VIVER DE RENDA CRIPTO

DO BITCOIN ÀS ALTCOINS

RESUMO

AULA 02

Do Bitcoin às Altcoins

Introdução

Dois meninos, Dan Elitzer e Jeremy Rubin, fanáticos por Bitcoin há muito tempo e conhecidos pela comunidade, fizeram o que muitos gostariam de fazer: pegar vários BTC e doar para os amigos.

A iniciativa foi realizada no MIT (Massachusetts Institute of Technology), com $500 mil arrecadados, e 3.108 alunos inscritos, cada um recebeu $100 em BTC. Na época 1 BTC equivalia a $336.
Eles conseguiram monitorar o que os alunos fizeram com as doações que receberam. Viram que 30% nem chegou a fazer uma wallet - finalizar para conseguir receber as moedas -, 11% vendeu as moedas nos primeiros 14 dias, 25% vendeu nos primeiros 4 meses.
Somente 14% seguia realizando as movimentações com suas carteiras.

É como se de 11.400 alunos no MIT, somente 3.8% tivesse compreendido a mensagem de Satoshi - e alguns deles seguem na cripto-economia até hoje.

Os $500 mil, da época, hoje representam $50 milhões. Os caras que fizeram o experimento, hoje são pessoas importantes no mercado cripto - incluindo Sam Trabucco, co-CEO da Alameda Research.

A reflexão do experimento foi: mesmo pessoas com boa educação, numa faculdade referência nos EUA, venderam seus satoshis, com poucos deles guardando para posterioridade. A esperança com o curso é que mais de 3.8% mantenha-se ativo no mercado, consiga atingir a liberdade financeira e enriqueça também intelectualmente, como as pessoas do experimento.

De onde vem o Bitcoin - O mito de Satoshi

A história de Satoshi começa em outubro de 2008, quando uma mensagem é disparada a uma lista de e-mails contendo, nada menos, que os antigos Cypherpunks. No dia 31 deste mês, a mensagem Bitcoin P2P e-cash paper foi enviada para intelectuais em criptografia em computação, contendo o *whitepaper* do Bitcoin.

A ideia descrita não era nova para os Cypherpunks. Estes, eram pessoas que estudavam matemática e criptografia há muitos anos e **o conceito de dinheiro eletrônico não era estranho para eles, pois já haviam visto outros modelos no passado.** Algumas respostas ao e-mail foram céticas, mas outras ficaram animadas com a tecnologia criada por Satoshi. Um deles, foi Hal Finney, uma figura fundamental para o Bitcoin em seus primeiros passos. Ele chegou a afirmar que cada unidade do Bitcoin poderia valer $10 milhões.

Cypher = Cifra = Criptografia = Ramo da matemática dedicado a decifrar e proteger segredos.

A criptografia evoluiu, ao ponto de tornar-se uma ciência, somente após a Segunda Guerra Mundial. Um filme que ilustra isso é o Imitation Game, que narra a vida de um cientista - Alan Touring - e mostra como ele conseguiu quebrar os segredos dos países do Eixo, ajudando os EUA a ganhar a guerra. Por um tempo, a criptografia era algo voltado apenas para o âmbito militar, **chegando a considerar a criptografia como uma arma, proibindo sua exportação - softwares criptográficos e livros inclusive.**

Atualmente, boa parte de nossas comunicações utilizam a criptografia para proteger nossas mensagens. Whatsapp, Telegram são exemplos de aplicativos que usam essa proteção, fazendo a chamada “criptografia de ponta a ponta”, ou seja, somente os envolvidos no diálogo conseguem ler a mensagem.

Antes da guerra, a principal forma de criptografia era a chamada Criptografia Simétrica. Neste caso, utiliza-se a mesma chave para cifrar e decifrar a mensagem, ou seja, usa-se o mesmo algoritmo para criptografar e descriptografar o conteúdo. Assim, caso alguém descobrisse a cifra, conseguia-se facilmente identificar e ler a mensagem.

Para resolver este problema, cientistas criaram a chamada Criptografia Assimétrica. Nela, a cifra utilizada para codificar a mensagem era distinta daquela para descriptografá-la. Essa pequena mudança, transformou a codificação das mensagens. Com este novo modelo, mesmo que outra pessoa descubra a cifra responsável por criptografá-la, não é possível decifrá-la.

A evolução da criptografia, somada às reiteradas tentativas de pessoas em criarem um dinheiro eletrônico, culminaram no desenvolvimento do Bitcoin.

Apesar de outras iniciativas, somente o Bitcoin moveu a “Janela de Overton”. Esta, pode ser definida como a gama de ideias toleráveis no discurso público. Com a gradual introdução dos conceitos criptográficos e do uso da tecnologia para aperfeiçoá-lo, o Bitcoin conseguiu ampliar essa gama de ideias. Sua aceitação aumenta a cada dia que continua funcionando corretamente. A ideia de uma moeda sem uma entidade central, algo inesperado nos anos 80, hoje é amplamente aceita pela sociedade, seja civil ou governamental.

A estimativa feita por Hal Finney de 1 BTC valer 10 milhões de dólares era impensável, até então. No entanto, o tempo tem demonstrado a possibilidade de este feito ser realizado.

Hal, apaixonado por matemática, desenvolvedor de games e participante dos Cypherpunks é apontado como uma das primeiras pessoas a postar sobre Bitcoin no Twitter e a interagir com a blockchain do Bitcoin.

Ele e todos os outros Cypherpunks já sabiam que qualquer indivíduo com um projeto de dinheiro eletrônico que desse certo, seria cooptado e perseguido pela lei para acabar com ele. Hashcash, E-gold, E-cash são alguns exemplos.

Por isso, Satoshi Nakamoto, após alguns anos interagindo com a comunidade, sumiu em 2011, entregando sua criação à comunidade. Seu objetivo era captar pessoas interessadas em contribuir com a rede e sair de cena, deixando aos demais participantes a responsabilidade de tocar para frente sua criação.

Sem identificar sua identidade, há um mistério sobre quem é Satoshi Nakamoto até hoje. Um dos principais apontados como criador do Bitcoin é Hal Finney. Ele trocou constantemente mensagens com Satoshi, ajudava no código e participou da primeira transação da história da blockchain do Bitcoin. Em 2010, foi diagnosticado com ALS, uma síndrome motora onde ocorre a degeneração de neurônios motores com consequente perda progressiva dos movimentos. Costuma ser fatal em 3 a 5 anos. Com poucos movimentos nas mãos, desenvolveu um mecanismo para conseguir continuar programando, utilizando os olhos. Assim, ajudava na correção do código do Bitcoin usando seus olhos para contribuir com a rede.

Em 2014, Hal Finney faleceu por consequências da doença e criogenou seu corpo, com a expectativa que pudesse ser despertado no futuro. Essa ideia de Hal Finney, vai ao encontro da filosofia do Bitcoin: a utopia Cypherpunk do futuro. A perspectiva da evolução tecnológica no futuro, e a preocupação em ter uma reserva de valor que transcende gerações, é a justificativa para a criação do BTC.

Seu dinheiro é programado para perder valor

Todo governo tem uma meta de inflação. Com o aumento da inflação, aqueles que usam o dinheiro governamental para poupar empobrecem. Uma inflação de 10.6% ao ano reduz o valor do dinheiro pela metade em 7 anos.

Por isso as pessoas escolhem outras formas de investimento: ações, CDI, título do tesouro, commoditties, etc.

Toda vez que novas moedas são emitidas e entram em circulação, esse dinheiro é distribuído de maneira não-uniforme. Quem está mais perto deste dinheiro, receberá a maior porção. Em contrapartida, aqueles distantes do Estado, terão acesso a poucas quantidades.
Esse conceito foi definido como Efeito Cantillion.

Em comparação, o Bitcoin não possui qualquer correlação a este conceito das moedas fiduciárias. Ao longo dos anos, muitas narrativas foram construídas sobre o que ele é, e sua utilidade. Uma das qualidades que o BTC vem demonstrando é a de ser um dinheiro programado para ganhar valor (ao contrário dos outros).

Não significa que ele não sofra desvalorizações, mas que as emissões de BTC não são alteradas de acordo com as políticas monetárias escolhidas por entes centralizados. Haverá volatilidade, mas, no longo prazo, a perspectiva é de escassez da moeda e apreciação em seu valor.

No Bitcoin há uma “Não-Política Monetária”, funcionando como um cronograma que trata das emissões de BTC ao longo do tempo. A cada “halving” - aproximadamente 4 anos - o número de moedas criadas desacelera pela metade. Até chegar num limite de 21 milhões de BTCs.

Halving é o termo dado a este momento que diminui para a metade o número de bitcoins emitidos a cada bloco, como recompensa ao minerador.

Nunca haverá mais de 21M de Bitcoins emitidos. Este número foi arbitrado por Satoshi e inserido em seu código de programação e é praticamente impossível alterar esta regra do algoritmo do Bitcoin. Essas e outras regras estão disponíveis no site do Bitcoin.org, sendo transparentes a quaisquer usuários.

Toda essa estrutura criada por Satoshi poderia não ter dado certo, ficando somente como lembrança para os nerds. Mas a história tem se desenrolado de forma diferente. A primeira compra física que desencadeou o start nas pessoas pelo Bitcoin foi a aquisição de uma pizza utilizando BTCs, em 2010, por Laszlo Hanyecz, Ele pagou 10 mil BTCs nas 2 pizzas, o dia ficou conhecido como Bitcoin Pizza Day - foi um feito catalisador na comunidade bitcoiniana, porque a partir daí começou a demonstrar às pessoas a aplicação do dinheiro eletrônico.

Endereços, Carteiras e Blocos

Uma analogia para compreender o que é o Bitcoin é entendê-lo como uma base de dados, tipo uma planilha de Excel. A planilha, internamente, implementa mecanismos para organizar as informações contidas nela:

- Cada coluna nessa planilha representa um endereço (uma pessoa).
- Sempre que houver uma atualização na rede, é como se essa grande planilha recebesse uma linha nova (unidade de tempo, equivalente ao bloco).
- Conforme o tempo passa, linhas novas são inseridas e, com novas pessoas participando da rede, novas colunas são criadas.
- Uma carteira é uma interface para ler o saldo de um endereço específico.

A esta planilha/base de dados, dá-se o nome de Blockchain.

Nela, constam todas as informações da história do Bitcoin. Deste modo, ao fazer o download do Bitcoin Core, um usuário tem acesso a todas as transações realizadas até hoje, com atualizações a cada 10 minutos.

Mesmo sendo possível acessar a Base de Dados do Bitcoin, poucas pessoas a conhecem. Para suprir a necessidade da maioria dos usuários, é suficiente apenas a interação com a interface gráfica para acessá-las. Estas, são fornecidas através de softwares ou empresas - corretoras, por exemplo.

Ainda assim, há usuários que fazem o download da Base de Dados e rodam seus nós (dispositivos que armazenam as informações da rede do Bitcoin e recebem as atualizações da Base de Dados).

Cada célula da planilha do Bitcoin recebe o nome técnico de UTXO, Unspent Transaction Output. A base de dados do Bitcoin funciona da seguinte maneira: quando o usuário X tem 50 BTCs e envia 10 BTCs ao usuário Y, acontecem duas coisas:

- O usuário Y, receptor da transação, recebe 10 BTCs.
- O usuário X, transmissor dos BTC, recebe o "troco" correspondente a 40 BTCs.

Através da lógica dos UTXOs, observa-se que não foram somente deduzidos 10 BTCs do saldo do usuário X, mas foram gerados 40 BTCs de "troco" e enviados ao endereço original da transação.

A Teoria dos Ciclos

Esse fenômeno, *bitcoinização,* é uma mega tendência. Não é um *hype,* mas o futuro monetário da sociedade. Contudo, ainda está em processo de amadurecimento e passando por ciclos. O Bitcoin, bem como todas outras tecnologias, está **sujeito ao efeito Lindy. Quanto mais tempo sobrevive, maior é a dificuldade de minar sua evolução.**

Ao longo desta tendência geracional, o Bitcoin vem desenvolvendo e trazendo consigo o crescimento de diferentes indústrias no setor. Por isso, todos criptoativos estão correlacionados à precificação do bitcoin. Sendo assim, analisar seus ciclos de preço - bear market, bull market, acumulação e reacumulação - são o meio mais eficiente de compreender o mercado.

O período de aumento de preço do Bitcoin é chamado de bull market. O período de quedas no preço do Bitcoin é chamado de bear market. Os períodos entre altas e baixas, quando o preço do Bitcoin mantém-se estável, é chamado de acumulação.

Nos últimos ciclos do Bitcoin, foi possível observar que:

- Meses após o halving, o bitcoin começa aumentar seu valor de mercado, atingindo suas altas máximas.
- Passados alguns meses deste evento do “cronograma” do Bitcoin, o BTC tende a sofrer desvalorizações.
- Com a aproximação do próximo halving, o preço do BTC estabiliza, até que retoma o crescimento, reiniciando um novo ciclo.

Mas a pergunta é: qual a melhor hora de comprar?

Um indicador útil para isto é o **MVRV,** que corresponde a Capitalização de Mercado/Valor Realizado.

Capitalização de Mercado *= Valor de Mercado do Bitcoin*

Valor Realizado *= Valor que todas as moedas de Bitcoin tinham se levar em conta a última vez que se movimentaram na blockchain. Pode ser entendido como o valor do Bitcoin se levar em conta a última compra de cada moeda.*

Dividindo estes dois valores, você conseguirá tirar uma média e verificar se a maioria dos investidores está no lucro ou prejuízo:

Se o valor estiver acima de 1, significa que a rede está no lucro.

Se o valor estiver abaixo de 1, significa que a maioria dos detentores estarão no prejuízo.

A melhor compra é realizada quando o MVRV está **abaixo de 1.**

É interessante reduzir riscos quando o MVRV está **acima de 3.5.**

OBS: *o MVRV deve ser utilizado para o Bitcoin e não para outras criptomoedas. Uma vez que ele é um indicador cíclico, faz mais sentido aplicá-lo ao BTC.*

A origem das Altcoins

Altcoins são "moedas alternativas". Houve uma "explosão cambriana de sistemas monetários". O sucesso do Bitcoin levou vários desenvolvedores a lançarem suas próprias versões do Bitcoin.

O jeito mais famoso de lançar uma nova moeda era realizando o chamado fork: consiste em baixar o código de uma criptomoeda que já existe, trocar algo nesse código e lançar uma moeda nova.

Por faltar originalidade e fundamento na maioria dos projetos, muitos não resistem aos ciclos de baixas do mercado cripto. Ao analisar as top 10 em capitalização de mercado dos bull markets, percebe-se que poucas moedas sobreviveram.

Uma forma eficiente para posicionar-se em altcoins é encontrar altcoins que poderão performar melhor que o Bitcoin no longo prazo ou utilizá-las para conseguir maiores lucros durante os ciclos de alta e vendê-las para comprar mais satoshis.

O interesse dos investidores nas altcoins consiste sempre com os *bull markets* do Bitcoin, diminuindo sua dominância no mercado neste período. Com a queda do Bitcoin, as altcoins sofrem desvalorização ainda maiores e os investidores voltam para o Bitcoin, aumentando sua dominância no mercado novamente.

Mesmo com os ciclos de alta e baixa, uma altcoin tem sobrevivido e crescido nos últimos anos: Ethereum. Fundada por Vitalik Buterin, o desenvolvedor prodígio via genialidade na criação de Satoshi Nakamoto, mas queria ir além. Sua ideia era conseguir escrever na Base de Dados do Bitcoin não só valores, mas implementar programas sobre ela. Por isso, idealizou e criou, junto de outros desenvolvedores, a Ethereum.

As duas blockchains têm culturas completamente diferentes. Enquanto os *bitcoiners* visam ser conservadores, obter uma rede robusta, sem líderes e afirmam ter um projeto "pronto", os adeptos da Ethereum visam constantemente implementar melhorias, adotam o lema "*move fast, break things"* e possui líderes importantes para sua comunidade, como o próprio Vitalik Buterin.

Por isso a Ethereum é considerada a principal altcoin do cripto-mercado.

Mas a questão é: quais são os critérios para avaliar uma altcoin? Você deve analisar seus **fundamentos e esquecer seu *whitepaper*.**

Para localizar os fundamentos, faça perguntas:

- O sistema cripto econômico atende uma necessidade real do mercado? O token paga por um serviço demandado de fato?
- Se todos os desenvolvedores morressem amanhã, estaria funcionando?
- O incentivo dos principais stakeholders envolvidos é alinhado com a perenidade da rede?

Além disso, você pode utilizar o modelo mental chamado **Trilema de Zooko** - um trilema em que se pode ter somente 2 de 3 atributos: **Baixo Custo, Descentralização e Segurança**.

Uma criptomoeda não consegue ter as três características. Por isso, quando avaliar uma moeda, veja o que o time de desenvolvimento está priorizando. **Muitas delas abrem mão da Descentralização.**