Programmable Wallets

Suggest Edits

Circle built Programmable Wallets on top of multi-party computation (MPC) technology to provide a comprehensive developer solution to store and interact with cryptocurrencies. That includes stablecoins, NFTs, and other ERC20, ERC721, and ERC1155 tokens.

As a developer, you can decide whether you or your users manage asset infrastructure. Circle provides a one-stop-shop experience with all the tools and services to handle the complexity of security, transaction monitoring, account recovery flows, and more.

What is a Wallet?

Within the crypto world, a “wallet” refers to any solution that allows users to store, send, receive, and spend digital assets, whether the wallet exists in software (a program or service) or hardware (a device or physical medium). A wallet doesn’t store digital assets. It stores the private keys to access those coins, which exist on public blockchain networks.

Problems with Wallets

Currently, the broad range of wallet solutions over various blockchain networks make it harder for developers to deliver a seamless, consistent wallet experience. Other solutions have each have their own latency, error rate, and native tokens for gas.

Wallet solutions have faced uphill battles with complex and difficult onboarding issues for mass adoption and scalability of Web3 apps:

- Unfamiliar authentication methods for handling private keys.
- Cumbersome approaches to gas fee management for transactions.
- Opaque debugging for failed transactions.
- High complexity for integrating apps with smart contracts.
- Developers must maintain the security of a user’s private keys amidst multiple vendors and offerings.
- No single end-to-end solution available to help them build in Web3.

What is MPC Technology?

Multi-party computation (MPC) is the next-generation cryptographic solution to multi-signature. MPC manages private keys by distributing key shards across multiple parties, securing against accidental or intentional acts to misuse private keys.

Circle’s Solution

Circle Programmable Wallets is a Wallet as a Service that simplifies creating and managing secure web3 wallets and their private keys. They extend wallet functionality with approachable user flows, provide optionality for developer and user infrastructure solutions and enable seamless smart contract integration.

Developers can interact with Programmable Wallets using RESTful APIs.Circle offers Web SDK and Mobile-ready SDKs for Android and iOS for user-controlled wallets, ensuring users have full control over their wallets. Updated16 days ago

What’s Next

- Infrastructure Models
- Table of Contents