CRIPTO & MOEDAS: UMA BREVE HISTÓRIA

Boas-vindas ao mini e-book de complemento sobre criptomoedas.

Nos vídeos, você acompanhou um pouco da história do nascimento das criptomoedas, agora vamos explorar um pouco mais sobre esse acontecimento, sua evolução e o porquê da sua importância.

Blockchain
ACADEMY

Primeiro, precisamos pensar em um conceito básico: O que é dinheiro?

Se pudermos resumir, o dinheiro é um dos **maiores instrumentos de facilitação** da vida em sociedade e não foi feito para consumo, mas sim para ser utilizado como **meio de troca**, possibilitando que as pessoas acessem bens e serviços.

O dinheiro resolve um grande problema: a coincidência de desejos.

No passado, quando a ideia de dinheiro (esse bem intermediário) não existia, as pessoas transacionavam por meio do escambo. No entanto, o **escambo**[1] não funciona em grande escala.

No modelo das trocas diretas, as duas pessoas têm que realizar um grande trabalho de coordenação para realizar uma troca, funcionando da seguinte forma:

1 - Tenho determinado item em minha posse: uma laranja.
2 - Quero algum outro item: uma maçã.
3 - Devo encontrar alguém com uma maçã e que queira trocar por uma laranja.

Pensando nos dias de hoje, isso fica bastante difícil, né?

Além disso, o modelo das trocas diretas traz 3 grandes problemas de coordenação:

Escala - os bens a serem trocados podem ser de escalas totalmente diferentes.
Durabilidade - os bens podem ter durabilidades diferentes.
Localidade - os bens podem não estar na mesma localidade e serem de difícil transporte.

EVOLUÇÃO DO DINHEIRO

Estima-se que o dinheiro, como ideia de meio de troca, já tenha mais de dois mil anos. Claro que era tudo bem diferente dessas notas e moedas que talvez você tenha na carteira hoje, esse tipo de dinheiro só começou a aparecer por volta do século VII na China.

Essa breve introdução serve para você perceber há quanto tempo a ideia do dinheiro existe e o gigantesco espaço de tempo que foi necessário para sua evolução até os dias atuais. Já estava na hora de surgir uma grande revolução e mudar a forma como todos nós lidamos com o dinheiro.

Escambo[1]: é o nome dado para um troca entre bens sem que para isso haja a necessidade de ter uma moeda intermediando. Nesse caso, um produto é trocado por outro. Para isso as duas partes precisam estar de comum acordo.

Dinheiro Digital:

Bitcoin não foi a primeira tentativa...Mas sim a primeira que deu certo.

Os cypherpunks (uma comunidade com diversas pessoas entusiastas da computação nos anos 90) acreditavam que era preciso ter uma forma de dinheiro nativamente digital, que teria que estar **livre da intervenção do governo**. Afinal, a própria Internet já não tinha fronteiras e era internacional! Uma moeda nativa da Internet deveria colocar todos, independentemente da nacionalidade, em **pé de igualdade**.

Além disso, um sistema como esse estaria fora das mãos dos agentes intermediários (como governos e grandes empresas) capazes de vigiar tudo que fazemos e concentrando muito poder. Além do mais, depois de testemunhar as muitas crises financeiras e hiperinflações no século XX, os Cypherpunks acreditavam que o sistema econômico mais sólido era aquele **que ninguém podia manipular**.

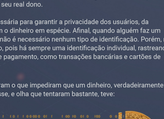
Um dinheiro eletrônico, **e-cash**, como era chamado, seria a grande ferramenta de privacidade para as pessoas. Para criar essa dinheiro, duas coisas eram necessárias:

1 - Um **sistema de registro** para garantir que o dinheiro só seria gasto uma vez e que somente pudesse ser gasto por seu real dono.

2 - A anonimidade, que era necessária para garantir a privacidade dos usuários, da mesma forma que funciona com o dinheiro em espécie. Afinal, quando alguém faz um pagamento em cédulas físicas, não é necessário nenhum tipo de identificação. Porém, no mundo digital isso é complicado, pois há sempre uma identificação individual, rastreando os usuários nos mecanismos de pagamento, como transações bancárias e cartões de crédito.

Esses dois problemas-chave foram o que impediram que um dinheiro, verdadeiramente digital e descentralizado nascesse, e olha que tentaram bastante, teve:

- **e-Cash** em 1989
- **Hashcash** em 1997
- **b-money** em 1998
- **Bit gold** em 1998



Todos eles esbarraram em um dos problemas chave, mas também graças a eles os erros puderam ser corrigidos durante o tempo, até chegarmos na criação do bitcoin em 2008. É isso tudo é super natural quando estamos falando de inovação!

Resumão:

Já vimos muita coisa até aqui, agora vamos tentar retomar alguns conceitos mais importantes e juntar tudo isso.

O Bitcoin é uma proposta de sistema financeiro alternativo, que visa dar privacidade e poder para os usuários. Esse sistema tem origens ligadas ao movimento cypherpunk, da década de 90, que queriam dar ferramentas para proteger a privacidade das pessoas frente ao mundo digitalizado controlado por grandes empresas/governos.

O Bitcoin não foi um projeto criado do zero, por um louco que se escondeu atrás do pseudônimo de Satoshi Nakamoto. Existiram vários projetos de dinheiro digital que vieram antes do Bitcoin, mas fracassaram por diversas razões. Esses projetos, no entanto, contribuíram para que o Bitcoin fosse criado, **pois cada fracasso trouxe lições importantes.**

A tecnologia blockchain **já existia antes do bitcoin**, mas a sua aplicação para a rede que deu vida à criptomoeda foi fundamental para seu sucesso. A partir dessa aplicação outros tipos de criptomoedas também puderam ser criadas, utilizando parte da tecnologia aplicada no bitcoin.

É preciso sempre deixar claro que existe essa **relação direta** da evolução do dinheiro com o bitcoin, não é atoa que ele é considerado reserva de valor por conta da sua escassez programada. **O bitcoin abriu as portas para a criptoeconomia** e graças a ele nós poderemos continuar avançando nesse mundo dos investimentos cripto!

Blockchain
ACADEMY