modulo.so

secure, frictionless, programmable non-custodial wallet infrastructure

@aaronqli

polymorpher

modulo.so

OTP Wallet

+   One-Time Password Auth

+   Air-gapped Security

+   Keyless Recovery

polymorpher/one-wallet

~~seed phrases~~

~~private keys~~
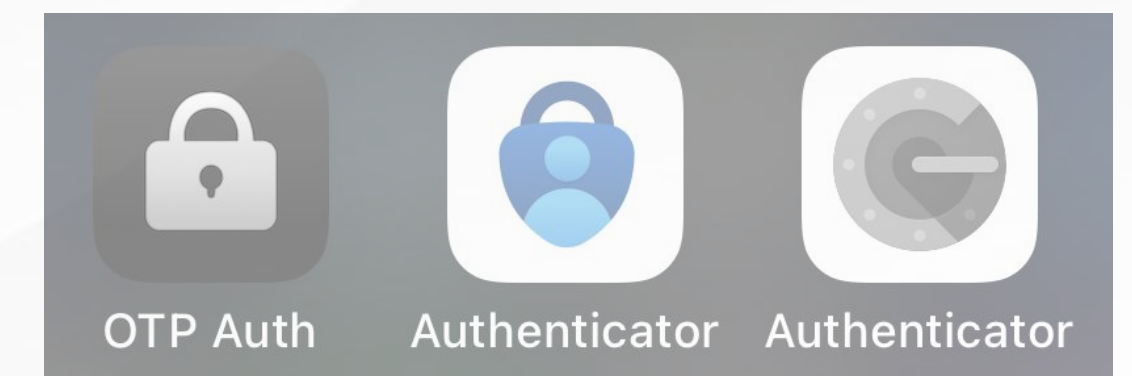
~~single point of failure~~

modulo.so

One-Time-Password Authentication

6-digit code every **30 seconds**

200 212

10-second setup using standard apps

OTP Auth   Authenticator   Authenticator

5-second per wallet operation end-to-end*

* assuming operating on fast underlying blockchain network, such as various POS EVM chains and Layer 2

modulo.so

Air-gapped Security

Offline auth code generation with sealed setup seed

Resilient to attacks in unsafe client environment

Secure against replay, side-channel, front-running

* assuming operating on fast underlying blockchain network, such as various POS EVM chains and Layer 2

modulo.so

Keyless Recovery

Restore wallet anywhere with only auth codes

Recover assets from client to pre-configured wallet

Social recovery without client from any wallet

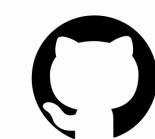* assuming operating on fast underlying blockchain network, such as various POS EVM chains and Layer 2

modulo.so

SMS Wallet

+ Non-custodial

+ Create or recover with SMS

+ SMS controlled mini-wallet

polymorpher/sms-wallet

modulo.so

Signup in 10 seconds

1. Scan signup QR code (open mobile browser)

2. Verify phone number with SMS

3. Save recovery QR code (or use password manager)

Recover wallet in 10 seconds

1. Scan recovery QR code (or load via password manager)

2. Verify phone number with SMS

modulo.so

SMS controlled mini-wallet

A hot wallet entirely controlled by user's SMS

Deposits into server operated smart contract

User pre-authorizes asset spend limit / destination

modulo.so

	Friction	Security	Target Asset Vol
SMS Wallet	Minimal	High[1]	Low*
OTP Wallet	Low	Very High[2]	Flexible

* SMS Wallet users can off-ramp to OTP Wallet

1. key protected by mobile browser sandbox; can also operate in 2FA mode and require SMS validation for each transaction

2. keyless; 2FA by default (browser + authenticator); may extend and operate in MFA modes

modulo.so

	Cost	Target Use Case	Build Time
SMS Wallet	$ - $$	Simple	days
OTP Wallet	$$ - $$$$	Sophisticated	weeks

modulo.so

	MFA	TOTP Auth	SMS	Smart Contract	Recovery	Customization
SMS Wallet	1-2		x		phone	full
OTP Wallet	x	x		x	multiple	full
Sequence			partial		key only	partial
Argent	x		partial	x	multiple	none
Magic			x		ph. / email	limited
MetaMask					none	none
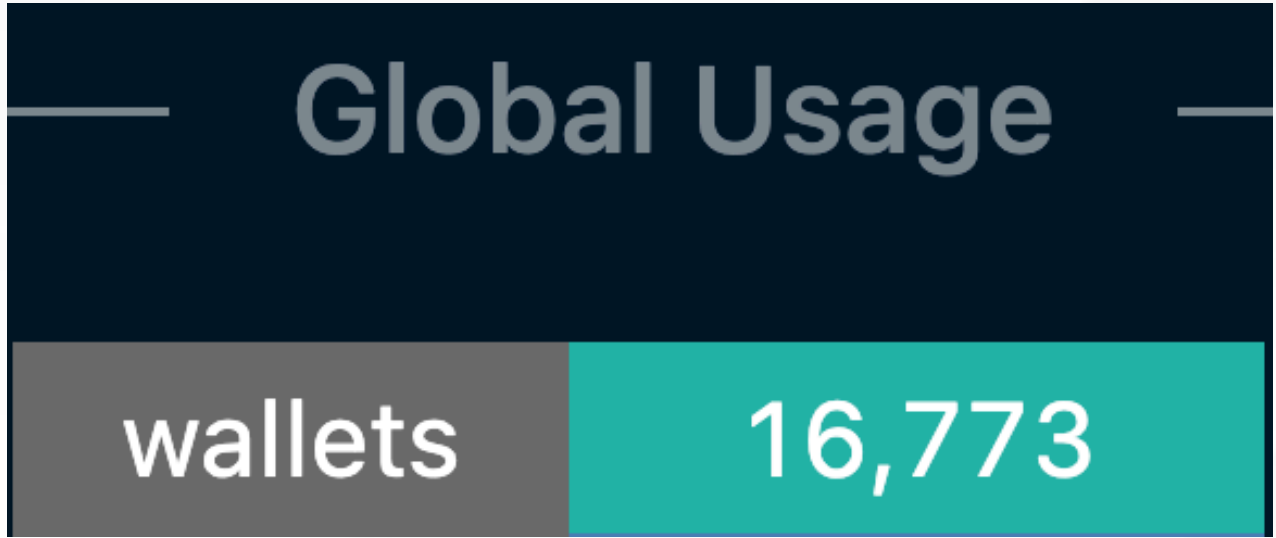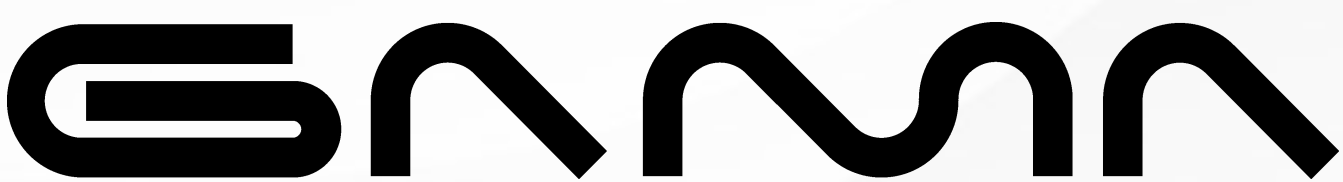
modulo.so

hello@modulo.so

📔 modulo.so/chat

✈️ @modulo_so