ENTREGÁVEL 9- Gestão de API para Exposição de Crypto-Wallets

09/05/2025

Controlo de versões

VERSÃO	DATA	AUTOR(ES)	DESCRIÇÃO	APROVAÇÃO
1.0	**09/05/2025**	**Nuno Barbosa**	**Primeira versão**	**Vera Carvalho**

Índice

1 Introdução

A exposição de produtos através de Interfaces de Programação de Aplicações (APIs) constitui uma prática consolidada no desenvolvimento de soluções digitais escaláveis e interoperáveis. Esta abordagem permite que componentes de software distintos comuniquem entre si de forma programática, assegurando a reutilização de serviços, a normalização de acessos e a integração eficiente com sistemas externos [Fie00; Pap08].

Ao disponibilizar funcionalidades de um produto via API, torna-se possível promover a integração com parceiros, clientes ou sistemas internos, num modelo desacoplado e controlado. Esta estratégia não só reduz a dependência de interfaces manuais como também facilita a automação de processos e a criação de novos canais digitais de distribuição [RS20].

Além disso, o uso de APIs facilita a adoção de arquiteturas modernas, como microserviços, e potencia a escalabilidade horizontal dos sistemas [New15]. Do ponto de vista económico e estratégico, a exposição via API permite a criação de ecossistemas digitais, nos quais terceiros podem desenvolver aplicações complementares, ampliando o valor do produto principal e promovendo a inovação aberta [Cor14; ONe16].

A crescente adoção de ativos digitais e o desenvolvimento da Web3 têm impulsionado a necessidade de soluções de custódia que sejam simultaneamente seguras, interoperáveis e escaláveis. Neste contexto, a exposição programática de funcionalidades de crypto-wallets através de APIs torna-se essencial para assegurar a integração fluida com plataformas descentralizadas, serviços financeiros digitais e mecanismos de identidade soberana [Ant17; WR21].

Ao expor uma crypto-wallet por meio de uma API, é possível desacoplar a camada de apresentação da lógica de custódia, permitindo que múltiplos clientes, aplicações móveis ou sistemas de terceiros interajam com a carteira de forma programática e segura [Gud+20]. Esta abordagem promove a reutilização de serviços críticos, como a assinatura de transações, a gestão de chaves, ou o controlo de permissões de acesso, garantindo simultaneamente a auditabilidade e rastreabilidade das operações [Bon+15].

Além disso, a disponibilização de uma carteira através de API permite acelerar a inovação no ecossistema Web3, uma vez que facilita a criação de integrações com bolsas descentralizadas (DEXs), plataformas de empréstimo, serviços de staking, e mecanismos de autenticação baseados em blockchain. Tal como em outras áreas da computação distribuída, a API atua como um contrato semântico e técnico entre fornecedores e consumidores de serviços, favorecendo a escalabilidade e a evolução modular da solução [Fie00; Pap08].

A exposição programática de crypto-wallets é particularmente relevante em contextos institucionais, nos quais se impõe o cumprimento de requisitos regulatórios, separação de funções e controlos de acesso granulares. Nestes casos, a API funciona também como uma camada de abstração para garantir conformidade com normas de segurança, como o uso de HSMs (Hardware Security Modules) ou técnicas de MPC

(Multi-Party Computation) [BS19; Dig23a].

2 Objetivos

Este entregável é focado na exposição de funcionalidades de uma crypto-wallet fornecida pelo **Porto by Anchorage Digital** através de uma API, com o intuito de promover a interoperabilidade e escalabilidade da solução.

Os objetivos principais incluem:

- **Definição de requisitos**: Identificar e documentar os requisitos funcionais e não funcionais da API, assegurando que atende às necessidades dos utilizadores e às exigências de segurança.
- **Identificar concorrentes**: Analizar os principais concorrentes que disponham desta funcionalidade, como a Fireblocks e BitGo, para compreender as melhores práticas e tendências do mercado.
- **Desafios**: Ir de uma abordagem de custódia custodial para uma abordagem de custódia própria, levanta grandes desafios que expomos neste documento.

3 Requisitos Técnicos para a Exposição Segura de *Cold Crypto-Wallets* via API

A concepção de uma API para carteiras criptográficas armazenadas em ambientes desconectados da rede (designadas cold wallets) exige um conjunto rigoroso de requisitos técnicos, orientados para a preservação da confidencialidade das chaves privadas, a integridade das operações de assinatura e a auditabilidade completa dos acessos. Neste tipo de arquitetura, a API desempenha o papel de intermediário entre o sistema que solicita operações criptográficas e o ambiente fisicamente isolado que as executa. Este desacoplamento deve ser implementado com salvaguardas formais contra fugas de informação, acesso não autorizado e manipulação de transações [Bon+15; BS19; OO19].

3.1 Modelo de Comunicação Assíncrona e *Air-Gapped*

A principal característica de uma cold wallet é a ausência de conectividade permanente à Internet. Por conseguinte, a API exposta ao mundo exterior deve funcionar como um sistema de orquestração assíncrona, onde as mensagens de entrada e saída são armazenadas de forma intercalar em zonas tampão seguras (message queues ou sistemas de persistência auditável). A assinatura de transações, por exemplo, requer extração da mensagem, transporte físico (ex.: USB ou QR code), execução isolada e reimportação do resultado assinado [Gud+20].

Este padrão exige que o backend da API suporte workflows de múltiplos passos, com controlo de estados intermediários e verificação de validade temporal (ex.: validade de nonces, expirabilidade de pedidos). É recomendável o uso de formatos serializáveis portáveis como CBOR ou Protobuf para minimizar ambiguidades na leitura em dispositivos com capacidades reduzidas.

3.2 Separação de Contexto e Mínimo Privilégio

A API deve aplicar o princípio do menor privilégio de forma estrita. Cada token de acesso ou identidade autenticada deve ter acesso unicamente aos endpoints e operações estritamente necessários à sua função. Isto aplica-se tanto à leitura de dados (ex.: saldos, histórico de transações) como a operações críticas (ex.: exportação de chaves públicas, submissão de payloads para assinatura).

Deve existir uma segmentação entre o domínio de controlo e o domínio de execução, com possibilidade de delegação baseada em papéis (RBAC) ou políticas baseadas em atributos (ABAC). A lógica de controlo deve ser desacoplada da execução física, protegendo o módulo de assinatura contra qualquer instrução não validada previamente [ST20].

3.3 Integridade Criptográfica de Mensagens e Operações

Cada solicitação enviada à API deve conter, obrigatoriamente, um identificador único (UUID ou nonce criptográfico) para prevenir ataques de repetição. As mensagens devem ser autenticadas com HMACs ou assinaturas digitais baseadas em esquemas robustos (ex.: Ed25519, secp256k1). As respostas devem igualmente incluir verificação de integridade, idealmente com prova de inclusão em log imutável (Merkle log).

Em ambientes empresariais, recomenda-se a utilização de enclaves de execução segura (ex.: Intel SGX, AMD SEV) como camadas adicionais de verificação interna antes da libertação de resultados para a rede externa [Dig23b; BS19].

3.4 Mecanismos de *Multi-Party Approval*

As operações de alto risco, como a movimentação de ativos, devem estar sujeitas a fluxos de aprovação multiutilizador (*m-of-n*), com suporte nativo na API. Estes fluxos devem permitir a orquestração de diferentes entidades, físicas ou lógicas, com autenticação segregada (ex.: hardware tokens, autenticação biométrica) e capacidade de aprovação assíncrona distribuída geograficamente.

A API deve também permitir políticas condicionais baseadas em lógica temporal ou contextual, tais como: ”requer 3 aprovações fora de horário laboral”, ou ”só aprova se o montante for inferior a 1 BTC” [Bon+15; New15].

3.5 Compatibilidade com Padrões do Ecossistema Blockchain

A compatibilidade com padrões reconhecidos é fundamental para garantir interoperabilidade. A API deve suportar:

Derivação Hierárquica de Chaves conforme BIP-32/BIP-44.

Assinatura de Mensagens Estruturadas conforme EIP-712 para Ethereum e ERC-191 para compatibilidade com contratos inteligentes.

Formatação de Transações conforme JSON-RPC 2.0 e suportes binários como RLP (Ethereum) ou PSBT (Bitcoin).

A adesão a estes padrões permite que a API sirva não apenas como interface para sistemas proprietários, mas como componente interoperável com carteiras de terceiros, auditorias externas e oráculos descentralizados [Fou19; Woo21].

3.6 Monitorização e Auditabilidade Imutável

Todas as interações com a API devem ser registradas com carimbo temporal certificado (ex.: RFC 3161) e armazenadas em estruturas imutáveis (ex.: journaling assinado, Merkle trees com checkpoints). Isto garante não apenas rastreabilidade interna, mas conformidade com requisitos legais (ex.: regulamentos financeiros, normas ISO 27001).

Os logs devem incluir metainformação suficiente para reconstruir sessões, identificar tentativas falhadas de acesso e rastrear modificações em configurações de segurança ou autorizações de utilizadores [ST06].

4 Análise de Concorrência

No contexto de soluções de custódia e integração programática com carteiras de ativos digitais, várias entidades de referência internacional disponibilizam APIs com funcionalidades avançadas. Esta secção apresenta uma análise comparativa de quatro dos principais fornecedores: **Circle**, **Fireblocks**, **Copper** e **BitGo**. A comparação incide sobre critérios técnicos essenciais como arquitetura, segurança, suporte a carteiras frias, mecanismos de aprovação e compatibilidade com standards Web3.

Estas plataformas fornecem serviços que combinam *hot*, *warm* e *cold storage*, com diferentes graus de isolamento físico, integração com módulos de segurança de hardware (HSM) ou computação multipartidária (MPC), e APIs orientadas para o controlo de ativos digitais em ambientes institucionais [Fir23a; Cir23a; Tec23; Inc23].

5 Critérios de Comparação

A Tabela 1 sintetiza as principais características técnicas com impacto direto na decisão de desenho e posicionamento de uma API de carteira fria:

Modelo Criptográfico: tecnologia subjacente à assinatura e proteção das chaves privadas (ex.: MPC, HSM).

Suporte a Carteira Fria: grau de isolamento físico e mecanismos de comunicação com dispositivos air-gapped.

Orquestração Multiutilizador: capacidade da API para configurar políticas de aprovação m-of-n, segregação de funções e fluxos condicionais.

Interoperabilidade Web3: suporte a standards como BIP-32/44, EIP-712, PSBT, JSON-RPC.

Disponibilidade da API: modelo de acesso programático (REST, gRPC), autenticação, e cobertura documental.

6 Análise Detalhada dos Concorrentes

6.0.1 Circle

A Circle oferece uma solução de *Wallet-as-a-Service* que permite a integração de carteiras digitais em aplicações de terceiros. A infraestrutura suporta carteiras controladas pelo utilizador e carteiras de custódia, com funcionalidades de assinatura de transações e gestão de políticas de segurança. A Circle utiliza tecnologia de computação multipartidária MPC para garantir a segurança das chaves privadas, permitindo que estas nunca sejam totalmente expostas durante as operações [Cir23a; Qui23].

Em termos de preços, a Circle adota um modelo baseado em carteiras ativas mensais MAW. As primeiras 1.000 carteiras ativas são gratuitas, sendo cobrados 0,05

Tabela 1: Comparação técnica entre fornecedores de APIs de custódia

Fornecedor	Modelo Criptográfico	Suporte a Carteira Fria	Orquestração Multiutilizador	Interoperabilidade Web3
Circle	HSM + MPC híbrido	Parcial (custódia com confiança em servidores internos)	Sim (policy engine com workflow configurável)	Elevada (suporte a EVM, EIP-712, JSON-RPC)
Fireblocks	MPC (SGX enclaves)	Sim (transações via air-gapped signing)	Sim (aprove com aprovação granular e quorum definido)	Elevada (suporte a BIP-32, EIP-712, PSBT)
Copper	MPC distribuído	Sim (ClearLoop + integração air-gapped)	Sim (admin console e permissões hierárquicas)	Moderada (foco em integração com exchanges)
BitGo	HSM + MPC opcional	Sim (integração com dispositivos offline e storage segregado)	Sim (políticas configuráveis e acesso por grupos)	Moderada (suporte básico a BIP-32, JSON)

dólares por carteira adicional. Existe também uma opção de API de assinatura, com preços diferenciados [Cir23b].

6.0.2 Fireblocks

A Fireblocks fornece uma plataforma de infraestrutura para ativos digitais, oferecendo soluções de custódia, gestão de tesouraria e integração de carteiras. A sua arquitetura baseia-se em tecnologia MPC combinada com enclaves de execução segura (SGX), permitindo a criação de carteiras frias onde a terceira parte da chave MPC é armazenada num dispositivo móvel desconectado da rede. As transações requerem a aprovação através de códigos QR bidirecionais, garantindo que as chaves privadas nunca são expostas online [Fir23a; Fir23b].

A Fireblocks oferece vários planos de preços. O plano básico tem um custo de 250 dólares por mês, permitindo até 100.000 dólares em ativos sob custódia. Planos superiores oferecem maior capacidade e funcionalidades adicionais, com preços que variam conforme as necessidades específicas do cliente [Fir23c].

6.0.3 Copper

A Copper disponibiliza soluções de custódia de ativos digitais, com ênfase na segurança e flexibilidade. A sua tecnologia de carteira fria combina MPC com isolamento físico, permitindo que os clientes personalizem as configurações de armazenamento para cada ativo, escolhendo entre cofres frios, mornos e quentes. Esta abordagem proporciona um equilíbrio entre segurança e acessibilidade, adaptando-se às necessidades específicas de cada cliente [Tec23; Cop23].

As informações detalhadas sobre preços não são publicamente disponibilizadas pela Copper. Recomenda-se o contacto direto com a empresa para obter uma proposta personalizada baseada nas necessidades específicas de cada cliente.

6.0.4 BitGo

A BitGo oferece serviços de custódia qualificada e auto-custódia para ativos digitais, com suporte para carteiras frias. A sua arquitetura de segurança utiliza uma abordagem de múltiplas chaves, onde os clientes controlam duas das três chaves necessárias para autorizar transações, mantendo-as em ambientes offline. As transações são iniciadas e parcialmente assinadas offline, sendo posteriormente carregadas para a BitGo para coassinatura, garantindo que as chaves privadas nunca são expostas online [Inc23; Bit23b].

Em termos de preços, a BitGo aplica uma taxa de 0,25% nas retiradas de ativos baseados em UTXO de carteiras de auto-custódia para contas sem contrato. Não são aplicadas taxas para depósitos ou retiradas dentro da mesma carteira [Bit23a].

7 Considerações Estratégicas

Do ponto de vista arquitetural, todas as soluções analisadas recorrem a técnicas de fragmentação ou isolamento das chaves privadas, mas divergem na forma como expõem estas funcionalidades via API. O modelo da Fireblocks distingue-se pela utilização de enclaves de execução segura (Intel SGX) como base da sua infraestrutura MPC, permitindo operações descentralizadas sem partilha direta de chaves [Fir23a].

A Copper, por sua vez, utiliza o protocolo *ClearLoop* para pré-liquidação segura de transações com custódia isolada, apoiada por políticas definidas via API. A BitGo opta por um modelo mais tradicional com suporte a HSMs físicos e possibilidade de integração com dispositivos offline, mantendo a API compatível com operações de assinatura out-of-band [Inc23].

O modelo da Circle é mais orientado para fluxos financeiros tradicionais (USDC, USDC-as-a-Service), mas inclui suporte API completo com políticas, logs e integração com EVM-compatible blockchains [Cir23a].

Resumo

As soluções estudadas demonstram abordagens distintas à gestão de segurança, isolamento físico e design de APIs. A escolha do modelo a seguir dependerá do grau de confiança requerido, da estratégia de integração, e do nível de flexibilidade desejado para fluxos multiutilizador.

8 Introdução

A API da Anchorage fornece uma interface segura e robusta para instituições interagirem com a plataforma de custódia de ativos digitais da Anchorage. Esta secção descreve os componentes principais, medidas de segurança e aspectos operacionais da API.

8.1 Sistema de Autenticação

8.1.1 Componentes Principais

- Chaves API (Tokens Bearer)
- Grupos de Permissões
- Assinaturas Ed25519

8.1.2 Fluxo de Autenticação

Cada pedido à API passa por um processo de autenticação em várias etapas:

1. Verificação da validade da chave da API
2. Confirmação das permissões associadas à chave
3. Para pedidos específicos, validação das assinaturas Ed25519

8.1.3 Requisitos de Assinatura

Para pedidos da API v2 que requerem assinaturas:

- A Anchorage mantém a chave pública no seu sistema
- Os clientes devem armazenar e gerir de forma segura a sua chave privada
- Cada pedido é validado assimetricamente usando a assinatura do cliente

8.2 Gestão de Permissões

8.2.1 Grupos de Permissões

Os grupos de permissões são fundamentais para o controlo de acesso à API:

- Devem ser estabelecidos antes da criação da chave da API
- Definem regras específicas de acesso para recursos organizacionais
- Controlam permissões granulares para diferentes endpoints da API

8.2.2 Requisitos de Quórum

A modificação dos grupos de permissões requer:

- Múltiplos utilizadores autorizados para aprovar alterações
- Endosso baseado em quórum para operações críticas
- Verificação sistemática da cadeia de aprovação

8.3 Administração de Chaves API

8.3.1 Gestão de Chaves

Os controlos administrativos para chaves API incluem:

- Criação restrita apenas a administradores autorizados
- Capacidade de revogar chaves imediatamente quando necessário
- Monitorização e rastreamento do uso das chaves

8.3.2 Responsabilidades de Segurança

Considerações Importantes de Segurança:

- As organizações são totalmente responsáveis pela distribuição das chaves API
- Todas as ações realizadas com chaves API válidas são consideradas autorizadas
- A Anchorage não pode reverter operações executadas via API
- Recomenda-se a revogação imediata da chave em caso de suspeita de comprometimento

Migração de APIs para o Porto

A migração das APIs atuais para o Porto apresenta um desafio complexo e multifacetado que exige consideração meticulosa, planeamento estratégico abrangente e execução precisa. Na base destes desafios reside uma transformação arquitetural fundamental e de longo alcance: o Porto opera como um sistema sofisticado de carteira de autocustódia onde as chaves privadas são mantidas de forma segura pelos clientes e partilhadas eficientemente entre os seus utilizadores designados, representando uma mudança arquitetural significativa da infraestrutura existente da Anchorage Digital, onde a empresa mantém o controlo centralizado sobre as chaves privadas.

De uma perspetiva técnica, inúmeras funcionalidades críticas das APIs enfrentam atualmente desafios substanciais de compatibilidade com o ambiente Porto. Operações essenciais envolvendo a criação de carteiras, mecanismos de transferência e funcionalidades de retenção ainda não alcançaram o estado operacional completo dentro do ecossistema Porto. Além disso, a infraestrutura da API de transações brutas requer desenvolvimento extenso para atingir o estado de produção, particularmente no que diz respeito à integração de serviços essenciais de terceiros como o Uniswap.

Para abordar e resolver estes desafios, a equipa de desenvolvimento projetou uma estratégia de implementação estruturada e faseada. Esta abordagem metódica começa com a implementação de APIs de Leitura, progride para APIs de Escrita incorporando mecanismos robustos de aprovação por quórum, e conclui com uma solução abrangente que opera sem requisitos de quórum.

Os requisitos de implementação incluem uma extensa matriz de componentes interligados. Um aspeto crítico envolve a reativação da funcionalidade da API em múltiplas plataformas, focando-se tanto na interface do Painel do Cliente como nas aplicações móveis iOS. A equipa de desenvolvimento deve executar testes abrangentes de vários *endpoints* específicos, incluindo sistemas de gestão de endereços, operações de carteira (excluindo funcionalidade de criação), capacidades de cofre, mecanismos de negociação, procedimentos de gestão de tipos de ativos e protocolos de gestão de chaves API.

O impacto desta migração estende-se além das considerações técnicas. O esforço de desenvolvimento irá melhorar as capacidades da Plataforma de Gestão de Ativos Digitais através da integração com sistemas e serviços externos. Embora certos clientes tenham implementado soluções provisórias, como a monitorização direta da atividade *blockchain*, a implementação das APIs Porto completas fornecerá uma solução otimizada e eficiente para atender às suas necessidades operacionais e de negócio.

Em conclusão, os desafios na migração de APIs para a plataforma Porto, embora substanciais e complexos, representam passos necessários na evolução das capacidades e ofertas de serviço da plataforma. A abordagem de implementação estruturada, combinada com protocolos de teste abrangentes e procedimentos de validação, garantirá a entrega de uma infraestrutura de API eficiente que atende aos requisitos do sistema avançado de carteira de autocustódia do Porto, mantendo a segurança e desempenho ideais.

9 Conclusão

Em suma, a exposição de funcionalidades de crypto-wallets através de APIs, como a proposta para o Porto by Anchorage Digital, representa um passo fundamental para promover a interoperabilidade e a escalabilidade no ecossistema de ativos digitais e na Web3. A crescente necessidade de soluções de custódia seguras e eficientes, especialmente em contextos institucionais sujeitos a rigorosos requisitos regulatórios, torna a disponibilização programática destas funcionalidades não apenas vantajosa, mas essencial.

A conceção de uma API robusta para cold wallets exige a implementação de requisitos técnicos rigorosos, focados na segurança das chaves privadas, na integridade das operações e na auditabilidade. Mecanismos como a comunicação assíncrona, a separação de contexto, a integridade criptográfica, a aprovação multiutilizador e a compatibilidade com padrões blockchain são cruciais para garantir a confiança e a interoperabilidade da solução.

A análise da concorrência, através da avaliação de plataformas como Circle, Fireblocks, Copper e BitGo, evidencia a relevância e a sofisticação das soluções existentes no mercado. Compreender as suas arquiteturas, modelos de segurança e funcionalidades de API é vital para o desenvolvimento de uma oferta competitiva e diferenciada para o Porto.

Em última análise, a implementação bem-sucedida de uma API para as crypto-wallets do Porto permitirá uma integração fluida com diversos sistemas e plataformas, facilitando a inovação, a automação de processos e a criação de novos serviços no emergente cenário da Web3, ao mesmo tempo que garante os mais elevados padrões de segurança e conformidade regulatória.

Referências

[Ant17] Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. 2nd. O'Reilly Media, 2017.

[Bit23a] BitGo. *Billing Methodology*. 2023. URL: https://www.bitgo.com/resources/billing-methodology/.

[Bit23b] BitGo. *Digital Asset Custody | Custodial Wallets*. 2023. URL: https://www.bitgo.com/products/custody-wallets/.

[Bon+15] Joseph Bonneau et al. "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". Em: *IEEE Symposium on Security and Privacy (SP)* (2015), pp. 104–121. DOI: 10.1109/SP.2015.14.

[BS19] Dan Boneh e Victor Shoup. "A Graduate Course in Applied Cryptography". Em: https://crypto.stanford.edu/~dabo/cryptobook/. 2019.

[Cir23a] Circle. *Circle API Reference*. 2023. URL: https://developers.circle.com.

[Cir23b] Circle. *Web3 Services product fee schedule*. 2023. URL: https://help.circle.com/s/article/Developer-platform-fee-schedule.

[Cop23] Copper. *Our cold wallet technology is engineered with enhanced security*. 2023. URL: https://copper.co/insights/company-news/cold-wallet-technology-enhanced-security-and-speed.

[Cor14] IBM Corporation. *The API Economy: Disruption and the Business of APIs*. 2014. URL: https://www.ibm.com/downloads/cas/GZJWR1M7.

[Dig23a] Anchorage Digital. *Security Architecture: How Anchorage Uses MPC to Secure Crypto Assets*. 2023. URL: https://anchorage.com/blog/how-anchorage-uses-mpc.

[Dig23b] Anchorage Digital. *Security Architecture: How Anchorage Uses MPC to Secure Crypto Assets*. 2023. URL: https://anchorage.com/blog/how-anchorage-uses-mpc.

[Fie00] Roy Thomas Fielding. "Architectural Styles and the Design of Network-based Software Architectures". Tese de doutoramento. University of California, Irvine, 2000. URL: https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm.

[Fir23a] Fireblocks. *Fireblocks Developer Documentation*. 2023. URL: https://developers.fireblocks.com.

[Fir23b] Fireblocks. *Fireblocks Key Features & Capabilities*. 2023. URL: https://developers.fireblocks.com/docs/capabilities.

[Fir23c] Fireblocks. *Fireblocks Pricing*. 2023. URL: https://www.fireblocks.com/pricing/.

[Fou19] Ethereum Foundation. *EIP-712: Ethereum typed structured data hashing and signing*. 2019. URL: https://eips.ethereum.org/EIPS/eip-712.

[Gud+20] Lewis Gudgeon et al. "SoK: Layer-Two Blockchain Protocols". Em: *arXiv preprint arXiv:2001.05119* (2020). URL: https://arxiv.org/abs/2001.05119.

[Inc23] BitGo Inc. *BitGo Wallet API Documentation*. 2023. URL: https://www.bitgo.com/api.

[New15] Sam Newman. *Building Microservices: Designing Fine-Grained Systems*. O'Reilly Media, 2015.

[ONe16] Mark O'Neill. *Digital API Economy: How APIs are Reshaping Business*. CA Technologies, 2016.

[OO19] Mizuki Oue e Kazuki Okanoya. *Design and Implementation of Secure Cold Wallet Systems*. 2019. URL: https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol52_focus1_EN.pdf.

[Pap08] Michael P. Papazoglou. *Web Services: Principles and Technology*. Pearson Education, 2008.

[Qui23] QuickNode. *Developer-Controlled Wallets by Circle*. 2023. URL: https://www.quicknode.com/builders-guide/tools/developer-controlled-wallets-by-cirlce.

[RS20] Tiago Rodrigues e Pedro Silva. "RESTful APIs as Enablers of Digital Transformation: A Case Study". Em: *Journal of Systems and Software* 170 (2020), p. 110758. DOI: 10.1016/j.jss.2020.110758.

[ST06] National Institute of Standards e Technology. *Guide to Computer Security Log Management (NIST SP 800-92)*. 2006. URL: https://csrc.nist.gov/publications/detail/sp/800-92/final.

[ST20] National Institute of Standards e Technology. *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53)*. 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[Tec23] Copper Technologies. *Copper ClearLoop Technology Overview*. 2023. URL: https://copper.co.

[Woo21] Gavin Wood. *Ethereum: A Secure Decentralised Generalised Transaction Ledger – Yellow Paper*. https://ethereum.github.io/yellowpaper/paper.pdf. 2021.

[WR21] Aaron van Wirdum e Pete Rizzo. *The Blocksize War: The Battle for Control Over Bitcoin's Protocol Rules*. BTC Media, 2021.