TELEGRAM

LEARNING

http://i2e.online

Carteiras digitais

10 de Agosto de 2022

documento extra

Carteiras Digitais

LEARNING

http://i2e.online

Criptografia e Carteiras de Criptomoedas

Uma carteira digital é uma das ferramentas essenciais para o acesso ao mundo das criptomoedas. Estas são, igualmente, fundamentais para o seu armazenamento e interação com diferentes blockchains.

Estes instrumentos informáticos utilizam um tipo de criptografia denominada de criptografia assimétrica, a qual, resumidamente, é um sistema criptográfico composto por chaves públicas, que, tal como o nome indica, podem ser distribuídas e chaves privadas, as quais, por sua vez, permitem reverter a encriptação da mensagem e, como é evidente, nunca devem ser partilhadas ou cedidas. Esta técnica, ao utilizar, duas chaves diferentes para realizar funções opostas (pública vai encriptar e privada reverter) assume o nome de criptografia assimétrica.

Nas carteiras de criptomoedas, com este mecanismo de encriptação, a chave pública é utilizada para gerar endereços públicos, a fim de serem distribuídos e partilhados. Com estes é possível receber, nessas carteiras, ativos digitais. A chave privada é aquela que permite assinar as transações (envio de valor) e aceder aos fundos da carteira, razão, pela qual, deve ser guardada com a maior segurança possível.

Estas chaves podem ser armazenadas em hardware, podem ser utilizadas por software ou, em alternativa, impressas em papel ou noutro material como, por exemplo, metal.

Atualmente, para facilitar a memorização das chaves privadas, existe o sistema de seed-phrase (frase semente), que permite a codificação das chaves privadas, através de 12 ou 24 palavras. Não vou explicar o mecanismo criptográfico, subjacente a este sistema, mas aconselho a pesquisa sobre o mesmo. As palavras da seed, inseridas na ordem correta, permitem fazer a recuperação da carteira e dos fundos nela contidos.

Um exemplo: possuo uma carteira com várias criptomoedas, entre as quais, bitcoins, no meu telemóvel. Por um incidente, este fica danificado, irremediavelmente. Adquiro um novo equipamento, instalo a carteira mobile e aplico as palavras da minha seed, pela ordem correta, et voilá, os fundos da carteira são carregados no novo dispositivo. Contudo, se essa seed for obtida por alguém, de um modo malicioso, executa os mesmos passos e, automaticamente, tem acesso aos meus fundos, de forma não autorizada.

Carteiras de Criptomoedas

De acordo com as suas caraterísticas de armazenamento ou "responsabilidade" da custódia das chaves, as carteiras podem ser classificadas da seguinte maneira:

- **Manutenção e "responsabilidade" na custódia das chaves**

Custodial (com custódia). São os tipos de carteiras, que os Exchanges, empresas de compra e venda de criptomoedas, utilizam e facultam aos seus clientes. A chave privada não está na posse do cliente. Para enviar fundos, quem assina a transação são os sistemas dos Exchanges, responsáveis pelas transações. Dá-se a ordem de transferência, mas a mesma só é executada, após a indicação e validação por parte do sistema.

Non custodial (sem custódia). São os tipos de carteira, onde a responsabilidade é toda da parte do utilizador, o qual tem na sua posse o conjunto de chaves: pública e privada, e é este quem assina as transações.

Carteiras digitais

LEARNING

http://i2e.online

Custodial
(com custódia)

Cold storage service
(sem ligação rede)

COINBASE VAULT

Digital currency wallets are great for day-to-day spending, but storing large amounts of digital currency for the long term requires extra security.

Hot storage
(com ligação rede)

BINANCE

kraken

crypto.com

TELEGRAM

Carteiras digitais

Custodial (com custódia)

Non-Custodial (sem custódia)

LEARNING

http://i2e.online

Cold storage service (sem ligação rede)

COINBASE VAULT

Digital currency wallets are great for day-to-day spending, but storing large amounts of digital currency for the long term requires extra security.

Hot storage (com ligação rede)

BINANCE

kraken

crypto.com

Cold wallets (sem ligação rede)

Físicas (equipamento)

- Ellipal
- Ledger
- Trezor

Físicas (material)

- Papel
- Metal

Hot wallets (com ligação rede)

METAMASK

EXODUS

Digitais (software)

Trust Wallet

Carteiras digitais

LEARNING

http://i2e.online

Custodial
(com custódia)

- ***Tu não controlas as chaves privadas***
- ***Tu não controlas, totalmente, os teus ativos***
- ***Uma entidade (empresa) armazena os teus ativos e mantém as chaves na sua posse***

- As transferências são **ordenadas por ti**, mas efetuadas pela entidade (***caso seja essa a vontade deles).***

- A tua conta bancária é uma carteira custodial, pois as somas de dinheiro existentes nas tuas contas estão armazenadas no banco (entidade) que as mantém, à partida em segurança.

- Quando ordenas uma transferência o banco executa a ordem e retira os fundos da tua conta, mas pode sempre negar-se a executar essa ordem.

Carteiras digitais

LEARNING

http://i2e.online

Non-Custodial (sem custódia)

- ***O controlo e responsabilidade dos fundos são teus a 100%***
- ***Tu controlas as chaves privadas***
- ***Tu controlas, totalmente, os teus ativos***
- ***A carteira armazena os teus ativos e tu tens as chaves na tua posse***
- ***As transferências são ordenadas e efetuadas por ti, via software da carteira digital.***

- O teu **porta-moedas** é uma carteira non-custodial, pois as somas de dinheiro existentes estão armazenadas, diretamente, por ti nos vários compartimentos da carteira.
- Quando fazes um pagamento retiras o dinheiro da carteira sem a regulação e/ou interferência (direta, salvo emissão de moeda) de uma entidade nesse ato.
- Tu decides de que compartimento retiras o dinheiro e como pagas, se notas e/ou moedas
- A responsabilidade é tua na totalidade, pois se perdes o porta-moedas perdes o dinheiro.

TELEGRAM

Carteiras digitais

LEARNING

http://i2e.online

	Custodial	Non-Custodial
Perdi a password e agora…?	O serviço de apoio ao cliente poderá ajudar-te a recuperar o acesso	Todos os teus ativos perderam-se para sempre. Não poderás recuperá-los
Episódio de acesso não autorizado…	Contacta o serviço de apoio o mais rapidamente	Poderás ter perdido os teus ativos caso os tenham levantado
Controlo dos activos digitais	Partilhado entre utilizador e entidade (ex Banco, Exchange)	É total por parte do utilizador
Sistema financeiro	Centralizado	Descentralizado
Nível de segurança	Definido pela entidade e utilizador	Só o utilizador define o nível de
Custos e taxas	Preçário da entidade	Definido pela rede
Risco de ataque	Ataques à entidade e/ou ao utilizador	Ataques apenas ao utilizador

Carteiras digitais

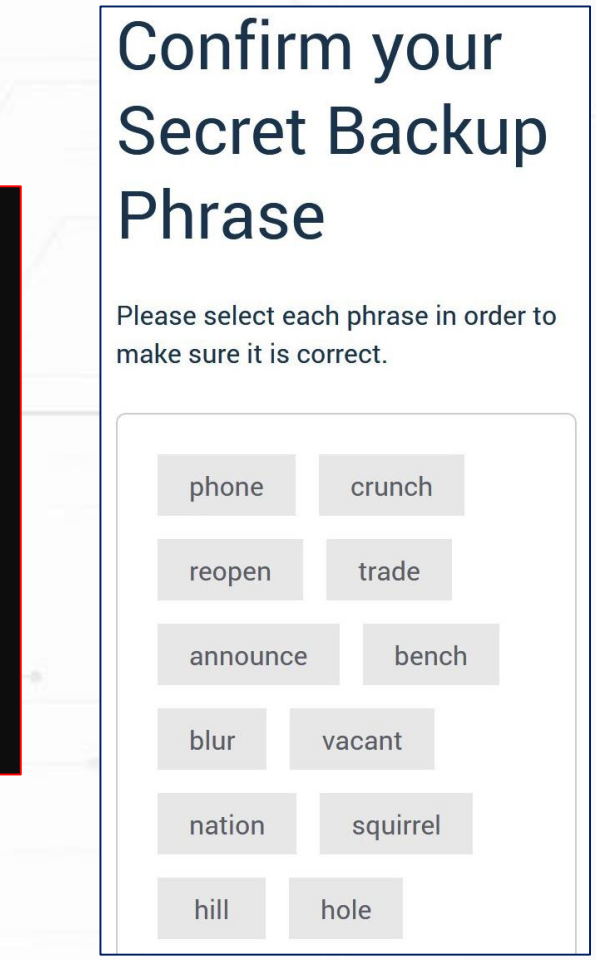
Atualmente, para facilitar a memorização das chaves privadas, existe o sistema de seed-phrase (frase semente), que permite a codificação das chaves privadas, através de 12 ou 24 palavras. Não vou explicar o mecanismo criptográfico, subjacente a este sistema, mas aconselho a pesquisa sobre o mesmo. As palavras da seed, inseridas na ordem correta, permitem fazer a recuperação da carteira e dos fundos nela contidos.

LEARNING

http://i2e.online

Seed ou Backup phrase

12 ou 24 palavras



Carteiras digitais

LEARNING

http://i2e.online

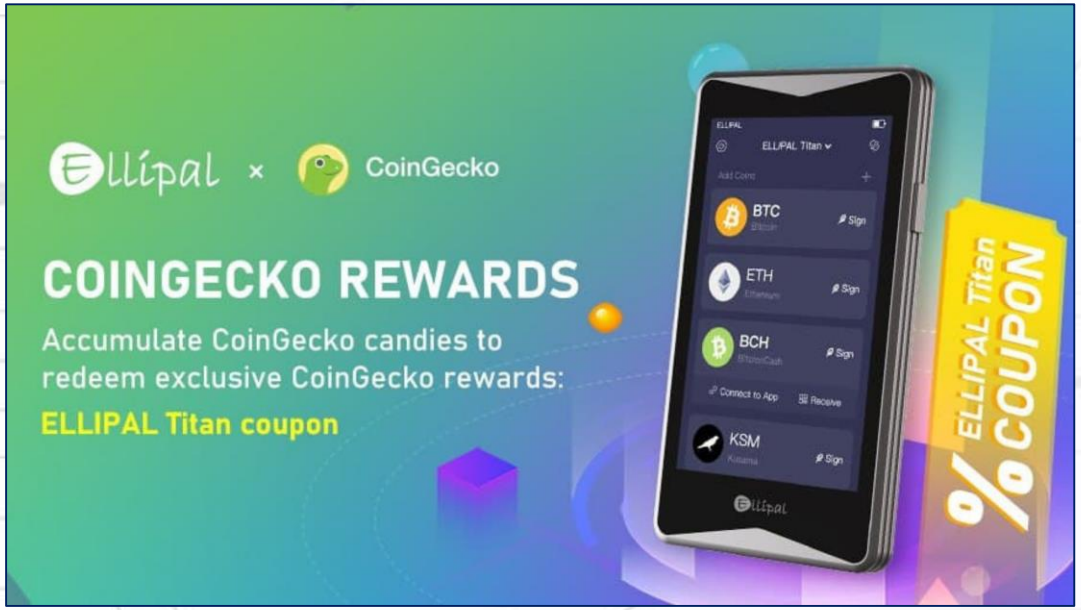
Esta tua frase/seed é:

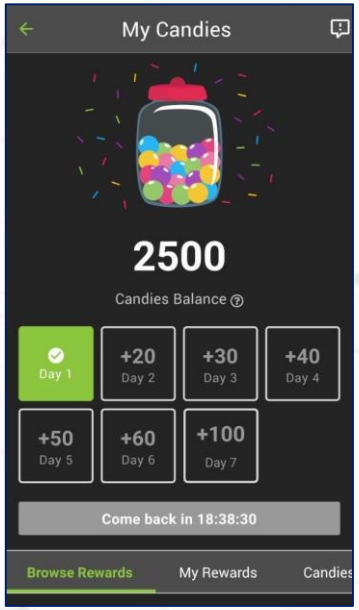
- O PIN do teu cartão Multibanco
- A combinação do teu cofre
- A chave da tua casa ou do teu carro
- **Aquilo que nunca podes perder**
- Aquilo que **deves guardar de forma segura em formato físico em mais do que um sítio diferente**
- **Aquilo que se perderes implica a perda total dos teus fundos**

Promoção Ellipal + Coingecko

LEARNING

http://i2e.online





- Abre conta na Coingecko
- Recolhe os candies diariament,
- quando tiveres 400 candies podes pedir um cupão de 5USD de desconto

- 11 dias seguidos a recolher candies já permitem ter os 400 necessários

Conclusões

LEARNING

i2e

http://i2e.online

- Criei este documento não com o intuito de alarmar ou espalhar o pânico, mas sim expor o meu conhecimento (de experiência feito);
- Fiquei com fundos bloqueados no Wirex até uma validação da conta (já anteriormente validada). Digo-te que não é agradável perceber que aquilo que é nosso pode, num segundo, deixar de ser, por tempo indeterminado, por vontade de uma plataforma qualquer;
- **No dia 1 de Agosto retirei fundos da Hodlnaut e todas as plataformas** *Dia 8 de Agosto saiu o mail da Hodlnaut a todos os clientes (fundos bloqueados, por tempo indeterminado, com efeitos imediatos*). Tens noção do que é acordar e pensar que tudo o que está lá, deixa de ser teu?! (tive muita sorte!); (**já agora esquece o documento das contas rendimento BTC**);
- Neste momento dispenso juros em troca da propriedade efetiva (não tem preço);
- Atualmente tenho fundos residuais em plataformas, tendo optado por carteiras non-custodial;
- Entre todas as carteiras físicas cold (equipamento) são as melhores, mas implicam o custo de aquisição