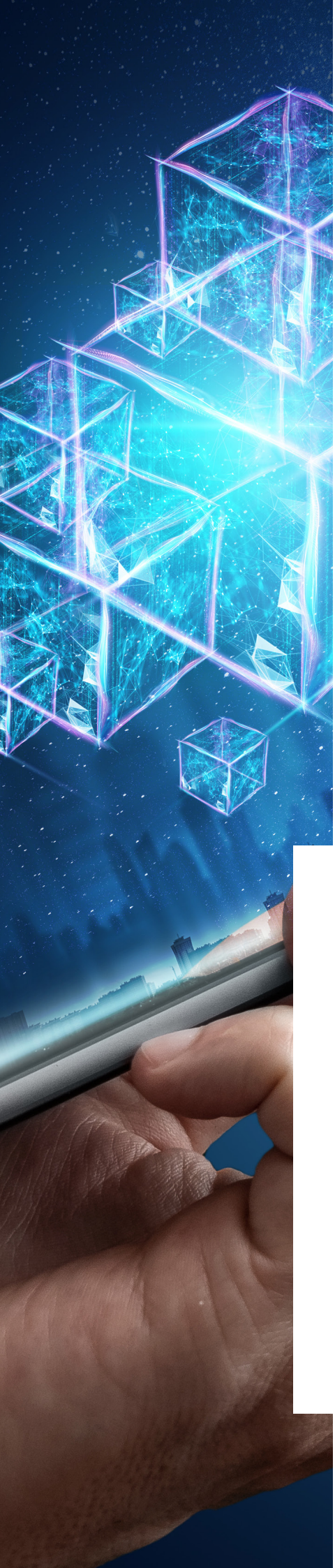
DINAMO NETWORKS | O MUNDO MAIS SEGURO

CRIPTOATIVOS SUMIRAM AS CHAVES, SUMIU O DINHEIRO!

A IMPORTÂNCIA DA CUSTODIA.

dinamonetworks.com



SUMÁRIO

RESUMO

A área de ativos digitais representa uma inovação global que apresenta desafios significativos em termos de segurança, especialmente na custódia das chaves criptográficas. Relatos frequentes de roubos de criptomoedas destacam que mais da metade desses incidentes ocorre devido ao furto das chaves privadas, gerando sérias preocupações em relação à segurança da custódia digital. Afinal, a perda das chaves criptográficas significa a perda dos ativos ou do próprio dinheiro. Existem diversos conceitos de custódia de criptomoedas e tokens, e a prestação desses serviços por instituições financeiras confiáveis e reguladas é crucial para promover a adoção da tecnologia de ledger distribuído (DLT, na sigla em inglês).

Neste artigo, iremos explorar as principais tecnologias de segurança utilizadas globalmente na custódia institucional. Além disso, destacaremos a importância de escolher soluções certificadas que estejam em conformidade com as melhores práticas de mercado, essenciais para mitigar os receios associados à custódia.

Um tema importante considerando o aumento de casos de uso envolvendo ativos digitais e tokenizados, e especialmente o projeto de criação de uma moeda digital do banco central brasileiro, o DREX.

ATIVOS DIGITAIS

No cenário global atual, os ativos digitais, virtuais ou criptoativos estão revolucionando a maneira de realizar transações financeiras, prometendo dar maior liberdade, eficiência e economia na forma de se relacionar no mundo dos negócios e meios de pagamentos. A tecnologia de registro distribuído, incluindo redes DLT (Distributed Ledger Technology) e blockchain, introduziu **inovações que não só criam novas oportunidades de negócio, mas também melhoram a segurança,** eficiência e reduzem os custos. Essas tecnologias estão sendo aplicadas em diversas áreas, incluindo a implementação de moedas digitais de bancos centrais (CBDCs) por governos, inclusive no Brasil com o atual piloto do DREX. De acordo com projeções de adoção, **espera-se que essas tecnologias se tornem ubíquas na vida diária da maioria da população.** Um estudo do Boston Consulting Group estima que até 2030, 10% do PIB mundial, o equivalente a 16 trilhões de dólares americanos, serão tokenizados.

A tokenização, que permite o armazenamento e a transação de ativos utilizando tecnologias de DLT e blockchain, promete uma captação de recursos mais eficiente e econômica em comparação com os métodos tradicionais atualmente utilizados. O uso de identidades descentralizadas para transações e interações dentro do ecossistema dos criptoativos é uma outra aplicação relevante. As Identidades Descentralizadas (DiD) permitem que indivíduos, organizações ou dispositivos tenham uma identidade única e autossuficiente na rede.

Com funcionamento baseado em algoritmos criptográficos, a tecnologia traz comprovadamente um alto nível de segurança. No entanto, os relatos frequentes de roubos envolvendo criptomoedas têm gerado preocupação e incerteza.

Desde 2011, estima-se que mais de 12 bilhões de dólares americanos foram roubados, o que equivale atualmente a quase U$ 50 bilhões considerando a cotação dessas criptomoedas [1].

> “12 bilhões de dólares americanos roubados”

Mais da metade desses roubos ocorrem devido ao furto das chaves privadas utilizadas para acessar e gerenciar os ativos digitais [2]. Esses furtos acontecem de várias maneiras, incluindo engenharia social, onde golpistas utilizam técnicas para enganar pessoas e obter suas chaves privadas; softwares maliciosos que, uma vez instalados, podem roubar as chaves privadas; e também através de hacks, como ataques a vulnerabilidades na cadeia de suprimentos (supply chain attacks) ou ataques de força bruta. Além disso, o **uso inadequado ou a perda das chaves por parte dos usuários também contribuem significativamente para esses problemas.** Estima-se, por exemplo, que quase 20% das bitcoins em circulação tenham sido perdidas pelos seus proprietários [2].

AS CHAVES SÃO O DINHEIRO!

No mercado tradicional, **o uso de chaves criptográficas é amplamente difundido, seja para transações, senhas ou certificados.** A possível perda dessas chaves geralmente pode ser mitigada rapidamente, permitindo a revogação e a redefinição de novas senhas, sem grandes consequências. Por exemplo, os certificados digitais são formas de identificação que devem ser armazenadas com segurança para evitar uso indevido, fraudes e vazamentos de informações. Um certificado perdido pode ser facilmente revogado para que um novo seja gerado.

No entanto, na tecnologia DLT, todas as operações se tornam imutáveis, o que significa que não podem ser desfeitas. **No caso dos criptoativos, as chaves representam diretamente os valores dos ativos, ou seja, o próprio dinheiro, e precisam ser protegidas de forma extremamente segura.**

As chaves representam diretamente os valores dos ativos, ou seja, o próprio dinheiro, e precisam ser protegidas de forma extremamente segura.

A maioria das redes DLT ou blockchain utiliza transações com assinaturas baseadas em criptografia assimétrica, que envolve duas chaves: **a chave privada, que é mantida em segredo e permite o acesso ao sistema, e a chave pública, que pode ser compartilhada e utilizada por qualquer pessoa.**

CARTEIRAS NÃO CUSTODIANTES E CUSTODIANTES

Para utilizar ou investir em criptoativos, é geralmente necessário possuir uma carteira digital (wallet). Elas são classificadas em duas categorias principais: carteiras não custodiais e custodiais. **Nas carteiras não custodiais, as chaves privadas são mantidas sob a responsabilidade direta do usuário** (ele mesmo é o custodiante). Isso confere ao usuário total controle sobre seus ativos, permitindo-lhe operar suas chaves diretamente. Defensores das criptomoedas frequentemente utilizam o argumento da auto-custódia como uma maneira de promover maior liberdade financeira, conforme o famoso lema "Not your keys, not your coins" (se não são suas chaves, não são suas moedas). **No entanto, gerenciar suas próprias chaves é uma responsabilidade significativa que nem todos os usuários estão preparados para assumir.**

Para permitir uma adoção mais ampla das tecnologias DLT, é necessário considerar a possibilidade de delegação da gestão das chaves para evitar o "esquecimento da senha". **As carteiras custodiais facilitam esse processo, permitindo que um terceiro de confiança armazene e gerencie as chaves privadas em nome do usuário.** Com a entrada de novos investidores em criptoativos, bancos e instituições financeiras estão explorando novas formas de oferecer serviços de ativos digitais com níveis mais elevados de segurança aos clientes. É altamente provável que, com a adoção crescente da tecnologia DLT, a tokenização de ativos, o advento do Real Digital (DREX) e o surgimento de novas moedas no sistema financeiro, **o mercado de custódia institucional experimente um crescimento exponencial.**

CUSTODIA INSTITUCIONAL DE CRIPTOATIVOS

Delegar suas chaves a uma instituição implica confiar na sua habilidade de gestão e nas práticas de cibersegurança adotadas. As soluções de custódia de ativos digitais devem rigorosamente seguir requisitos internos e externos de segurança. No Brasil, a Lei 14.478/2022 estabelece regulamentações e diretrizes para a prestação de serviços de ativos virtuais, visando proporcionar maior proteção aos usuários desses serviços. A normatização dos processos envolvendo ativos virtuais, incluindo o tema da custódia, está atualmente sendo definida pelo Banco Central do Brasil, com uma conclusão prevista durante 2025. A CVM publicou em 2023 a resolução 175 permitindo a fundos que investem em criptoativos, que até agora precisavam de um custodiante regulado no exterior, possam guardar os ativos digitais em instituições brasileiras reguladas.

> **"A normatização dos processos envolvendo ativos virtuais, incluindo o tema da custódia, está atualmente sendo definida pelo Banco Central do Brasil"**

Um tema amplamente debatido, já implementado em outras jurisdições, como a regulação da VARA nos Emirados Árabes Unidos ou na Suíça, é a segregação patrimonial, que garante a separação entre os ativos dos usuários e da prestadora de serviços. Essa condição é crucial para assegurar que os ativos dos usuários não sejam indevidamente utilizados

ou colocados em risco pela prestadora, e para facilitar a recuperação dos ativos em caso de falência da instituição. Outras definições processuais e tecnológicas precisarão ser recomendadas ou exigidas para garantir a segurança contínua dos ativos.

As instituições que oferecem serviços de custódia de criptoativos implementam suas próprias soluções de segurança ou contratam provedores de infraestrutura especializados, que auxiliam na aplicação das melhores práticas de segurança para proteção das chaves e na implementação de governança para autorização de transações e acesso aos ativos.

TOKENIZAÇÃO E CUSTÓDIA

No caso de instituições que emitem ativos tokenizados, são utilizados contratos inteligentes que estabelecem as regras fundamentais aplicáveis aos tokens. Esses contratos possibilitam funções essenciais, como emissão, queima, restrições de transferência, congelamento e ações corporativas associadas aos ativos. Os contratos inteligentes são criados em redes DLT ou blockchain por meio de chaves criptográficas. **É crucial que as chaves privadas dos emissores dos tokens sejam altamente protegidas para evitar que essas funções sejam ativadas ou modificadas indevidamente.**

MÉTODOS PARA CUSTÓDIA: TEMPERATURA DAS CARTEIRAS

A temperatura da carteira está diretamente relacionada à sua acessibilidade através da rede/servidores e à vulnerabilidade a acessos não autorizados em caso de infraestrutura comprometida. As carteiras são avaliadas com base em segurança, velocidade e escalabilidade, e são classificadas como frias (cold wallets) ou quentes (hot wallets).

As Cold Wallets, ou carteiras frias, são consideradas mais seguras por serem desconectadas da internet, minimizando assim os riscos de ataques cibernéticos. No entanto, requerem processos manuais mais demorados (geralmente de 1 a 24 horas) para assinar transações. As variantes “Frozen” ou “Deep” oferecem ainda mais segurança ao utilizar ambientes completamente isolados (air-gapped) para armazenar chaves privadas e servidores. Embora extremamente seguras, essas soluções são difíceis de escalar em caso de aumento no volume de transações.

Por outro lado, as Hot Wallets, ou carteiras quentes, estão sempre conectadas à internet, facilitando as transações ao permitir a assinatura e a transmissão rápida pelas redes blockchain. Elas podem ser vulneráveis a riscos de segurança devido à conexão contínua com a infraestrutura de TI, mas proporcionam acesso rápido e automático para assinatura de transações com chaves privadas.

Existem também as **Warm Wallets, ou carteiras mornas, que são configuradas para oferecer acesso facilitado com camadas adicionais de segurança, como o uso de dispositivos criptográficos em hardware** (Hardware Security Module - HSM). Essas carteiras são projetadas para equilibrar facilidade de acesso e segurança robusta durante processos de transação.

A maioria das empresas custodiantes utiliza uma combinação dessas carteiras, adaptando-se ao tipo de transações e à necessidade

de agilidade no acesso aos ativos. Processos automáticos são implementados para manter apenas a quantidade mínima de ativos em carteiras quentes em tempo integral, reduzindo assim os riscos de exposição.

No Japão, por exemplo, a Agência de Serviços Financeiros (FSA) estabeleceu regras que determinam que pelo menos 95% dos ativos dos clientes sejam mantidos em cold wallets, ou seja, que não estejam conectadas à internet.

PROCESSOS DE ASSINATURA DE TRANSAÇÕES

Métodos mais elaborados de custódia utilizam diferentes abordagens de assinatura das transações para aumentar a segurança. As assinaturas digitais, fundamentais em redes DLT, seguem três etapas principais:

- **Geração do par de chaves** (pública e privada);
- **Geração da assinatura:** utilização da chave privada para assinar transações;e
- **Verificação da assinatura:** Verificação da autenticidade através da chave pública.

Na abordagem tradicional de assinatura simples, uma única chave privada é usada para criar e validar transações na blockchain, o que pode representar um único ponto de falha se comprometida, resultando na perda dos ativos da carteira. Para mitigar esse risco, diferentes técnicas são aplicadas. São elas:

As Multiplas Assinaturas (Multisig) exigem várias assinaturas de diferentes chaves privadas para movimentar fundos, denotadas como M de N, onde M é o número mínimo de assinaturas necessárias de um total de N chaves privadas. Embora ofereça segurança adicional, Multisig pode apresentar desafios operacionais e de escalabilidade (incompatibilidade com algumas redes, dificuldades de alterar o esquema M de N, privacidade do esquema M de N, multiplicação das taxas de transações).

O **Esquema de Compartilhamento Secreto de Shamir (SSSS)** fragmenta a chave privada em partes secretas, distribuídas e armazenadas em locais distintos, e atribuídos a diferentes partes. Para a assinatura de uma transação, é necessária a reconstrução da chave privada completa.

A **Computação multipartidária (MPC – Multi-Party Computation)** possibilita assinaturas divididas entre várias partes, eliminando um único ponto de falha. No MPC, múltiplos fragmentos de chaves, conhecidos como shares, são gerados em um esquema M de N, onde apenas um subconjunto desses shares é necessário para realizar uma assinatura, **sem a necessidade de reconstruir a chave privada completa.** Essa abordagem oferece flexibilidade para ajustar os limiares ou os signatários sem exigir a criação de novas carteiras, sendo compatível com qualquer rede utilizada. **Apesar de sua eficiência e praticidade, a tecnologia ainda suscita dúvidas por ser relativamente nova e complexa, além de gerar preocupações em relação à criptografia convencional.** Os protocolos MPC continuam em fase de estudo no NIST (National Institute of Standards and Technology), o principal órgão de segurança dos Estados Unidos, e ainda não foram oficializados como padrões de mercado [3]. Esses ainda são protocolos proprietários, o que pode acarretar riscos de falhas, como já ocorreu recentemente em protocolos

usados por grandes plataformas de custódia digital [4]. Como envolvem necessariamente mecanismos conectados à internet não são adaptados a custódia fria (Cold).

USO DE HARDWARE CRIPTOGRÁFICO - HSM

O Hardware Security Module (HSM) é uma tecnologia consolidada e amplamente adotada no setor financeiro, sendo **utilizada por décadas pelos principais bancos e instituições financeiras para realizar operações criptográficas e armazenar chaves criptográficas de maneira segura.** Ele segue rigorosas normas de certificação internacional, como o FIPS 140-2 emitido pelo NIST, garantindo conformidade com as regulamentações do setor [5].

Suas propriedades físicas e mecanismos de controle asseguram a segurança no armazenamento de materiais criptográficos, como chaves, e nos processos criptográficos envolvidos, como assinaturas digitais e transações. Entre os mecanismos estão procedimentos avançados de detecção e resposta a violações, velocidade otimizada dos processos criptográficos, controle rigoroso de acesso às chaves (incluindo o uso de esquemas de compartilhamento secreto SSSS), alta disponibilidade e redundância geográfica.

O **HSM é essencial para a gestão segura e institucional de chaves criptográficas utilizadas em blockchain e ativos digitais,** possibilitando a assinatura de transações diretamente no equipamento. Ele oferece segurança garantida no acesso às chaves por meio de mecanismos como compartilhamento secreto entre múltiplas partes (esquema M de N). **Além de operacionalizar assinaturas digitais de maneira segura e certificada, o HSM suporta abordagens avançadas como Multisig e SSSS.** Para o MPC, ainda estão em andamento estudos para oferecer total suporte do HSM aos algoritmos de assinatura, mas já existem soluções híbridas que combinam essas tecnologias para proteger backups ou os fragmentos de chaves MPC de forma tão segura quanto qualquer outra chave privada.

> **“O HSM é o meio de operacionalizar assinaturas digitais de forma segura e certificada, inclusive para abordagens mais elaboradas.”**

É importante ressaltar que a utilização de HSMs dedicados e administrados pelo custodiante possibilita a identificação precisa da posse das chaves criptográficas dos ativos digitais, trazendo controle e autonomia ao custodiante, evitando, assim, a delegação da responsabilidade (ou terceirização) de custódia a plataformas SaaS ou a operadores de serviços em nuvem.

PANORAMA REGULATÓRIO GLOBAL DE CUSTÓDIA

O panorama regulatório global para custódia de ativos digitais está cada vez mais enfatizando a segurança e a proteção dos ativos através da utilização de Hardware Security Modules (HSMs) e da exigência de posse das chaves privadas em território nacional. Países ao redor do mundo estão estabelecendo diretrizes claras para instituições financeiras e custodiantes que lidam com criptoativos, visando mitigar riscos de segurança cibernética e garantir a conformidade com as melhores práticas.

Várias autoridades regulatórias pelo mundo, como a Bermuda Monetary Authority [6] ou a Hong Kong Securities and Futures Commission [7] já recomendam o uso do HSM homologados pela norma FIPS 140-2 como o mecanismo de armazenamento de chaves mais seguro.

Além disso, há uma tendência crescente em alguns países para exigir que as chaves privadas associadas a criptoativos sejam mantidas em território nacional. Isso visa assegurar que as autoridades locais tenham capacidade de supervisão e controle sobre esses ativos, reduzindo potenciais riscos relacionados a jurisdições estrangeiras e facilitando a aplicação de regulamentos locais de forma mais eficaz.

PILOTO DREX

A nova moeda digital do Banco Central do Brasil, o Real Digital (DREX), promete trazer diversos benefícios para a economia brasileira tornando as transações financeiras mais rápidas, eficientes e inteligentes.
O DREX é uma CBDC (Central Bank Digital Currency – CBDC), uma versão digital do Real (BRL/R$). Com a moeda digital oficial, será possível realizar transações programáveis: pagamentos podem ser vinculados a certas condições, como recebimento de um pagamento ou de um produto, possibilitando maior automação no sistema financeiro e menores custos de verificação. Operações financeiras podem ser vinculadas entre si para criação de novos produtos e casos de uso benéficos para a população.

Desde 2020, o BACEN estuda a utilização da tecnologia de registro distribuído para realizar transações. Em abril de 2023, foi iniciado o Piloto do Real Digital para testar e viabilizar o projeto de CBDC. Para o piloto, o Banco Central selecionou a plataforma DLT Hyperledger Besu, desenvolvida pela fundação Linux.

O principal desafio no piloto é simular operações e casos de uso com o DREX endereçando os temas essenciais do projeto que são Programabilidade (Oportunidade de criar serviços e soluções baseadas em Smart Contracts), Descentralização (diferentes validadores e participantes) e Privacidade das transações. Mas o tema da Segurança é também essencial para o piloto: uma das diretrizes é a adoção de padrões de resiliência e segurança cibernética equivalentes aos aplicáveis a infraestruturas críticas do mercado financeiro.

É neste contexto que a DINAMO Networks, com suas soluções de segurança criptográfica em hardware (HSM – Hardware Security Module), participa do piloto DREX, fornecendo suas soluções de segurança digital para a proteção de chaves criptográficas utilizadas e das transações na rede do piloto. Os principais casos de uso são:

Segurança e integridade da rede BESU com proteção dos nós

participantes da rede utilizando HSM. A integridade da rede depende da segurança das chaves utilizadas pelos nós da rede. Essas chaves são usadas para identificação e comunicação entre os nós, e para a propagação e validação das transações (em blocos) na rede. O uso da tecnologia de HSM proporciona proteção avançada contra os ataques físicos e lógicos, garantindo integridade e confidencialidade das chaves criptográficas envolvidas.

Custódia das chaves de ativos (carteiras) em HSM e segurança das Transações. Os ativos que transitam pela rede são protegidos pelas chaves privadas das carteiras detentoras. A tecnologia de HSM também se aplica à proteção e custodia de chaves de ativos tokenizados nas carteiras digitais (wallets). O HSM garante a proteção institucional e escalável das chaves privadas, utilizadas pelas instituições ou pelos usuários finais para acesso aos tokens e ativos.

A utilização da tecnologia de HSM dentro desse cenário assegura a conformidade legal e aprimora a reputação dos participantes, porque auxilia na adesão às regulamentações e diretrizes de segurança tais como a LGPD, a ISO 27001 ou a resolução 4893 do Banco Central (política de segurança cibernética).
Além dos requisitos de segurança, a tecnologia HSM permite processar altos volumes de transações e assinaturas digitais com alta performance (throughput) e arquitetura escalável, importantíssimo para as validações das transações e operações do DREX.

SANAR A PREOCUPAÇÃO DA CUSTODIA

Com a chegada das novas moedas digitais, incluindo o Real Digital (DREX), que adotará tecnologias de registro distribuído em sua implementação, **surge a necessidade premente de resolver os desafios relacionados à custódia.** Este é talvez um dos maiores obstáculos enfrentados pelo mercado atualmente.

Apesar da ampla gama de soluções de segurança disponíveis para o universo dos criptoativos, **o mercado institucional tende a optar por soluções já consolidadas que garantam o cumprimento das melhores práticas.** Atualmente, a maioria da custódia de ativos digitais é concentrada em poucos players americanos. É essencial que boas práticas sejam disseminadas, recomendadas e regulamentadas pelos órgãos competentes, à semelhança do que ocorreu com o Sistema de Pagamentos Brasileiro e o PIX. Ademais, **é crucial incentivar a entrada de novos players no mercado de custódia para estabelecer uma indústria nacional de alto nível.**

Além de possibilitar a identificação da posse das chaves criptográficas dos ativos digitais, o HSM também permite determinar a identificação da localização geográfica do armazenamento dessas chaves. Isso contribui para a preservação da soberania nacional sobre os ativos virtuais, evitando situações em que a propriedade formal ocorre em território nacional, mas a posse efetiva é controlada fora do país por prestadores externos terceirizados.

> **“Além de possibilitar a identificação da posse das chaves criptográficas dos ativos digitais, o HSM também permite determinar a identificação da localização geográfica do armazenamento dessas chaves.”**

A implementação das melhores práticas de segurança por parte das instituições garantirá uma maior adoção dessas novas tecnologias, impulsionando a inovação e marcando uma nova era digital, comparável ao impacto da Internet. Bem-vindos à era dos ativos digitais.

SOLUÇÃO DINAMO BLOCKCHAIN

Chegou a hora de você descobrir a forma mais segura do mundo de custódia com o DINAMO Blockchain.

Com a API da DINAMO Blockchain, empresas do ecossistema de criptoativos que têm necessidades de custódia podem integrar facilmente suas aplicações - Wallet, Trading e outros - ao serviço criptográfico em hardware especializados. Garantindo o compliance das operações, por meio de certificações globais, como o FIPS 140-2, do National Institute of Standards and Technology (NIST), principal órgão americano de segurança. Quer saber mais? Visite nossa página: www.dinamonetworks.com/blockchain/

Referências

1 https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/
2 https://www.chainalysis.com/
3 https://csrc.nist.gov/Projects/threshold-cryptography
4.https://www.coindesk.com/tech/2023/08/09/fireblocks-discloses-zero-day-vulnerabilities-impacting-leading-mpc-wallets
5 https://csrc.nist.gov/publications/detail/fips/140/2/final
6 https://cdn.bma.bm/documents/2022-04-06-15-21-50-Digital-Asset-Custody-Code-of-Practice-2022.pdf
7 https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/Guidelines-for-Virtual-Asset-Trading-Platform-Operators/Guidelines-for-Virtual-Asset-Trading-Platform-Operators.pdf?rev=f6152ff73d2b4e8a8ce9dc025030c3b8

A DINAMO Networks é a empresa especialista em proteção de dados e sigilo de informações. Por meio da sua expertise tecnológica, oferece um barramento de serviços criptográficos adaptados a diversos casos de uso de criptografia. Essas APIs de segurança de alto nível são baseadas no uso dos equipamentos especializados de segurança criptográfica, os Hardware Security Modules - HSMs, ou, cofre digitais, que também são fabricados pela empresa disponibilizados On-Premises ou em diversos modelos de nuvem.

Mais informações, visite nosso site:

dinamonetworks.com.

DINAMO NETWORKS | O MUNDO MAIS SEGURO