near/dev/hub

Understanding Chain Abstraction

Introduction

Chain Abstraction was designed to enhance the user experience on NEAR by streamlining interactions across multiple blockchains. It simplifies the complexities of dealing with multiple blockchains. By enabling NEAR account holders to execute transactions on other chains without needing several private keys (i.e., one per blockchain) and facilitating easy payment for cross-chain transactions with NEAR tokens, Chain Abstraction offers a seamless and user-friendly approach to blockchain interoperability. Whether you're looking to execute transactions on Ethereum or purchase digital collectibles, these components ensure the process is straightforward and accessible, even for those with limited technical expertise.

High-level

- Chain Signatures: Enable NEAR accounts to sign transactions on other chains without multiple private keys using a multi-party computation (MPC) network.

  Example: *a NEAR account can operate Ethereum transactions without needing an Ethereum private key.*

- Intent Relayers: Simplify paying for transactions on other chains using NEAR, removing the need for users to manage different tokens or understand complex cross-chain transactions.

  Example: a user pays in NEAR to buy an NFT on Ethereum; the system handles the conversion and cross-chain transaction seamlessly.

Chain Signatures and Intent Relayers

Now, let’s take a quick look at the two main components of Chain Abstraction, Chain Signatures, and Intent Relayers:

Chain Signatures allow NEAR users to sign off on transactions on different blockchains without having separate private keys for each blockchain. For example, if you have a NEAR account, you can carry out transactions on the Ethereum blockchain without needing an Ethereum

private key. This is done through a system (called a multi-party computation network) where multiple parties work together to perform a task without sharing their private data.

Intent Relayers make paying for transactions on other blockchains easier for users using their NEAR tokens. This means users don't have to hold different types of tokens or understand the technical details of making transactions across different blockchains. For instance, if you want to buy a digital collectible (NFT) on the Ethereum blockchain, you can pay with NEAR, and the system will automatically convert NEAR to the necessary currency and complete the transaction for you.

More In-Depth Terminology

Relayers:

Covering gas fees

- Allowing users to start using a dApp without acquiring funds is a powerful tool to increase user adoption. NEAR Protocol provides a service enabling developers to subsidize their users' gas fees.
- This concept, known as "Account Abstraction" in other chains, is a built-in feature in NEAR. Users can wrap transactions in messages known as meta-transactions that any other account can relay to the network.
- On NEAR, the relayers simply attach NEAR to cover gas fees and pass the transaction to the network. There, the transaction is executed as if the user had sent it.

Multi-chain signatures:

One account, multiple chains

- Currently, users and applications are siloed in different chains. This means a user needs to create a new account for each chain they want to use. This is cumbersome for the user and the developer, who needs to maintain different codebases for each chain.
- NEAR Protocol provides a multi-chain signature service that allows users to use their NEAR Account to sign transactions in other chains. Users can use the same account to interact with Ethereum, Binance Smart Chain, Avalanche, and NEAR.
    - You don't trade tokens across chains, you trade accounts holding tokens. Smart contracts hold keys using the MPC service, those keys hold accounts on other chains. Smart contracts can swap ownership of those keys as easily as you'd swap an NFT.
- Multi-chain signatures combine smart contracts that produce signatures, with indexers that listen for these signatures and relayers that submit the transactions to other networks. This allows users to hold assets and use applications in any network, only needing a single NEAR account.
    - The indexer isn’t required, as the signature is returned on-chain. Though certainly most apps will use it.

Developer takeaways

- Simplified Onboarding: NEAR Account aims to streamline user onboarding and account recovery processes, reducing friction for new users.
- Cross-Blockchain Transactions: Chain Signatures facilitate executing transactions across blockchains, minimizing the need to manage multiple keys.
- Unified User Experience: Account Aggregation seeks to defragment the Web3 experience, enabling smoother transitions across networks or applications.
- Intent Relayers: This feature allows the execution of user intents on various chains, enhancing interoperability.
- Testnet Launch: The new features are scheduled to debut on the NEAR testnet by early March 2024, indicating a timeline for developers to prepare for integration and testing.
- In the case of the **multi-chain relayer** there will be a paymaster account on ETH that will deposit funds to the users' ETH address. The user would pay in NEAR or a NEAR FT (e.g $SWT) for gas

Real-life Examples

- Bridgeless cross-chain DeFi
    - No minting/burning of assets
    - No message passing between chains
- Defi on Bitcoin (and other non-smart contract chains)
- Multichain account abstraction with gas relayers
- Trust minimized bridges between Ethereum and non-smart contract chains
    - Requires a one-way bridge between NEAR and the non-smart contract chain
    - So NEAR can see when assets were deposited
    - All bridge requests go through NEAR
    - Uses Rainbow Bridge to verify Ethereum state (doesn’t need to go the other way)