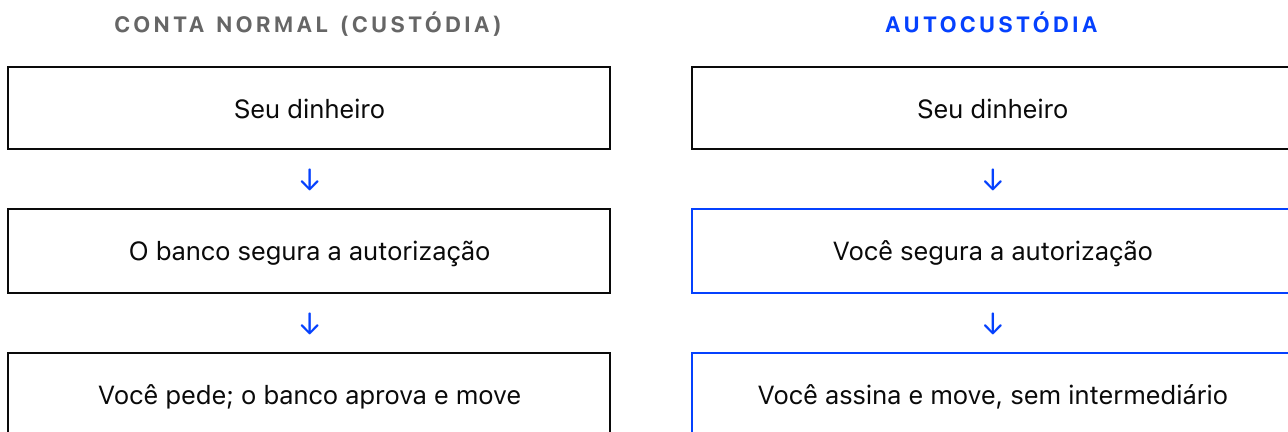


Autocustódia e smart wallet: como o modelo funciona

O que muda quando a autorização de mover o dinheiro passa do banco para o usuário — e por que a infraestrutura por trás disso é software, não custódia.

01 O modelo em uma frase

Numa conta normal, o seu saldo é uma linha na base de dados do banco — e quem manda na linha é o banco. Na autocustódia, o saldo é um registro numa blockchain pública, e quem manda é quem tem a autorização para movê-lo. Autocustódia é você segurar essa autorização, em vez do banco.



Fluxo 1 — A diferença é quem segura a autorização.

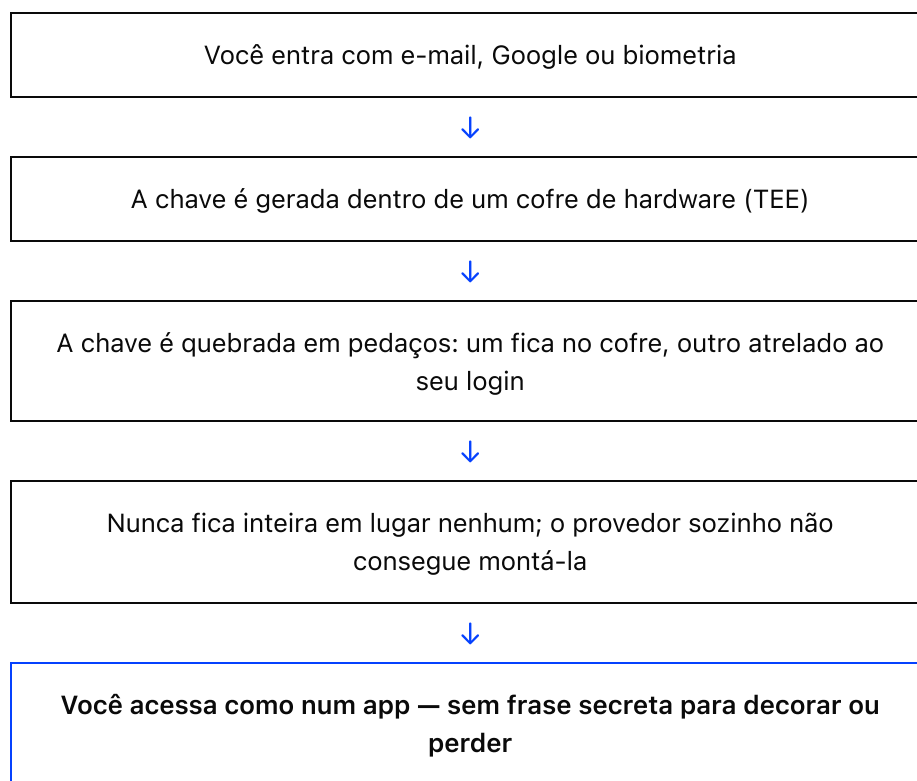
02 A peça central: a chave e a assinatura

Toda carteira tem um par: a **chave pública** (o endereço, como o número da conta — pode compartilhar) e a **chave privada** (a autorização para gastar — tem que ser secreta). Movimentar fundos é assinar uma ordem com a chave privada. Quem tem a chave, controla o ativo.

Conta custodial	A chave fica com a instituição (banco, corretora). Você pede, ela assina.
Autocustódia	A chave é sua. Você assina, sem intermediário.

03 Sem frase secreta: como a chave é protegida

No modelo antigo, ser dono da chave significava guardar uma frase de 12 palavras (a *seed*). Perdeu a frase, perdeu tudo. O Privy resolve isso sem seed phrase:



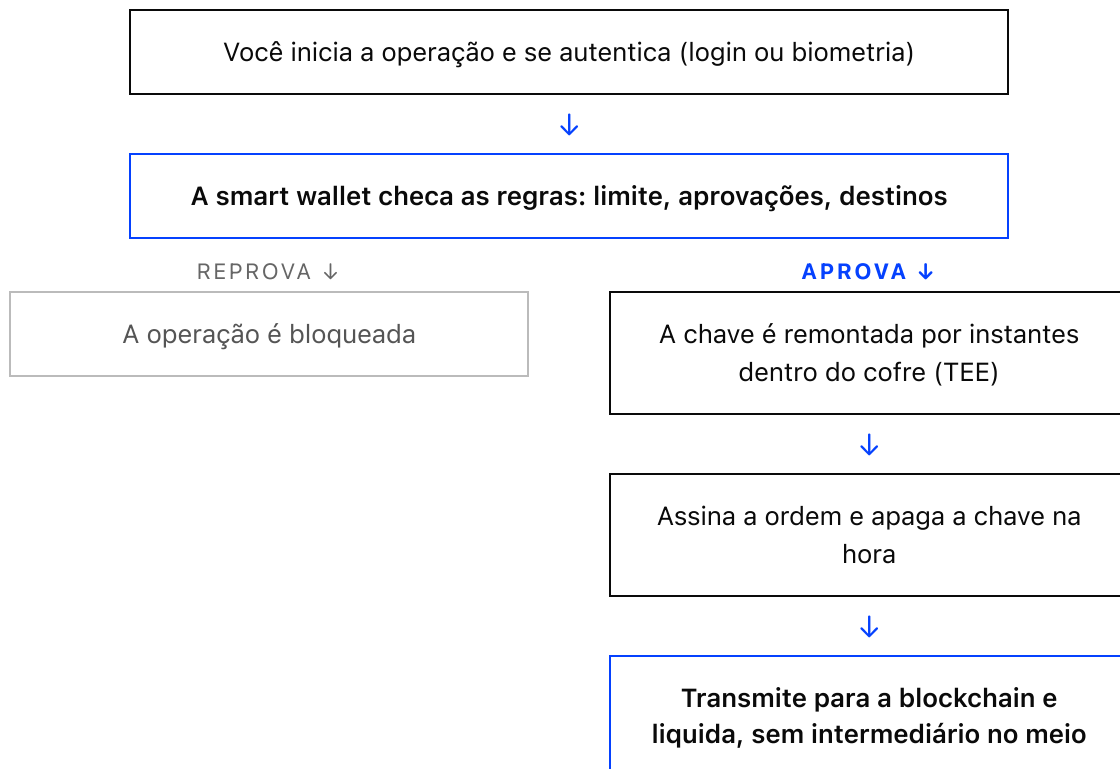
Fluxo 2 — Proteção da chave sem seed phrase.

04 O que é uma smart wallet

Existem dois tipos de carteira. A simples (EOA) é só um par de chaves — faz o básico. A **smart wallet** é um contrato inteligente, um programa na blockchain, o que permite programar o comportamento da conta:

Recuperação sem seed	Perdeu o dispositivo? Recupera o acesso por regras definidas, sem perder os fundos.
Regras de gasto	Limite diário, dupla aprovação acima de um valor, lista de destinos permitidos.
Patrocínio de taxa	Pagar a taxa de rede em stablecoin — ou outra parte paga por você (paymaster).
Chaves de sessão	Autorizar um app a agir de forma limitada, por um tempo, sem dar acesso total.
Operações em lote	Várias ações executadas numa transação só.

05 O caminho de uma transação



Fluxo 3 — Da autenticação à liquidação on-chain.

06 Conta normal × smart wallet autocustodial

	Conta bancária normal	Smart wallet autocustodial
Onde está o saldo	Base de dados privada do banco	Registro numa blockchain pública
Quem move o dinheiro	O banco	Você (login + cofre de hardware)
Como a ordem é validada	O banco aprova internamente	Assinatura criptográfica + regras do contrato
Onde fica o ativo	No balanço do banco	Fora do balanço de qualquer um; é seu on-chain
Recuperar acesso	Central do banco	Regras da smart wallet, sem seed phrase
Programabilidade	O que o banco oferecer	Regras no próprio contrato da carteira
Se o intermediário quebra	Seu dinheiro fica preso	Seus ativos continuam seus

07 Quem é o Privy: a infra por trás da carteira

O Privy é a infraestrutura de carteira que roda por baixo. Fundado em 2021 em Nova York por Henri Stern (ex-Protocol Labs/Filecoin) e Asta Li, levantou cerca de US\$ 40 milhões com fundos como Sequoia, Paradigm, Ribbit e Coinbase. Roda mais de 75 milhões de contas em mais de 1.000 times de desenvolvedores, com clientes como OpenSea e Hyperliquid.

Em junho de 2025, foi comprado pela **Stripe**, uma das maiores empresas de pagamento do mundo — que também comprou a Bridge, de stablecoins, por US\$ 1,1 bilhão. O Privy segue como produto independente dentro da Stripe. A infra que sustenta a carteira está debaixo de uma gigante de pagamentos, não de uma startup solta.

2021	~US\$ 40M	75M+	1.000+	jun/2025
FUNDAÇÃO	LEVANTADOS	CONTAS	TIMES DEV	AQUISIÇÃO STRIPE

08 O lado jurídico: é software, não empresa de ativos virtuais

A Lei 14.478/2022 (Marco Legal dos Criptoativos), no art. 5º, define prestadora de serviços de ativos virtuais (PSAV/VASP) como quem executa, **em nome de terceiros**, serviços como trocar, transferir ou custodiar ativos. O Privy não faz nada disso em nome de ninguém: quem assina é o usuário, e o software não guarda o ativo. Falta o elemento central da lei — logo, o Privy não é PSAV. É software de tecnologia. É a diferença entre quem fabrica o cofre e o banco que guarda o dinheiro dentro dele: só o segundo é regulado como custodiante.

O Privy executa a operação (troca, transferência) em nome de terceiro?

NÃO ↓

O Privy guarda ou controla o ativo do cliente?

NÃO ↓

**Logo, não é PSAV (Lei 14.478/2022, art. 5º).
É software de tecnologia.**

Fluxo 4 — PSAV é quem executa ou custodia em nome de terceiro. Aqui, quem executa é o próprio usuário.

09 Em resumo

Autocustódia é trocar “confiar que uma instituição guarda e libera meu dinheiro” por “eu seguro a autorização para mover o meu dinheiro”. A smart wallet e a infra do Privy fazem isso funcionar com a facilidade de um app — login, recuperação, regras — sem a parte assustadora da seed phrase e sem tirar de você o controle. E, por ser só ferramenta, o Privy fica fora do perímetro da lei de ativos como PSAV.

Fontes: Lei 14.478/2022, art. 5º · Documentação de segurança do Privy (TEE + key sharding) · Anúncio da aquisição pela Stripe (jun/2025).