

## 1. Venly Wallet

### 1.1. Fundamentos e Tecnologias Utilizadas

A Venly é uma plataforma multi-chain que suporta 14 blockchains EVM e não-EVM. Oferece compatibilidade com os padrões ERC-20, ERC-721 e ERC-1155, e utiliza modelos de custódia e autocustódia, com gerenciamento seguro de chaves privadas via esquemas de compartilhamento secreto (SSS) e criptografia AES-256/RSA-2048. A infraestrutura é hospedada na AWS, com conformidade ISO-27001, SOC 2 Tipo 2 e GDPR.

### 1.2. Arquitetura

A arquitetura da Venly Wallet é composta por três camadas principais:

- **Interface do Usuário (web, mobile, widget):** Permite interação e autenticação via PIN, biometria ou senha.
  - **Backend:** Gerencia carteiras, autenticação, assinatura de transações e comunicação com múltiplas blockchains.
  - **Segurança e infraestrutura:** Inclui criptografia de dados, auditorias externas, monitoramento de vulnerabilidades e logs em nuvem.
- O fluxo geral é: Usuário → API Venly / SDK → Blockchain. A infraestrutura em nuvem (AWS) garante escalabilidade e auditoria contínua.

### 1.3. Produtos e Serviços (Business)

A Venly engloba diversos produtos e modelos de negócio:

- **Wallet as a Service (WaaS):** Integração de carteiras digitais em aplicações Web3.
- **Venly Authenticator:** Aplicativo móvel para autenticação segura de transações.
- **NFT API / Digital Assets:** Criação e gerenciamento de NFTs (ERC-721, ERC-1155).
- **Venly Pay:** Sistema de pagamento fiat-para-crypto e venda de NFTs.
- **Marketplace:** Permite compra e venda de NFTs e ativos digitais.
- **Integrações corporativas:** Voltadas a jogos, e-commerce e programas de fidelidade.

### 1.4. Segurança e Compliance

A Venly aplica padrões de segurança robustos, como criptografia AES-256 e RSA-2048, além de controle de autenticação multifator e auditorias externas (*NonceAudit*, *LeastAuthority*). Possui certificações ISO-27001 e SOC 2 Tipo 2 e está em conformidade com GDPR.

## 1.5. Análise Técnica e Estratégica

- **Pontos Fortes:**
  - APIs prontas reduzem tempo de integração.
  - Segurança e compliance elevadas.
  - Flexibilidade de integração (custodial/non-custodial, multichain).
  - Solução completa para empresas Web3 e marketplaces de NFTs.
- **Desafios Potenciais:**
  - Custódia parcial pode exigir confiança adicional.
  - Adaptação regulatória entre jurisdições.
  - Dependência de infraestrutura de terceiros (AWS).

## 2. Frontier Wallet

### 2.1. Fundamentos / Tecnologias

Wallet não-custodial ("Your keys, Your crypto") que suporta mais de 60 cadeias (multi-chain) para criptomoedas, DeFi, NFTs. Oferece suporte para troca ("swap"), ponte ("bridge"), staking, liquidez, DeFi dentro do próprio app. Provavelmente usa uma arquitetura típica de carteira HD (hierarchical deterministic) + integração com múltiplos nós / RPCs de cadeias, com UI para usuário final. Mencionam pesquisa de conta ("OneBalance / Credible Accounts") como modelo de "account abstraction / rollup" futuro.

### 2.2. Arquitetura

- Front-end móvel (iOS/Android) + extensão de navegador.
- Back-end que coordena conexões de rede, nodes RPC, agregação de dados de portfólio, operações de DeFi.
- Multi-chain node layer: a carteira interage com múltiplas cadeias via RPC/SDK.
- Autonomia de chaves (non-custodial): o usuário tem controle da chave privada (seed phrase).
- Para "bridge/swap", há integração com smart contracts DeFi externos.

### 2.3. Business / Produtos / Serviços

- Carteira multi-cadeia com uma interface "tudo-em-um" para DeFi + NFTs.
- Serviço de tracking de portfólio e agregador DeFi.
- Possivelmente token de utilidade (\$FRONT) para staking e incentivos.
- Modelo para adoção de usuários de DeFi que buscam simplicidade e multi-cadeia.

## 3. Dapp Pocket Wallet

### 3.1. Fundamentos / Tecnologias

Carteira para armazenamento e transferência de ativos virtuais, com acesso a mais de 2.000 dApps. Provavelmente possui um browser de dApps built-in, integração com Web3 e suporte a smart-contracts para yield/DeFi. Pode usar smart contract wallet ou abstração de conta, dado a menção "BLS Wallet Smart Contract Wallets".

### 3.2. Arquitetura

- Mobile app que incorpora browser Web3 ou interface que liga ao ecossistema de dApps.
- Possível uso de "smart contract wallet" (carteira baseada em contrato) para abstração de usuário e segurança (permite recuperação, meta-transações etc.).
- Layer de "bundling user ops" sugerido para reduzir tarifas / simplificar UX.

### 3.3. Business / Produtos / Serviços

- Carteira de consumo com foco em usuários que querem usar dApps, ganhar yields e participar de Web3 sem construir infraestrutura.
- Potencial modelo "SDK/API" para terceiros integrarem carteira ou usar saldo dentro de apps.

## 4. Trust Wallet

### 4.1. Fundamentos / Tecnologias

Carteira móvel não-custodial amplamente usada (parte do ecossistema Binance). Integra browser de dApps embutido, suporte a múltiplas cadeias e tokens padrão, e integração via WalletConnect ou navegador interno. Padrão comum: HD wallet, seed phrase, chave privada mantida pelo usuário, sem custódia centralizada.

### 4.2. Arquitetura

- App cliente que detém a chave privada no dispositivo do usuário.
- Integração com dApps via protocolo como WalletConnect ou in-app browser.
- Backend leve para indexação / visualização de saldo/ativos, mas a lógica de custódia permanece no dispositivo.

### **4.3. Business / Produtos / Serviços**

- Carteira de consumo volumosa, com foco em facilidade de uso para usuários de Web3.
- Integração com exchange e serviços da Binance (possivelmente swap, staking).
- Suporte para DApps, NFTs, multi-cadeia.
- Modelo gratuito para usuários finais, monetização possivelmente via serviços dentro do app.

## **5. Snowflake Wallet**

### **5.1. Fundamentos / Tecnologias**

Específica para plataforma Solana, com foco em multisig (múltiplas assinaturas) para carteiras. Multisig implica arquitetura de controle compartilhado de chave ou assinatura múltipla, aumentando a segurança para grupos/organizações.

### **5.2. Arquitetura**

- Cada carteira requer múltiplas assinaturas para autorizar transações (ex: M-of-N).
- Provavelmente integração com Solana RPC e infraestrutura para gestão de chaves múltiplas, aprovação de transações, interface de gerenciamento de membro/assinante.
- Pode usar módulos on-chain de multisig (smart contracts ou programas Solana) + coordenação de assinaturas off-chain.

### **5.3. Business / Produtos / Serviços**

- Para uso institucional ou grupos de usuários que precisam dividir o controle de carteira (ex: tesouraria de DAO, coletivo de NFTs).
- Valor agregado: segurança reforçada, compartilhamento de controle, visibilidade/controle de quem assina.
- Modelo de negócio: possivelmente gratuito ou assinatura para uso com recursos avançados.

## **6. Goki Wallet**

### **6.1. Fundamentos / Tecnologias**

Também para Solana, focada em "make, control, and check multisig wallets". Multisig requer mecanismos de assinatura múltipla, coordenação entre signatários, possivelmente

integração com carteiras hardware ou módulos de assinatura modular.

## 6.2. Arquitetura

- Voz-modelo parecido com Snowflake: carteira corporativa/organizacional com várias chaves ou parteagens.
- No backend, coordenador de transações, verificação de múltiplas assinaturas antes de emissão on-chain.
- Front-end para gestão de membros, aprovações, estado de assinatura, histórico.

## 6.3. Business / Produtos / Serviços

- Voltado para equipes, DAOs, projetos de Web3 que requerem governança ou tesouraria distribuída.
- Valor oferecido: governança, segurança, controle, visibilidade de transações multi-assinatura.
- Pode oferecer planos pagos ou serviços de suporte para grandes contas.

# 7. Sepior Wallet

## 7.1. Fundamentos / Tecnologias

Sepior é uma "Sepior MPC wallet" que utiliza a tecnologia MPC (Multi-Party Computation). Essa tecnologia distribui partes de chave entre múltiplas entidades/servidores, sem que qualquer parte individual detenha a chave inteira, aumentando a segurança.

## 7.2. Arquitetura

- **Módulo de MPC para geração/distribuição de chaves:** Cada "party" tem um fragmento/parte do segredo e atua para assinar transações sem expor a chave completa.
- **Servidores/coordenador:** Gerenciam o protocolo MPC, verificação de assinaturas e interface para operações.
- **API/SDK:** Para empresas que querem integrar carteira corporativa ou custódia institucional.
- **Integração on-chain:** Para envio/recebimento de ativos por smart contracts ou transações normais.

## 7.3. Business / Produtos / Serviços

- Voltado para usuários institucionais ou custódias que precisam de alta segurança.
- Oferta de carteira "enterprise grade" com MPC, possivelmente em modelo SaaS ou

- licença de uso.
- Pode incluir recuperação de chave, auditoria, integração com KYC/AML se for ambiente institucional.

## 8. Ellipal

### 8.1. Fundamentos / Tecnologias

Ellipal é mais conhecido como hardware wallet ou cold wallet (modelo "Ellipal Titan"). Possui arquitetura air-gapped (sem cabo ou conexão direta) via QR-code ou Bluetooth limitado, para reduzir vetores de ataque. A chave privada é mantida offline, sem contato com a internet (ideal para segurança máxima).

### 8.2. Arquitetura

- Dispositivo físico que gera/armazena a chave privada.
- App companion móvel para visualizar saldos e preparar transações; as transações são assinadas no dispositivo offline e transmitidas via QR-code ou outro canal.
- Infraestrutura de atualização de firmware segura, chip seguro para armazenamento da chave (Secure Element).
- Integração com várias redes/cryptos via firmware + suporte de tokens.

### 8.3. Business / Produtos / Serviços

- Hardware wallet vendida como produto físico.
- App gratuito/companion para interação.
- Receita via venda de dispositivo, acessórios, possivelmente serviços premium ou compatibilidade adicional.
- Mercado de usuários que valorizam segurança máxima (HODLers, investidores de longo prazo).

## 9. D'CENT Wallet

### 9.1. Fundamentos / Tecnologias

Carteira híbrida: hardware + mobile app, com suporte a Bluetooth ou NFC. Suporte multi-cadeia e integração com DeFi, possivelmente Ledger-style, mas mais "acessível".

## 9.2. Arquitetura

- Dispositivo físico para chave privada (biometric feature ou display embutido).
- Aplicativo móvel para interagir, verificar saldos e autorizar transações.
- Comunicação via Bluetooth ou USB entre aparelho e app.
- Backup/recuperação via seed phrase ou outro método seguro.

## 9.3. Business / Produtos / Serviços

- Venda de hardware wallet D'CENT + suporte de software/app.
- Mercado de usuários que querem mais segurança do que um app puro, mas menores barreiras do que instituições.
- Potencial para serviços premium (ex: staking integrado, NFT, carteira corporativa).

# 10. Ronin Wallet

## 10.1. Fundamentos / Tecnologias

Carteira para a rede Ronin Network (side-chain da Ethereum focada em games como Axie Infinity). Suporte para tokens, NFTs (Axies), bridging entre Ethereum e Ronin. Disponível como extensão de navegador + mobile app.

## 10.2. Arquitetura

- Extensão de navegador ou mobile app que conecta ao Ronin RPC.
- Smart contracts para bridging (lock/unlock dos tokens de Ethereum para Ronin).
- Interface para jogos (Axie) com integração de wallet diretamente ao game.
- Potencial modelo de "omnibus" ou "segregated" (depende da infraestrutura do game).

## 10.3. Business / Produtos / Serviços

- Carteira dedicada para o ecossistema de game/web3: armazenar Axies, tokens Ronin, participar de gameFi.
- Facilita transações rápidas e baixas taxas na side-chain Ronin para gamers.
- Valor: UX simples para gamers/web3 newbies; conectividade direta com o jogo.

## 11. SafePal Wallet

### 11.1. Fundamentos / Tecnologias

SafePal oferece hardware wallet (modelo S1) + aplicativo móvel. Comunicação air-gapped ou via QR-code para maior segurança. Suporte multi-cadeia (Ethereum, BSC, etc) no dispositivo.

### 11.2. Arquitetura

- Dispositivo físico com armazenamento seguro da chave privada.
- App companion para interface de usuário e preparação de transações.
- Transmissão de transação assinada via QR ou Bluetooth, sem exposição da chave privada à internet.
- Possível integração com APIs para verificação de saldo, tokens e compatibilidade com dApps.

### 11.3. Business / Produtos / Serviços

- Venda do hardware wallet + app gratuito.
- Acessórios de segurança premium.
- Mercado de usuários focados em segurança (HODLers, entusiastas de cripto).
- Potencial para serviços premium ou clube de membros.

## 12. Qredo Wallet

### 12.1. Introdução

A Qredo Wallet é uma infraestrutura de custódia descentralizada voltada para o mercado institucional. Ela se diferencia por eliminar o uso de chaves privadas tradicionais, substituindo-as por um sistema de Multi-Party Computation (MPC) e consenso descentralizado. Seu objetivo é fornecer segurança de nível bancário, liquidez cross-chain e controle de ativos digitais sem comprometer a soberania do usuário.

### 12.2. Fundamentos e Arquitetura

A Qredo é construída sobre uma arquitetura de blockchain Layer-2, que atua como uma rede de mensagens e liquidação entre carteiras MPC.



- **Camada de Rede (Layer-2 Network):** Utiliza nós validadores independentes que executam a Qredo Network, garantindo integridade e consenso sem a necessidade de custodiante centralizado.
- **Multi-Party Computation (MPC):** O controle de uma carteira Qredo é distribuído entre várias partes. Nenhum nó ou entidade detém a chave completa; as assinaturas são reconstruídas dinamicamente no momento da transação. Isso elimina o risco de perda de chaves privadas ou comprometimento por ataques diretos.
- **Interoperabilidade Cross-chain:** A Qredo permite a movimentação de ativos entre diferentes blockchains (Ethereum, Polygon, Bitcoin, Solana, etc.) com liquidação segura via contratos inteligentes e mensageria criptografada.

### 12.3. Tecnologias Utilizadas

- **Linguagens:** Rust e Go (backend de rede e protocolos de consenso), TypeScript (SDKs e APIs).
- **Protocolos:** Multi-Party Computation (MPC), Threshold Signatures, Tendermint Consensus adaptado.
- **APIs e SDKs:** Fornece APIs REST e SDKs para integração institucional (custódia, trading, auditoria).
- **Camada Criptográfica:** Usa o padrão FROST (Flexible Round-Optimized Schnorr Threshold) para assinaturas seguras e rápidas.

### 12.4. Modelo de Negócio

A Qredo se posiciona como infraestrutura de custódia e liquidez descentralizada B2B. Seus principais produtos e serviços incluem:

- Custódia descentralizada institucional (Qredo Network)
- Qredo Wallet App e Dashboard: Ferramenta de governança e controle de acesso a ativos digitais multiusuário.
- Liquidity Hub: Pool de liquidez que permite transferências e swaps cross-chain sem expor as chaves privadas.
- Qredo API: Integrações com corretoras, custodians e plataformas DeFi/TradFi.
- Governança on-chain (Qredo DAO): Token QRDO é usado para governança e incentivos de rede.

### 12.5. Segurança e Conformidade

A Qredo adota uma abordagem zero-trust e regulatory-grade compliance:

- Custódia descentralizada com MPC.
- Auditorias independentes (Certik, Kudelski).
- Conformidade com regulamentos como MiCA e GDPR.
- Recuperação multiusuário e controle hierárquico (empresarial).

## **12.6. Integrações e Casos de Uso**

- Alchemy Dapp Store: A Qredo está listada como uma das principais soluções de custódia MPC integráveis via API.
- Parceiros institucionais: Fireblocks, MetaMask Institutional, Coinbase Prime.
- Casos de uso: Gestão de tesouraria de DAOs; Custódia de fundos DeFi; Liquidação segura entre blockchains heterogêneos.