



VIVER DE RENDA CRIPTO

FORMAS DE EXPOSIÇÃO

RESUMO
AULA 03

Formas de Exposição

DCA vs. "De uma vez"

Um dos dilemas que os investidores vivem, sobretudo os iniciantes, é como se dará a sua exposição aos ativos – “compro o que eu quero de uma vez, e tento achar o fundo, ou compro aos poucos?”.

Dollar-Cost Averaging (DCA, em português “A média do custo em dólar”) é a estratégia de investimento na qual um investidor divide o valor total a ser investido nas compras periódicas de um ativo alvo, como o Bitcoin. O objetivo de fazer isso é reduzir o impacto da volatilidade na compra geral.

As compras ocorrem independentemente do preço do ativo e em intervalos regulares – a cada mês, a cada 15 dias ou a cada semana. Essa estratégia remove muito do trabalho detalhado de tentar cronometrar o mercado a fim de fazer compras de ativos pelos melhores preços. O DCA também pode ser entendido como um plano de investimento automático constante: faz-se compras regulares e os lucros são recebidos de pouco a pouco.

Com isso, temos a carteira se comportando de forma mais suave, com menos volatilidade. Sim, aportes recorrentes minimizam a volatilidade e, acredite, você não está acostumado a este tipo de volatilidade - aproximadamente 90% ao ano.

Há estudos que mostram que se o investidor comprasse BTC no pico do penúltimo ciclo de alta do Bitcoin, em dezembro de 2017, mas continuasse fazendo aportes recorrentes, todos os meses, seu lucro em 3 anos seria de 340%. Mas se esse mesmo investidor tivesse feito um único aporte em dezembro de 2017, tudo de uma única vez, ele passaria metade dos 3 anos no vermelho (teria 1 ano e meio de prejuízo) e, no final, cerca de 112% de lucro. No decorrer dos anos o

DCA tem se mostrado uma estratégia mais vencedora. Por isso, a recomendação é de não investir tudo de uma vez.

Pensando em alocação percentual do patrimônio ou da renda, seria mais sensato alocar todos os meses uma porcentagem da renda do que uma porcentagem do patrimônio. Por exemplo, digamos que algum aluno do curso tenha renda mensal de R\$5.000,00 e ele separa 5% para investir em criptoativos todos os meses, isso significa que ele investirá cerca de 250 reais por mês, ao invés de fixar um percentual do seu patrimônio nessa classe de ativo. Isso pode te dar algumas vantagens, como:

- Você não elimina os vencedores. Se você fixar 5% do seu patrimônio em cripto e esses ativos se valorizarem e atingirem 8% do seu portfolio, você não venderia 3%, mas continuaria com seus pequenos aportes mensais. A ideia por trás disso seria de “não cortar as rosas do jardim a não ser que elas fiquem doentes”. Ou seja, a venda dos criptoativos viria somente se houvesse razões reais e concretas para isso;
- Como os aportes são pequenos, representam 5% da renda ou do seu montante de investimento mensal, os prejuízos (quando ocorrerem) serão pequenos, não farão tanta diferença;

A Regra dos 10 dias

Diversos estudos mostram que a valorização (os ganhos) dos mercados se dá em poucos dias do ano. Em média, excluindo os 10 melhores dias do ano, o retorno atualizado do S&P500 cai de 9.2% para 5.4%. Já para o Bitcoin, excluindo os 10 melhores dias do ano, o retorno anualizado do BTC, em média, cai de 100% para negativo. É... isso mesmo. Isso quer dizer que se você não estiver exposto ao Bitcoin nesses 10 dias você deixa de ganhar muito.

Não é possível prever esses 10 dias. Isso acontece sem avisos. O ponto chave é que se alguém não está exposto em Bitcoin e prefere acertar o “melhor dia para comprar” o risco é muito grande de perder essa janela dos “10 melhores dias do ano”.

Na verdade, existem alguns estudos gringos que afirmam que o "time in the market" ganha de lavada do "timing the market". Em uma tradução ruim, isso significa que comprar bitcoin e segurá-los por muito tempo é muito mais importante do que ficar tentando adivinhar os melhores momentos para comprar e vender seus BTCS. Você pode/deve variar sua exposição a alguns criptoativos conforme os ciclos do mercado vão se alterando, mas sempre esteja exposto, sobretudo em Bitcoin.

Até aqui, os pontos principais são: faça aportes recorrentes; pense em aportar uma porcentagem da renda e não do patrimônio; garanta que você está exposto aos criptoativos que você escolher, sem tentar achar o “melhor momento”.

Dilema entre conveniência e segurança

Agora é preciso entender como você se expor ao mercado cripto.

A questão é que não existe uma resposta certa. Existe o que se encaixa melhor para cada perfil. Nada no ecossistema cripto é oito ou oitenta. Em certo ponto, as coisas se dão de forma ambígua e se faz necessário escolher o que abrir mão para estar de acordo com outras coisas que cada um entende como “essencial” – para alguns o que mais importa são as taxas, para outros a descentralização, e assim por diante. A partir daí fica claro que existem tradeoffs e, talvez, o principal dilema está entre conveniência e segurança, como mostra a próxima figura.

Conveniência × Segurança



Como podemos ver, se expor à criptoativos através de ETFs ou fundos são a forma mais simples, mas também é o meio que se têm menos controle e gestão. Ao comprar criptos numa exchange/corretora (como a Binance, por exemplo) se tem um pouco mais de autonomia, pois é possível movimentar as moedas quando e como for oportuno, mas as chaves (que já veremos o que são) não são suas. Outra forma possível, de se expor à criptoativos, é tendo uma carteira de autocustódia gratuita no seu computador ou comprando um aparelho dedicado para guardar suas criptos e, dessa forma, gerir e custodiar seus ativos sozinho. Independente da sua escolha, se lembre que, quando você tem seus ativos e dados com terceiros, isso é uma fragilidade na sua segurança.

As três possibilidades são válidas e podem coexistir, ou seja, se pode ter criptoativos em todos esses formatos – elas não são eliminatórias. Você pode escolher estar exposto das três maneiras ou escolher um formato só.

Exchanges - aprendendo a comprar sua primeira cripto

Quando você for comprar suas criptomoedas através de uma corretora, existem três taxas que você deve estar atento: a taxa de depósito (quando manda dinheiro para a corretora), a taxa de saque (quando tira dinheiro da corretora) e a taxa de negociação (quando vende ou compra algo dentro da corretora). Pela imagem abaixo é possível ter uma visão das taxas das principais corretoras no Brasil:

Exchange	Deposit BRL	Deposit BTC	Withdraw BRL	Withdraw BTC	Passive Execute	Active Execute	Progressive Fee
Alterbank	-	-	R\$ 3,00	฿ 0.00050	-	-	-
Binance	R\$ 2,60	-	-	฿ 0.00050	0.10%	0.10%	Yes
Biscount	(min. R\$ 50,00)	-	R\$ 14,50 (min. R\$ 20,00)	(min. ฿ 0.00100)	-	-	-
BitBlue	(min. R\$ 300,00)	-	R\$ 10,00 (min. R\$ 300,00)	(min. ฿ 0.00200)	0.20%	0.20%	-
BitcoinTrade	-	-	R\$ 4,90	-	0.25%	0.50%	-
Bitnuvem	(min. R\$ 10,00)	-	0.20% (min. R\$ 10,00)	฿ 0.00002 (min. ฿ 0.00001)	0.12%	0.12%	-
Bitpreço	-	-	0.20% + R\$ 4,90	฿ 0.00020	-	-	-
Bitrecife	-	-	0.98%	(min. ฿ 0.00300)	0.20%	0.40%	-
Bitso	-	-	-	฿ 0.00020	0.20%	0.40%	Yes
Blocklane	-	-	R\$ 10,00	฿ 0.00050	0.15%	0.25%	-
BrasilBitcoin	-	-	0.50% + R\$ 4,99 (min. R\$ 10,00)	(min. ฿ 0.00015)	0.20%	0.50%	-
BULLGAIN	-	-	0.99% + R\$ 8,99	(min. ฿ 0.00300)	0.30%	0.35%	-
Coinext	(min. R\$ 50,00)	-	0.19% + R\$ 8,99 (min. R\$ 20,00)	-	0.25%	0.50%	Yes
CoinextOTC	-	-	-	-	-	-	-
Cointrade	-	-	0.90% + R\$ 10,90 (min. R\$ 20,00)	-	0.35%	0.35%	-
ComprarBitcoin	-	-	0.99% + R\$ 10,00	-	0.30%	0.30%	-
CryptoMarket	-	-	R\$ 8,90	฿ 0.00040 (min. ฿ 0.00300)	0.09%	0.09%	Yes
Foxbit	(min. R\$ 5,00)	(min. ฿ 0.00080)	(min. R\$ 10,00)	฿ 0.00040 (min. ฿ 0.00160)	0.25%	0.50%	Yes
Foxbit Invest	-	-	-	-	-	-	-
FTX	-	-	0.30% + R\$ 10,00	฿ 0.00500	0.02%	0.07%	Yes
Mercado Bitcoin	(min. R\$ 50,00)	(min. ฿ 0.00050)	(min. R\$ 100,00)	฿ 0.00040 (min. ฿ 0.10000)	0.30%	0.70%	Yes
NovaDAX	(min. R\$ 50,00)	(min. ฿ 0.00050)	1,50% + R\$ 8,90 (min. R\$ 100,00)	0,10%	0,20%	0,40%	Yes

Uma forma de comprar criptoativos é através do Peer-to-Peer (p2p). Nesse caso, se negocia diretamente com alguma pessoa, transfere o valor em reais (ou a moeda que mais convir) para o vendedor e ele envia no endereço do cliente as criptomoedas que foram negociadas. É bom frisar que existem riscos nesse tipo de operação também. É necessário certificar, de alguma forma, que essa pessoa é idônea, que já fez esse tipo de serviço outras vezes, que te garanta segurança, entre outras coisas que se julgar importante.

Nesse mesmo contexto, existem algumas palavras no universo cripto que não devem fazer parte do seu vocabulário, como por exemplo: cripto-robôs, opções binarias e rentabilidade garantia. Esses termos são, em sua grande maioria, sistemas de golpes e pirâmides. Então, fuga de qualquer produto ou serviço que te proponha esse tipo de coisa.

Para você conseguir fazer o cadastro na Binance, converter seus BRLs (reais) em BTCs (bitcoin) - como foi feito na aula - e fazer as configurações de segurança na corretora, segue os links:

Como depositar BRL na Binance

- https://bit.ly/VRC_como_depositar_BRL_na_Binance

Como converter os seus BRL (reais) em Bitcoin (BTC) ou em qualquer outra moeda na Binance

- https://bit.ly/VRC_como_converter_BRL_em_BTC

15 Dicas para Melhorar a Segurança da Sua Conta Binance -

- https://bit.ly/VRC_como_melhorar_segurança

Auto-Custódia

Muitas pessoas ficam por entender como é, na prática, “ser o seu próprio banco”. Isso poderia se traduzir quando se tem a capacidade de mover suas moedas, e gerar ganhos, sem qualquer entidade centralizadora e sem terceirizar seus ativos para quem quer que seja.

No entanto, para isso, é preciso garantir que somente você tenha acesso aos seus ativos. Matematicamente falando, quem possui o que chamamos de “chave privada” é quem é dono desses ativos. Pense numa chave mágica, uma chave secreta, que desbloqueia o acesso a determinados ativos. Seguindo o mesmo exemplo da aula 2, para

blockchain, é como se cada espaço/cédula em branco daquela “planilha” pudesse ter uma chave de acesso própria.

Todo espaço na blockchain pode ser representado por uma chave mágica que dá acesso aos seus respectivos ativos. Precisamente, um par de chaves, que seria: uma chave pública e uma chave privada – todas as moedas que existem estão associadas a uma chave pública e a uma chave privada.

Você pode estar se perguntando, “Mas como se dá a criação dessas chaves? ”. Bem, qualquer pessoa portando um número, entre 1 e 10^{77} (10 elevado a 77), pode fazer uma operação com esse número escolhido através da chamada criptografia de curva elíptica – que não vamos entrar no detalhe aqui. Essa operação gerará um outro número. Nesse exemplo, o número escolhido é a chave pública e o número que foi originado por essa operação matemática é a chave privada. Tudo isso pode ocorrer sem intermediário algum, como foi dito, qualquer pessoa com uma calculadora conseguiria fazer isso.

Pouquíssimas pessoas entendem o que ocorre por trás de uma chave pública e uma chave privada. A beleza desse processo está em ser fácil e barato derivar um número escolhido (chave pública) para gerar um outro número dentro da criptografia de curva elíptica (chave privada), e ser praticamente impossível fazer o contrário, descobrir uma chave privada a partir de uma chave pública. Qualquer pessoa conseguiria também verificar se uma chave privada está ou não associada a uma determinada chave pública – assinaturas criptográficas são fáceis de verificar e impossível de reproduzir. Contudo, a maioria dos usuários não fazem isso que acabamos de exemplificar – pegar um número e a partir dele derivar outro número numa operação de criptografia de curva elíptica. Existem aparelhos e programas específicos que fazem isso para nós e chamamos esses aparelhos de “wallets”. Wallets são programas ou aparelhos dedicados a este tipo de cálculo e verificação.

A partir do momento que se cria uma wallet você recebe uma representação memorizável dessa chave privada na forma de 12 palavras: a Seed. A sua Seed é a coisa mais importante quando se tem numa wallet.

Em cripto, uma wallet faz basicamente 3 coisas: 1) Criar uma “seed”; 2) Guardar essa seed; 3) Assinar e transmitir transações.

Uma “seed” é uma forma fácil de humanos memorizarem um código binário com 128 ou 256 bits (256 ou 512 0s / 1s). Dá para criar a sequência a partir da sua cabeça, mas provavelmente não seria randômico de verdade. Quando se gera uma seed randomicamente é muito difícil. O espaço de alternativas é praticamente infinito. Existem muitas seeds possíveis. Por isso, “adivinar” uma seed de 12 palavras é tão difícil quanto acertar o cara ou coroa 128 vezes seguidas. Já adivinar uma seed de 24 palavras é tão difícil quanto adivinar 1 dentre todos os átomos da Via Láctea.

A seed é apenas uma forma de memorizar seu endereço privado com 12 palavras. Ela é tudo que você precisa para mover seus criptoativos. Se você tiver essa chave mágica você consegue fazer isso de qualquer lugar do mundo a qualquer hora.

Segue o link para você conseguir criar sua carteira, ter sua seed e começar a dar os primeiros passos na descentralização de seus ativos:

Passo a passo para criar e usar uma carteira (metamask).

- https://bit.ly/VRC_crie_sua_wallet

Um ponto importante é que as “wallets” são criadas diretamente na blockchain. Ou seja, os dados ficam armazenados diretamente na respectiva rede. Serviços de carteiras custodiais apenas facilitam a sua criação e operação através de sua interface. Assim, caso deixem de existir - a Metamask quebrar, por exemplo - você poderá usar

qualquer outro serviço de carteira compatível, ou até mesmo, acessá-las na própria blockchain usando sua seed. Ou seja, uma seed pode restaurar o acesso aos ativos em qualquer wallet, em qualquer lugar ou momento do tempo. Então, cuide muito bem de sua seed.

Quando você quiser enviar alguma moeda para sua carteira, é necessário se atentar se essa carteira já está configurada para receber essa moeda ou se a carteira suporta a rede na qual essa moeda existe. Não é possível mandar Bitcoin para um endereço de Ethereum, por exemplo.

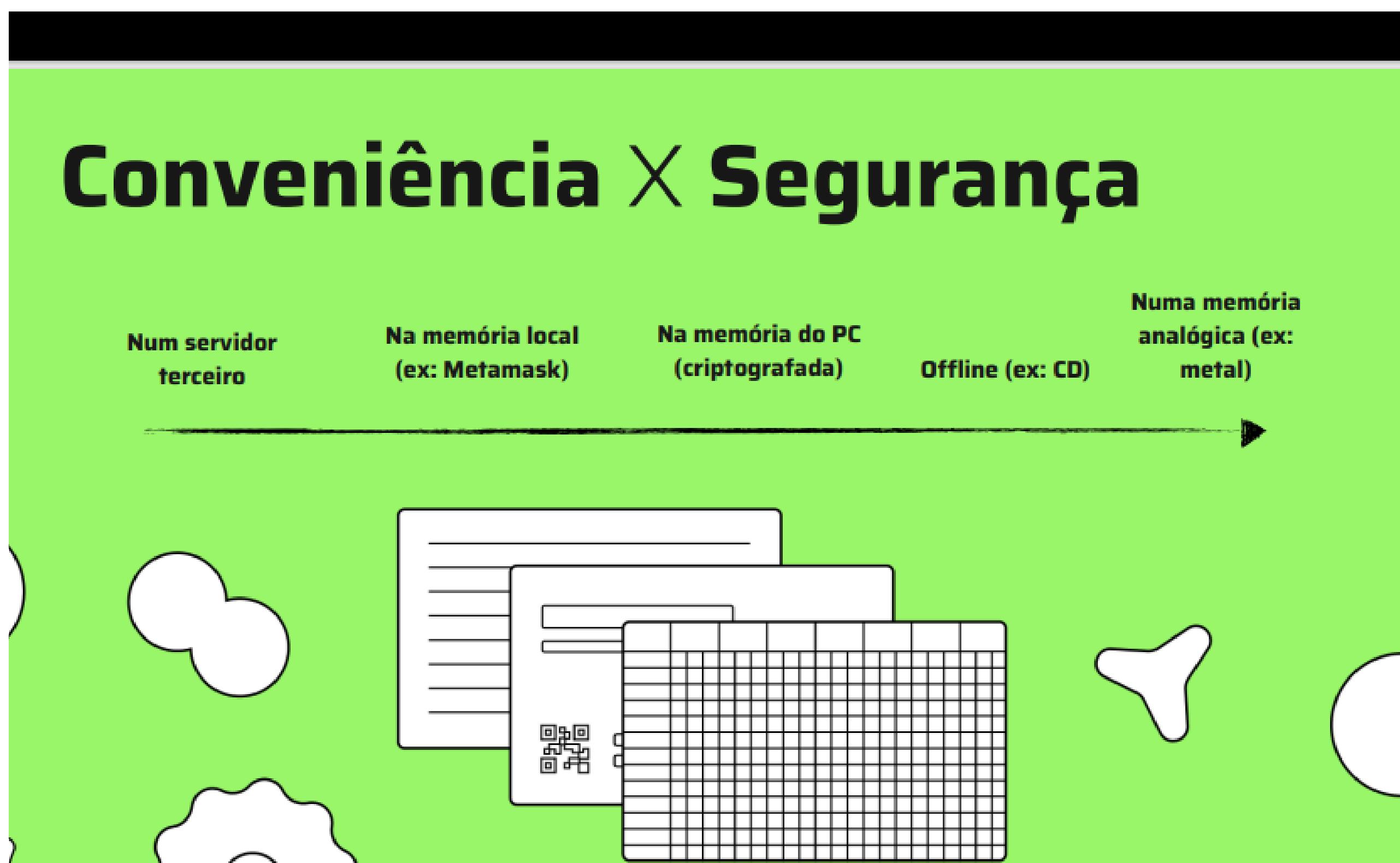
“Mas isso é seguro? ”. É muito comum esse tipo de pergunta.

Não existe uma solução universal. A segurança “ideal” é proporcional à quantia que se tem para proteger. A segurança para uma carteira de \$20 milhões é diferente da segurança para uma carteira de \$500. Quando se tem muitos ativos em custódia, é natural se preocupar com backups mais elaborados, como gravar sua seed em placas de titânio, guardar em cofres, entre outras soluções. No entanto, o mais importante é manter 3 princípios para garantir a segurança da sua seed:

- simplicidade – precisa ser fácil de ler e fácil de entender a ordem das palavras;
- redundância – tenha no mínimo 2 backups;
- descentralização – não deixe seu backup e sua gravação original no mesmo lugar;

Na imagem abaixo, temos uma comparação de como operar no universo cripto. Quanto mais para a esquerda (um servidor terceiro é equivalente a uma corretora, por exemplo) mais conveniente – via de regra, se tem custos menores, maior facilidade, mas a custódia é delegada a um terceiro e, por sua vez, as moedas são desse “terceiro”; quanto mais para a direita mais seguro – maior descentralização, autocustódia plena, mas, pagando mais caro por

isso. Para a maioria das pessoas, na progressão de segurança, usa-se hot wallets (conectadas a internet) e, por fim, hard/cold wallets (que não são conectadas a internet).



Segue um checklist de boas práticas para sua seed:

- Nunca guardar a seed em meio eletrônico;
- Nunca escrever a seed em nenhum site;
- Backups: Redundância e Descentralização;
- Renovação de senhas (a cada 6 meses, aproximadamente);
- Usar um computador virgem e que nunca vai se conectar à internet para criar carteiras de longo prazo;
- Sempre testar um setup (mandar e retirar poucos valores) antes de usar para valer;
- A primeira coisa a fazer quando você obteve sua seed, é um backup da chave. A segunda coisa: outro backup (seja em papel, papel TerraSlate, Metal, etc).

Veículos de investimento

Alguém pode ter entendido a transformação social e econômica que estamos vivendo, mas, pode ser, que essa pessoa não deseja se responsabilizar por toda gestão e custódia dos seus ativos. Nesse caso, é possível comprar produtos que dão exposição a criptoativos, como os descritos na imagem abaixo:

Comparando **Veículos**

QR CAPITAL	Hashdex	BLP ASSET
QBTC11	QETH11	HASH11
0.75% a.a	0.75% a.a	1.3% a.a
R\$15,19	R\$13,30	R\$45,04
Qualquer	Qualquer	Qualquer
Índice Monoativo	Índice Monoativo	Índice Cesta
ETFs	Hashdex	BLP ASSET
BLP20FIM	BLP40FIM	BLP100FIM
1.5% + 20% (CDI)	1.75% + 20% (CDI)	2% + 20% (CDI)
R\$100	R\$1k	R\$10k
Qualificado	Qualificado	Professional
Gestão Ativa	Gestão Ativa	Gestão Ativa
Fundos		

As duas principais vantagens em se expor ao ecossistema cripto, dessa maneira, seria a forma de tributação - que se dá de forma indireta - e a sucessão desses ativos - que, via de regra, é mais simples e objetiva. Cabe analisar o perfil de cada investidor para entender se faz sentido ou não ter esses produtos na carteira. Antes de qualquer decisão de investimento que é influenciada por questões tributárias ou contábeis, consulte o seu contador (sempre!). Isso é uma orientação genérica.

Porém há uma ressalva: cuidado com os fundos. A Instrução 555/2014 da CVM limita quanto o pequeno investidor pode se expor em ativos de renda variável no exterior (como criptomoedas). A limitação obriga fundos destinados ao varejo a operarem em um

regime inflexível (20% renda variável e de 80% renda fixa). Nesse caso, ETFs costumam ser mais “claros”. Como sugestão de análise, HASH11 e QBTC11 costumam ser baratos e cumprem bem a função de acompanhar os respectivos ativos que se propõe.