Copy

Introduction

1.1 Evolution and Current Status of Blockchain Privacy

Since the birth of Bitcoin, blockchain technology has experienced explosive growth. From Bitcoin's peer-to-peer electronic cash system to Ethereum's Turing-complete smart contract platform, decentralized ledgers have not only reshaped the concept of money but are also reshaping the global financial system. However, this transparent ledger characteristic, while bringing trust, has also become an obstacle to large-scale adoption. Under the existing public blockchain architecture, the details of every transaction, the balance of every account, and the circulation path of every NFT can be viewed and tracked by anyone without any barriers.

For individual users, this means complete exposure of their financial situation; for businesses, it means the leakage of trade secrets such as supply chain relationships and cash flow; for institutions, it means that their trading strategies can be easily detected by competitors through on-chain data analysis.

Existing privacy solutions attempt to address this issue, but often fall short in some aspects:

Archived copy · cryp2nova.com

- Privacy public blockchain
  Platforms like Zcash and Monero employ ZK-SNARKs or ring signature technology, offering extremely strong privacy protection. However, most of them do not support smart contracts, or only support very limited scripting functionality, making them unable to run complex DeFi applications. This results in privacy assets failing to generate returns, becoming "Dead Money".
- Privacy smart contracts
  Examples include Secret Network and EVM-based mixers. The former often requires learning a new programming language (such as Rust), disconnecting from the vast EVM developer ecosystem; the latter, like Tornado Cash, while running on Ethereum, only supports fixed-denomination deposits and withdrawals, and due to a lack of compliance measures, easily becomes a breeding ground for illicit funds, leading to severe sanctions from regulatory agencies 1.
- Layer 2 privacy solution
  Privacy layers based on Rollups, such as Aztec, utilize the security of L1. However, users migrating assets between L1 and L2 face the risks and delays associated with cross-chain bridges, and L2 liquidity is often fragmented, unable to directly interact with blue-chip DeFi protocols on L1.

1.2 Industry Pain Points and Problem Statement

Through in-depth market research and technical analysis, we have identified three core pain points in the current Web3 privacy field, which are precisely the problems that Anubis was designed to solve:

- EVM ecological isolation
  Most privacy-focused public blockchains employ custom virtual machines and programming languages. This means that the massive amounts of smart contract code, development tools (such as Hardhat, Foundry, and Remix), and security auditing experience accumulated in the Ethereum ecosystem cannot be reused. Developers need to relearn complex circuit programming languages (such as Circom and Leo), which significantly raises the barrier to entry for developing privacy applications. Therefore, there are high migration costs for developers and slow ecosystem development.

Archived copy · cryp2nova.com

- The "All or Nothing" dilemma of privacy
  Traditional privacy transactions encrypt all information (sender, recipient, amount, asset type). This completely black-box model leads to a serious consequence: DeFi protocols lose composability. For example, an Automated Market Maker (AMM) needs to know the token balances in the liquidity pool to calculate slippage and price. If all balances are hidden, the AMM algorithm cannot function. Therefore, DeFi protocols are unable to analyze transaction data and calculate key metrics such as TVL and trading volume, thus hindering the development of financial applications.
- Privacy paradox of contract interaction
  Users face a dilemma when interacting with smart contracts: either complete transparency, exposing counterparties, amounts, and strategies; or complete privacy, but the contract cannot verify the validity of the transaction and therefore cannot be executed. Existing systems struggle to find a balance between "hiding user identity" and "exposing contract logic". Currently, there is a lack of a mechanism that allows contracts to execute public logic while protecting the privacy of the caller's identity.

1.3 Anubis' Vision and Solutions

Anubis proposes a novel "Selective Privacy" architecture. The core idea of this architecture is to treat privacy as a programmable attribute, rather than a network-wide mandatory default state.

- Publicly visible state attributes
  Smart contract address, transaction type, transaction amount
- Privacy protection status attribute
  Sender address, receiver address, user balance

By integrating zero-knowledge proof verification and dual-ledger synchronization mechanisms at the protocol layer, Anubis achieves the following goals:

- DEX trading volume can be statistically analyzed
  The types and amounts of assets traded can be (selectively) disclosed, allowing external observers to verify the trading volume and depth of the DEX, thus maintaining market transparency and credibility.

Archived copy · cryp2nova.com

- Contract auditable
  The code and state transition logic of smart contracts are public, and anyone can verify that the contract has no backdoors.
- Users cannot be tracked
  Although macro data is publicly available, the identity of the transaction initiator is completely cut off from the on-chain history through stealth addresses and zero-knowledge proofs. No third party (unless they have the view key) can associate the transaction with a specific user.
- Meeting regulatory requirements
  Through the built-in compliance interface, users can present view keys or compliance certificates to regulatory agencies, meeting anti-money laundering compliance requirements while protecting their privacy.

Next
Design Goals and Principles

Last updated 5 months ago

Archived copy · cryp2nova.com