACY AS A CORE PRIMITIVE**
   Enforced mathematically via zero-knowledge proofs.

3. **ON-CHAIN VERIFICATION ONLY**
   All protocol rules and proofs are validated directly on Ethereum.

4. **SEAMLESS EVM INTEGRATION**
   Compatible with existing wallets, tooling, and infrastructure.

5. **SECURE, CONTROLLED EVOLUTION**
   Upgradeable via UUPS proxies with multisig, role-based access control, and timelocks.

3. Protocol Architecture

Incognito EVM consists of three integrated layers:

3.1 FRONTEND LAYER

A Next.js web application built with TypeScript, Material UI, and Framer Motion. Zero-knowledge proofs are generated client-side using Barretenberg, with Ethereum interaction handled via Ethers.js v6 and support for standard Ethereum wallets.

Targeted launch: **https://app.incognito-evm.com**

3.2 BLOCKCHAIN LAYER

Deployed and/or targeted for Ethereum Mainnet and Sepolia:

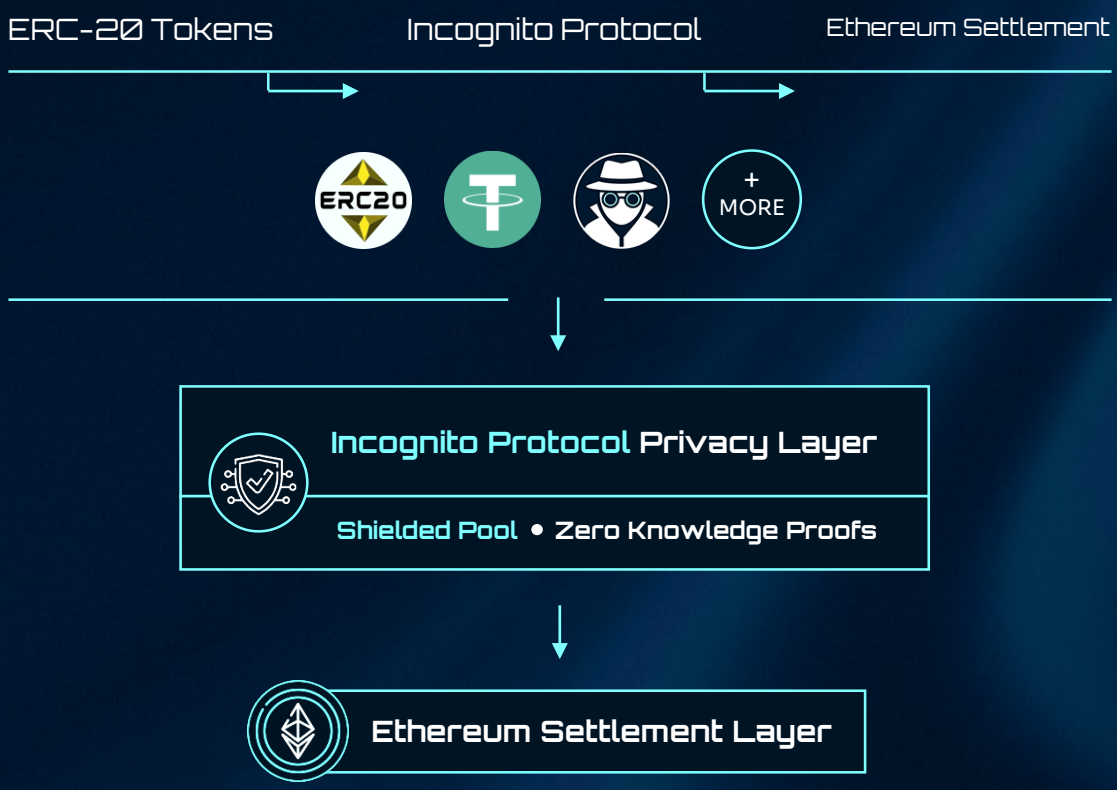
- $INC token contract (ERC-20 with privacy extensions, UUPS upgradable)
- Shielded pool (commitments, nullifier registry, Merkle tree)
- Zero-knowledge proof verifiers (Solidity v0.8.22, Hardhat, OpenZeppelin)
- Security modules: ReentrancyGuard, Pausable, AccessControl

3.2.1 Protocol Extensibility

Incognito is designed to support additional assets through the same shielded pool and zero-knowledge framework, enabling privacy-preserving transfers for other ERC-20 tokens without altering the core trust model, cryptographic assumptions, or custody guarantees.

3. Protocol Architecture

Asset support is implemented at the protocol level, allowing new ERC-20 tokens to leverage the existing commitment, nullifier, and verification architecture while maintaining consistent security and privacy properties.



3. Protocol Architecture

Transact Privately on Ethereum

PUBLIC TRANSFER	INCOGNITO TRANSFER
 Your Wallet	 Recipient Wallet
Visible Amounts Linked Addresses	Amount Hidden Wallets Unlinked

3.3 STORAGE LAYER

Decentralized storage via IPFS (Web3.Storage) is used as a secure “dead drop” for encrypted secrets required in private transfers.

4. Zero-Knowledge Privacy Layer

INCOGNITO EMPLOYS **ZK-SNARKS** TO ENFORCE PRIVACY:

- **Circuit language:** Noir
- **Proof system:** UltraPlonk

EXECUTION MODEL:

- Proof generation occurs client-side (Barretenberg)
- Proof verification occurs on-chain via smart contracts

HYBRID PRIVACY DESIGN:

- Shielded pool for deposits and withdrawals (commitments + nullifiers prevent double-spend)
- IPFS-encrypted notes for Private Send, decryptable only by the intended recipient

PRIVACY GUARANTEES:

- Transaction amounts are hidden
- Sender–recipient relationships are broken
- Deposits are unlinkable from withdrawals and transfers
- Anonymity sets grow with protocol usage

LIMITATIONS:

Network-level metadata, timing, and relayer usage remain observable. Effective anonymity depends on usage diversity and operational security practices.

5. How Incognito Differs

Feature	INCOGNITO	Classic Mixers	Programmable Privacy Systems
Deployment	Ethereum Mainnet (L1)	Ethereum L1	Often L2 / rollups
Custody	Fully non-custodial	Non-custodial (pool risk)	Varies
Bridging	Not required	Not required	Frequently required
Composability	Native Ethereum	Limited	High, off-mainnet
Privacy Model	Shielded pool + encrypted notes	Pooled mixing	Advanced ZK / FHE
Scope	INC transfers + gasless ETH	Generic assets	Broader, complex
Audit Status	Cyberscope.io	Varies	Varies

Not a Mixer

Incognito EVM is not a mixer and does not rely on pooled liquidity, withdrawal delays, or anonymity-set obfuscation. Privacy is achieved through cryptographic unlinkability enforced by zero-knowledge proofs.

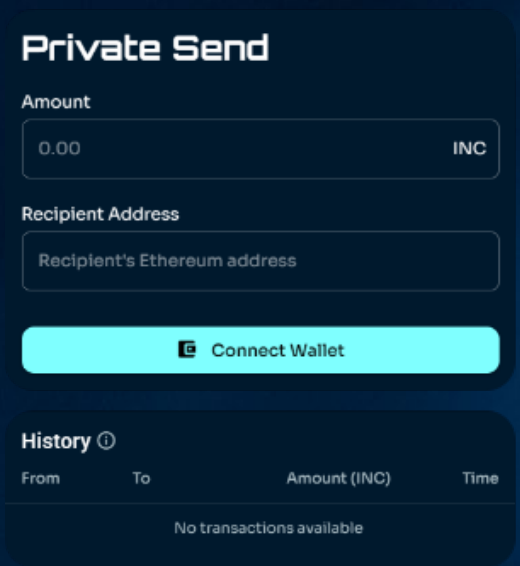
6. Core Features & Transaction Lifecycle

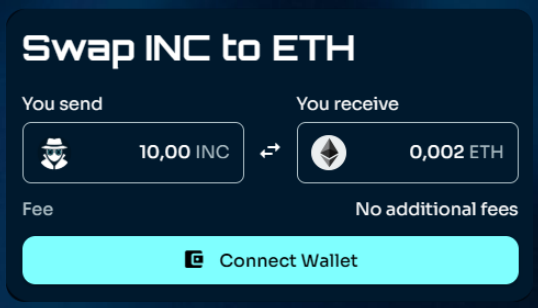
Targeted for Q1 2026 activation:

- Private Deposit → Shielded pool
- Private Send → Encrypted INC transfers
- Private Withdrawal → Nullifier-protected
- Gasless Swap → INC → ETH (small capped amount with a market-based discount)

Planned transaction flow (non-custodial, typically <1 minute):

1. 1Client-side ZK proof generation
2. Encrypted secret upload to IPFS (Private Send)
3. On-chain proof verification
4. Relayer submission for gasless execution (if used)



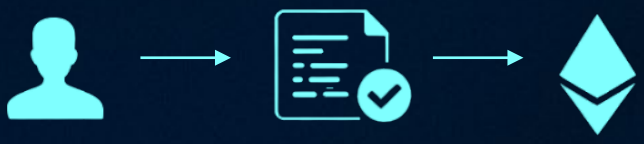


7. Gasless Execution Model

Incognito enables users to acquire small amounts of ETH using $INC:

- Relayer pays gas fees
- Users retain custody at all times
- Value capped with a market discount to prevent arbitrage

This removes the “no ETH in privacy wallet” friction common to Ethereum usage.



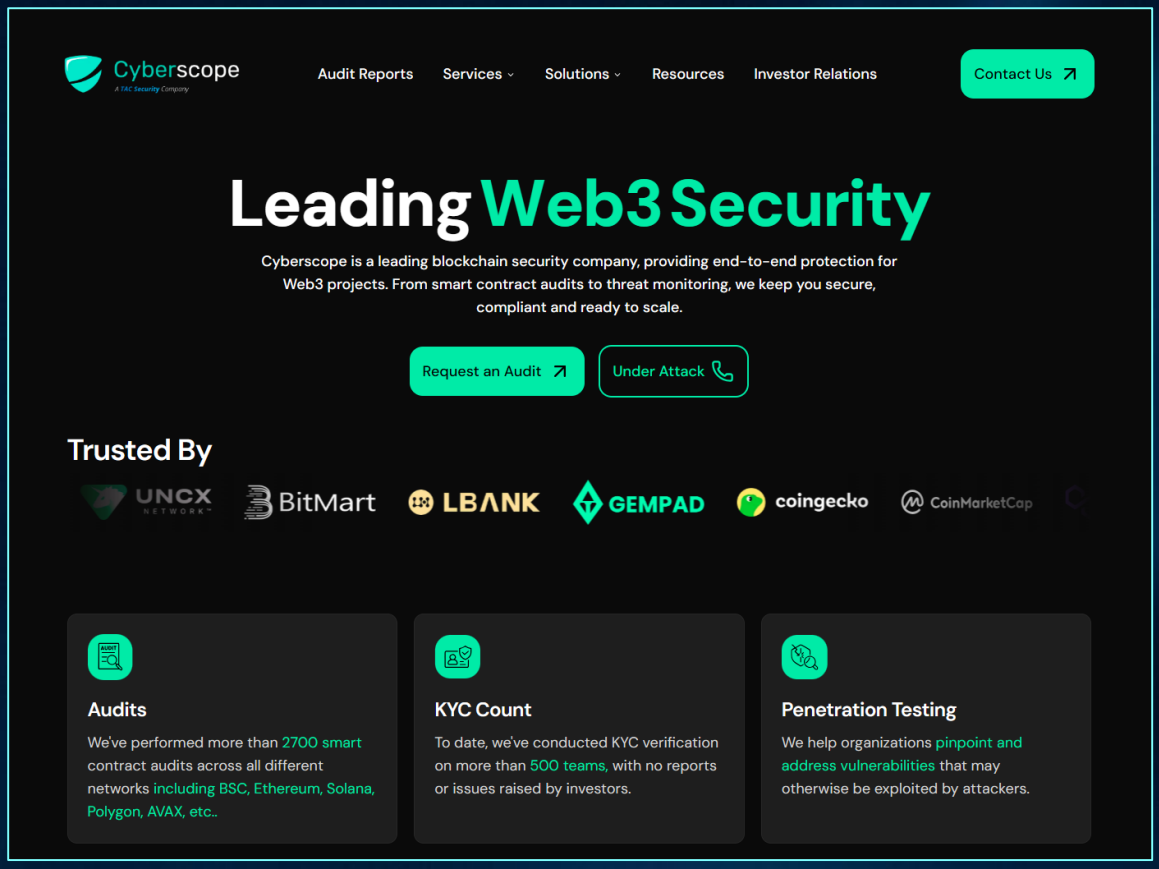
8. Governance & Upgradeability

- Multisig-controlled roles (3-of-5 Admin, Pauser, Upgrader, Swap Manager)
- 48–72 hour time locks on upgrades
- UUPS proxy pattern
- Planned transition to $INC-based governance as the protocol matures

9. Security & Audits

Cyberscope
A TAC Security Company

- Professional smart contract audit completed by Cyberscope.io.
- OpenZeppelin security standards applied
- ReentrancyGuard and Pausable modules
- Fully non-custodial architecture
- Security anchored to Ethereum Mainnet consensus



10. Token Model & Economics

- **Token:** $INC (ERC-20, 18 decimals)
- **Total Supply:** 1,000,000,000 INC (fixed)

Utility:

- Activate privacy-enabled features
- Pay advanced protocol fees
- Participate in future governance

Fees:

- Private INC transfers: gas only
- Future features (BTC, stablecoins, NFTs, messaging): partial burns + team allocation (deflationary)

Tokenomics: (TBC)

Currently in design, focused on sustainability, usage incentives, and deflation. Final parameters will be disclosed prior to governance activation.

11. Roadmap

Timelines are indicative and subject to change based on security review outcomes.

Q1 2026

- Private send
- Deposit
- Withdraw
- Gasless swap (targeted)

Q2 2026

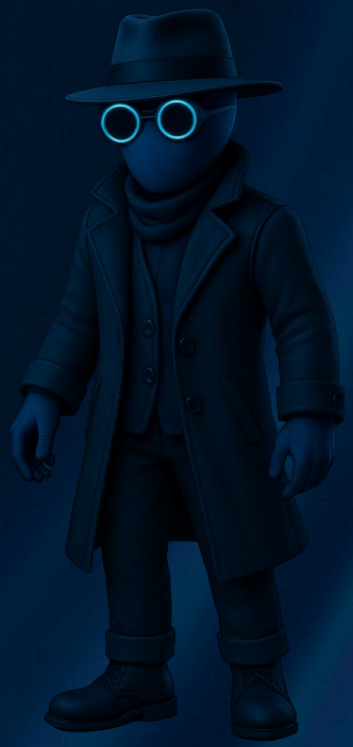
- Incognito Card
- NFTs
- Messaging
- USDT/USDC, ERC-20 Protocol

Q3 2026

- Incognito BTC (private Bitcoin transfers)

All phases are subject to security review and staged deployment.

12. Limitations & Trade-offs



- Focuses on unlinkability, not total invisibility
- Network metadata and timing remain observable
- Anonymity effectiveness grows with adoption
- ZK computation introduces additional gas costs

13. Conclusion

Ethereum excels at transparency and composability.

Incognito EVM completes it with scalable, on-chain privacy.

By making discretion a built-in primitive, Incognito empowers individuals, DAOs, and institutions to transact confidently, without leaving the ecosystem that defines Web3.

Privacy is no longer an edge case.

It is essential infrastructure.

Incognito makes it native.