1 — Openfort*

Fundamentos / Tecnologias
Plataforma de infraestrutura para *account abstraction* e criação de wallets para jogos/apps; oferece SDKs open-source que permitem onboarding com métodos Web2 (Google, email) e gestão de contas sem expor chaves privadas.

Arquitetura
SDKs + backend para orquestração de transações (paymasters / gas relaying), camadas de conta (smart contract accounts) e integração com diversos provedores RPC. Permite a delegação do pagamento de gas e multisign/relayers no backend.

Produtos / Serviços (Business)
Open-source SDKs para developers, infra para account abstraction (WaaS-ish), exemplos para jogos que querem login via Web2. Monetização via planos enterprise / suporte e serviços gerenciados.

Segurança / Compliance
Código auditável (open-source) e ênfase em reduzir *vendor lock-in*. Risco: responsabilidade do integrador ao operar relayers/serviços custodiais auxiliares.

Análise Técnica / Estratégica
Ótimo para produtos que precisam de UX Web2-to-Web3. Ajuda adoção, mas cria dependência do provedor (relayers/infra) se não for bem desenhado.

---

2 — MetaMask

Fundamentos / Tecnologias
Carteira EVM líder — extensão de navegador + app móvel; usa HD wallets (Hierarchical Deterministic), provider JSON-RPC, e extensões (Snaps) para estender funcionalidades. Suporta integração com Infura/Alchemy/otros.

Arquitetura
Client-side (extensão/app) que guarda chave no device; expõe `window.ethereum` / provider; backend leve para downloads/ops. Snaps permite execução de mini-apps isolados dentro da extensão.

Produtos / Serviços (Business)
Extensão, mobile, MetaMask Institutional (solução para clientes institucionais), Snaps (ecossistema extensível). Monetização por serviços institucionais e parcerias.

Segurança / Compliance
Chaves armazenadas localmente;

riscos: phishing, extensões maliciosas e erros do usuário. Snaps introduzem novo vetor, mas são sandboxed;
recomendações: auditorias e boas práticas UX.

Análise Técnica / Estratégica
Padrão de fato para EVM UX — forte adoção, grande base de usuários e ecossistema de devs; competição cresce com AA, mas MetaMask continua essencial para compatibilidade.

---

3 — BingX Exchange*

Fundamentos / Tecnologias
Carteira ligada à exchange BingX — oferece tanto serviços *custodial* (carteira da exchange) quanto conteúdos sobre self-custody; foco em integração com produtos de trading.

Arquitetura
Modelo híbrido: infra exchange (custodial hot wallets centralizados) para negociação rápida; materiais e guias para usuários sobre self-custody e transferências on-chain.

Produtos / Serviços (Business)
Carteira de exchange (custódia) + materiais educativos; serviços integrados de trade, staking e produtos financeiros da plataforma.

Segurança / Compliance
Práticas típicas de CEX: fundos em cold/hot wallets geridos centralmente, políticas de proof-of-reserves e mecanismos internos de risco; usuários expõem chave à exchange enquanto estiverem em saldo custodial.

Análise Técnica / Estratégica
Boa experiência para traders (liquidez/velocidade), mas risco de custódia centralizada. Recomendado nicho: usuários que priorizam conveniência e trade ativo.

---

4 — Rainbow Wallet

Fundamentos / Tecnologias
Carteira mobile/extension focada em Ethereum com design-first UX; vem adotando *smart wallet* / account abstraction e integrações sociais/design modernas.

Arquitetura
Mobile + extensão; integra provider WalletConnect e APIs de indexação; camadas para swaps, token pages e integração com infra de AA quando aplicável.

Produtos / Serviços (Business)
App mobile/extensão com UX para NFTs, swaps, token discovery; foco em consumidor retail, integração com provedores de liquidez, **acompanhamento de carteiras de terceiros**.

Segurança / Compliance
Chaves no device (non-custodial); foco em prevenção UX contra phishing e assinatura consciente; recursos de social recovery / smart wallets em roadmap/implementação. X

Análise Técnica / Estratégica
Ótima experiência para usuários Ethereum-first; aposta em design e features modernas para competir com MetaMask móvel.

---

5 — Zengo

Fundamentos / Tecnologias
“Keyless Wallet” baseada em MPC/threshold cryptography — divide responsabilidades de chaves entre múltiplas partes para evitar um único ponto de falha.

Arquitetura
MPC backend + cliente móvel; as operações de assinatura são realizadas de forma distribuída entre servidores sem reconstruir chave completa no device. Oferece SDKs e API para integração.

Produtos / Serviços (Business)
App móvel com onboarding simplificado; oferta para consumidores e integração enterprise (MPC as a service). Modelo focado em reduzir risco humano (backup, recuperação).

Segurança / Compliance
MPC reduz risco de perda/exfiltração de chave; requer confiança nas implementações/provedores MPC e auditorias criptográficas regulares.

Análise Técnica / Estratégica
Muito atrativo para usuários que querem segurança alta sem complexidade de seed phrases; bom fit para empresas e usuários mass market que valorizam recuperação e UX.

*Multi chain

---

6 — Rabby Wallet

Fundamentos / Tecnologias
Extensão de navegador e wallet para EVM com foco explícito em segurança para DeFi: simulação de transações, pré-visualização de balanço e controle de permissões.

Arquitetura
Extensão + possível app companion; integra vários RPCs e ferramentas de simulação (antes do `eth_sendTransaction`) para evitar assinaturas maliciosas.

Produtos / Serviços (Business)
Wallet browser-first para usuários ativos de DeFi, com funcionalidades de segurança e UX que reduzem riscos na interação com contratos. Possivelmente monetização por integrações/parcerias.

Segurança / Compliance
Simulação de transação e prévia de saldo são funcionalidades de prevenção de fraudes e erros; continua exposto a riscos de extensão/exploit se o ambiente do usuário for comprometido.

Análise Técnica / Estratégica
Aposta clara em diferenciação por segurança operacional para traders/usuários DeFi avançados — nicho promissor frente a MetaMask.

---

7 — Phantom Wallet

Fundamentos / Tecnologias
Carteira originalmente focada em Solana (extensão + mobile), hoje multi-chain (Solana, Ethereum, Base, Sui, etc. em expansão). Suporte a tokens, NFTs e integrações Web3 via adapter.

Arquitetura
Extensão + apps móveis; integração direta com nodes/RPCs Solana e outros; UI para NFT management, swaps e cross-chain features (Crosschain Swapper).

Produtos / Serviços (Business)
Wallet consumer com ênfase em UX para Solana;
Funcionalidades: staking, NFT pages, token extensions e ferramentas de desenvolvedor.
Monetização via serviços auxiliares e parcerias.

Segurança / Compliance
Chaves em device (non-custodial); foco em proteção contra phishing e integração com hardware wallets; rápido crescimento de base exige controles contínuos.

Análise Técnica / Estratégica
Líder no ecossistema Solana, agora expandindo multi-chain; forte presença entre usuários de NFTs/jogos.

---

8 — Kraken Wallet

Fundamentos / Tecnologias
Kraken Wallet é a oferta self-custody da exchange Kraken: produto non-custodial separado dos serviços custodiais da exchange, voltado a conectar usuários a DeFi/NFTs.

Arquitetura
App (mobile/desktop) que gerencia chaves localmente para o usuário; integrações com DeFi, NFTs e múltiplas chains; separado do backend de custódia da exchange.

Produtos / Serviços (Business)
Self-custody wallet para usuários Kraken, com multi-wallet management e interface integrada para DeFi/NFTs; parte da estratégia maior da Kraken (expansão de produtos como Krak/P2P).

Segurança / Compliance
Usuário detém chaves — responsabilidade de segurança recai sobre o usuário; Kraken como exchange mantém produtos custodiados separados com controles regulatórios próprios.

Análise Técnica / Estratégica
Permite à Kraken ampliar ecossistema e retenção de usuários oferecendo tanto custódia quanto self-custody; compete com wallets de exchange e soluções non-custodial.

---

9 — Safe (Gnosis Safe)

Fundamentos / Tecnologias
Carteira baseada em smart contracts (multisig) para governança e tesouraria — permite políticas M-of-N, módulos, guards e integração programável.

Arquitetura
Smart contract wallet que substitui EOA por contrato configurável; camada de módulos (extensibilidade), backend para interface e execução de transações com vários signatários.

Produtos / Serviços (Business)
Ferramenta para DAOs, equipes e tesourarias; dashboards, integração com serviços de custódia institucional e módulos de automação.

Segurança / Compliance
Modelo mais seguro para gestão coletiva de ativos (reduz SPOF); código open-source e auditado, com melhores práticas para empresas/DAOs.

Análise Técnica / Estratégica
Padrão para gestão de tesourarias; alto valor em contextos institucionais/DAO, onde governança e controle são críticos.

---

10 — Ready Wallet

Fundamentos / Tecnologias
Smart wallet com foco em UX bancária on-chain (antigo Argent → Ready): smart accounts, 2FA on-chain, modules como paymasters e proteções antifraude.

Arquitetura
Smart contract account + mobile app; incorpora guardrails (fraud protection), social recovery e integrações de pagamento (cartões, cashback no app Ready).

Produtos / Serviços (Business)
Carteira/serviço financeiro on-chain com cartão de gastos, cashback e UX estilo “neobank”, monetização via serviços e planos.

Segurança / Compliance
Smart contracts para recuperação e proteção; combina conveniência (recuperação, suporte humano) com elementos de custódia controlada via esquema descentralizado.

Análise Técnica / Estratégica
Boa proposta para adoção massiva: traz garantias familiares (proteção de fraude, suporte) para usuários que migrariam do mundo tradicional para Web3.

---

11 — Backpack

Fundamentos / Tecnologias
Wallet self-custody com foco em Solana (e crescente multi-chain): extensão + mobile, suporte a NFTs/xNFTs, hardware-wallet connectors e integração com ecossistema Solana.

Arquitetura
Extensão + mobile app; integração com nodes Solana e outros serviços; suporte a xNFTs e ferramentas específicas do ecossistema.

Produtos / Serviços (Business)
Gestão de cripto e NFTs, swaps simples, integração com hardware wallets; foco no público Solana/NFTs.

Segurança / Compliance
Non-custodial, compatível com hardware wallets; riscos usuais de extensão/phishing mitigados por boas práticas de UX.

Análise Técnica / Estratégica
Forte posição em Solana e NFT userbase; competição com Phantom mas com foco em funcionalidades para creators/xNFTs.

---

12 — Portal (Wallet / SDK)

Fundamentos / Tecnologias
Nome “Portal” aparece em múltiplos projetos: existe Portal (iniciativa de infraestrutura cross-chain / gaming) e também soluções de MPC embutidas (Portal SDK) para empresas; foco em integração enterprise e cross-chain.

Arquitetura
SDKs de key management/MPC ou wallet embutida para dapps; infra para mover stablecoins e criar wallets programáveis via APIs. Ideal para infra financeira e empresas que precisam criar wallets em escala.

Produtos / Serviços (Business)
APIs/SDKs para emissão de wallets, movimentação de stablecoins e integração empresarial; orientado a empresas fintech/stablecoin e jogos que precisam de infra de wallet.

Segurança / Compliance
Projetado para uso corporativo, com controles de custódia, auditoria e integração compliance; riscos dependem de como o integrador configura MPC/guardrails.

Análise Técnica / Estratégica
Bom fit para equipes que querem infra wallet pronta (stablecoin ops, users onboarding em massa) sem construir toda stack de key management.

Conceitos importantes:

1. Hierarchical Deterministic Wallet

HD Wallet vem de Hierarchical Deterministic Wallet
É um tipo de carteira criptográfica que:

- Gera todas as chaves privadas e endereços de forma determinística (previsível a partir de uma raiz),
- A partir de uma única seed phrase (palavras mnemônicas),
- Seguindo uma hierarquia padronizada de derivação.

Ou seja:
Com apenas uma seed de 12 ou 24 palavras, você pode gerar infinitos endereços (contas) — sempre na mesma ordem e estrutura.

2. O que é Account Abstraction?

Account Abstraction (AA) é uma evolução no design das blockchains (especialmente Ethereum) que permite que as contas de usuário funcionem como contratos inteligentes — ou seja, programáveis.
Em vez de o usuário depender de uma EOA (Externally Owned Account) com uma chave privada fixa, ele passa a ter uma smart account, que define suas próprias regras para autenticação, autorização e execução de transações.

3. O que é um Paymaster?

Um Paymaster é um contrato inteligente especial dentro do ecossistema ERC-4337 (Account Abstraction) que paga as taxas de gas em nome do usuário.
Em outras palavras:
O Paymaster é o “patrocinador” da transação — ele decide quando e para quem pagar o gas.
Isso permite experiências “gasless”, onde o usuário não precisa ter ETH (ou o token nativo) para interagir com a blockchain.

4. O que é um Relayer?

Um Relayer é um serviço ou nó que envia transações para a blockchain em nome do usuário.
Ele age como um intermediário confiável, pegando uma transação assinada (ou uma UserOperation) e publicando-a on-chain pagando o gas necessário.
Em resumo:
O usuário não envia a transação diretamente — o relayer envia por ele, pagando o gas, e depois pode ser reembolsado ou patrocinado por um Paymaster.

5. O que é MPC?

MPC (Multi-Party Computation), ou Computação Multi-Partidária Segura, é uma técnica criptográfica que permite várias partes cooperarem para realizar um cálculo (como assinar uma transação) sem nunca revelar suas chaves privadas umas às outras. Em termos simples:
Em vez de uma única chave privada armazenada em um local, a chave é dividida em partes (chamadas shares) entre vários participantes.
Nenhum participante isolado consegue gerar uma assinatura ou reconstruir a chave completa

Para refletir:

- Faz sentido ser multi chain?
- Faz sentido permitir multi sign?
- Devemos ter um tratamento específico na própria carteira sobre NFT?
- Vamos usar sed phrase ou keyless?
- Foco em UX, segurança, prevenção de fraude?
- Será plugin, desktop, mobile, outro?
- Faz sentido a função de acompanhar carteira de terceiros?
- Conceito de Account Abstraction faz sentido?
- Teremos integração com sistema off-chain?