Um curso de Bitcoin gratuito e de código aberto desenvolvido pela Area Bitcoin

---

Índice - Bitcoin 4 All -
Por dentro do Bitcoin: como Bitcoin funciona?
(descentralização, blockchain e teoria dos jogos)

---

6. Como Funcionam as Transações

6.1 Transações digitais com fiat dependem de intermediários
6.2 Bitcoin permite enviar valores como dinheiro físico

---

7. As Tecnologias Fundamentais

7.1 Criptografia, timestamps e redes P2P
7.2 O papel do mecanismo de consenso
7.3 A coordenação sem necessidade de confiança

---

8. Os Três Componentes da Rede Bitcoin

8.1 O código: regras públicas e auditáveis
8.2 Mineradores: inclusão de blocos e segurança da rede
8.3 Nodes: verificação, autonomia e resistência a ataques

---

9. O Poder dos Nodes

9.1 Qualquer pessoa pode rodar um node
9.2 Custo baixo e grande impacto
9.3 Como nodes impedem fraudes e centralização

---

10. Contabilidade Pública e Verificável

10.1 Por que a contabilidade do Bitcoin sempre fecha
10.2 Comparativo com a opacidade dos bancos centrais
10.3 Bitcoin é audível por qualquer pessoa

---

11. Bitcoin Não é uma Empresa

11.1 Criptomoedas com líderes vs Bitcoin horizontal
11.2 Por que o Bitcoin não tem marketing nem CEO
11.3 O protocolo avança por consenso, não por ordens

---

12. Resiliência à Censura e a Ataques

12.1 Bitcoin resiste há mais de 10 anos a ataques contínuos
12.2 Como sistemas centralizados falham mais facilmente
12.3 Projetos que se dizem descentralizados, mas não são

---

13. Por Que Nenhuma Cópia Superou o Bitcoin

13.1 Forks e clones de 2015 a 2018
13.2 Por que nenhuma “nova versão” do Bitcoin vingou
13.3 Efeito de rede e confiança descentralizada não se replicam

---

14. Incentivos e Teoria dos Jogos

14.1 Atacar é caro, colaborar é lucrativo
14.2 Bitcoin transforma adversários em aliados

---

15. O Problema dos Generais Bizantinos

15.1 A analogia da guerra: falta de coordenação
15.2 P2P, blockchain e consenso como solução confiável

---

16. Blockchain: O Registro Imutável

16.1 O que é a timechain (ou blockchain)
16.2 Blocos encadeados: o papel do hash
16.3 A costura digital: alterar o passado afeta todo o sistema

---

17. Funções de Hash e Verificação

17.1 O hash resume e protege as informações
17.2 Qualquer alteração muda o hash e invalida o bloco
17.3 A verificação constante por nodes e mineradores

---

18. Forks: Atualizações no Protocolo

18.1 O que são forks e por que ocorrem
18.2 Soft fork vs hard fork

Bitcoin 4 All - Texto Completo

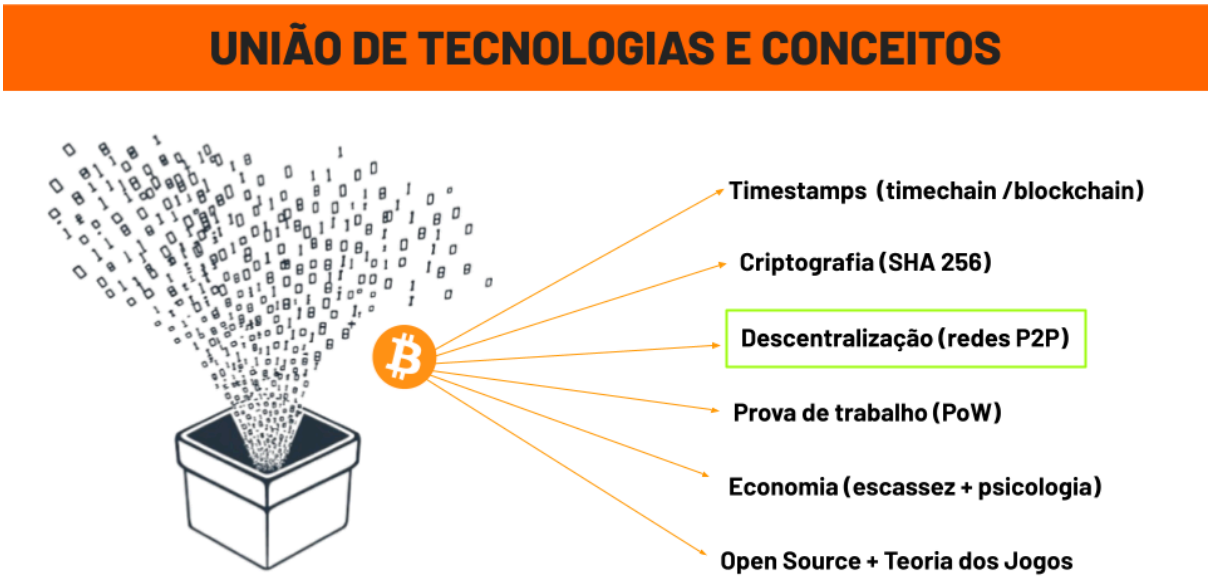
Bitcoin 4 All é um curso gratuito e de código aberto criado pela Area Bitcoin. O objetivo é ajudar mais pessoas a entender o Bitcoin e inspirar qualquer pessoa a se tornar um multiplicador da educação sobre Bitcoin.

Sobre este e-book

Publicado pela Area Bitcoin – 2025

Por dentro do Bitcoin: como Bitcoin funciona?
(descentralização, blockchain e teoria dos jogos)

Nessa aula você vai mergulhar no funcionamento do Bitcoin, aprendendo sobre suas características, como funciona a blockchain, a mineração, os halvings e conceitos técnicos fundamentais. Não se preocupe se você não entender tudo de primeira. É normal precisar revisar e reassistir algumas vezes para que o aprendizado se consolide. Com o tempo, os conceitos vão se encaixar e fazer cada vez mais sentido.



(Slide 88) - Bitcoin 4 All

Como você viu na aula 1, Bitcoin é a junção de várias tecnologias e conceitos. A descentralização é o que separa Bitcoin de qualquer outra invenção na história recente.

DESMATERIALIZAÇÃO E DESCENTRALIZAÇÃO

Tecnologia desmaterializa funções

Descentraliza o acesso a valor e desmaterializa o sistema financeiro global

A internet do valor

(Slide 89) - Bitcoin 4 All

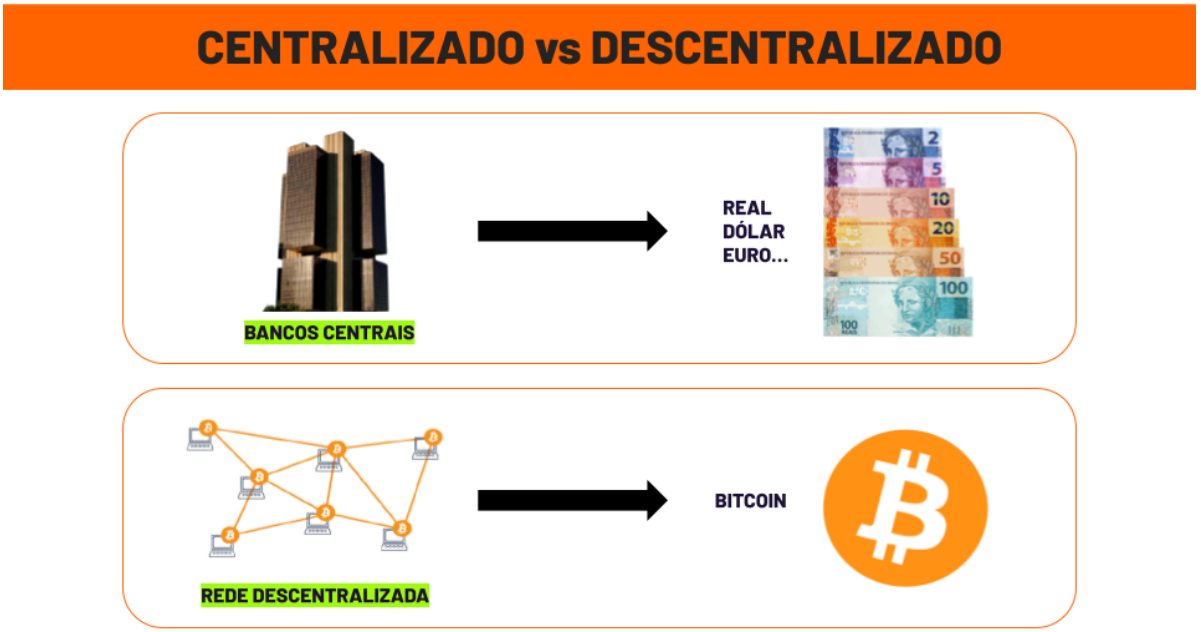
E o que está acontecendo nas últimas décadas é a ação de duas forças tecnológicas agindo ao mesmo tempo: a descentralização e a desmaterialização das coisas. A desmaterialização começou nos anos 90 com computadores e smartphones, que condensam e desmaterializam diversos dispositivos que antes a gente só conhecia na forma física. Rádio, agenda, televisão, câmera, calculadora, fax, tudo isso em apenas 20 anos foi desmaterializado e digitalizado para a palma da sua mão, no seu celular. Virou tudo em um.

Bitcoin continua essa mudança evolutiva e tecnológica trazendo ambos esses efeitos para a economia e para o dinheiro. Ou seja, o bitcoin descentraliza acesso a valor para qualquer pessoa de qualquer lugar do mundo sem restrição de acesso e também desmaterializa o sistema financeiro bancário de agências, cofres, caixas eletrônicos e caixas fortes. E se a internet já descentralizou a informação e mudou o mundo, imagina o que o Bitcoin não pode fazer ao descentralizar valor e poder de decisão. Além de desmaterializar bancos centrais, bancos comerciais e as propriedades de um dinheiro sólido.

(Slide 90) - Bitcoin 4 All

Bitcoin só consegue fazer isso porque é descentralizado. Sem descentralização, Bitcoin seria uma empresa. É a descentralização que diferencia Bitcoin de todo o resto e que proporciona imutabilidade. Se não há ninguém tomando decisões por outras pessoas significa que é uma rede que é dificil de mudar. Para que seja feita qualquer mudança, quase todos os participantes precisam concordar em mudar. E isso não é nada fácil nem no Bitcoin e nem em qualquer sistema que envolva milhares de seres humanos tomando decisões. A descentralização é o que garante a imutabilidade das propriedades e que as regras do bitcoin seguirão as mesmas. Traz confiança de que ninguém conseguiria monopolizar ou corromper o bitcoin autoritariamente.

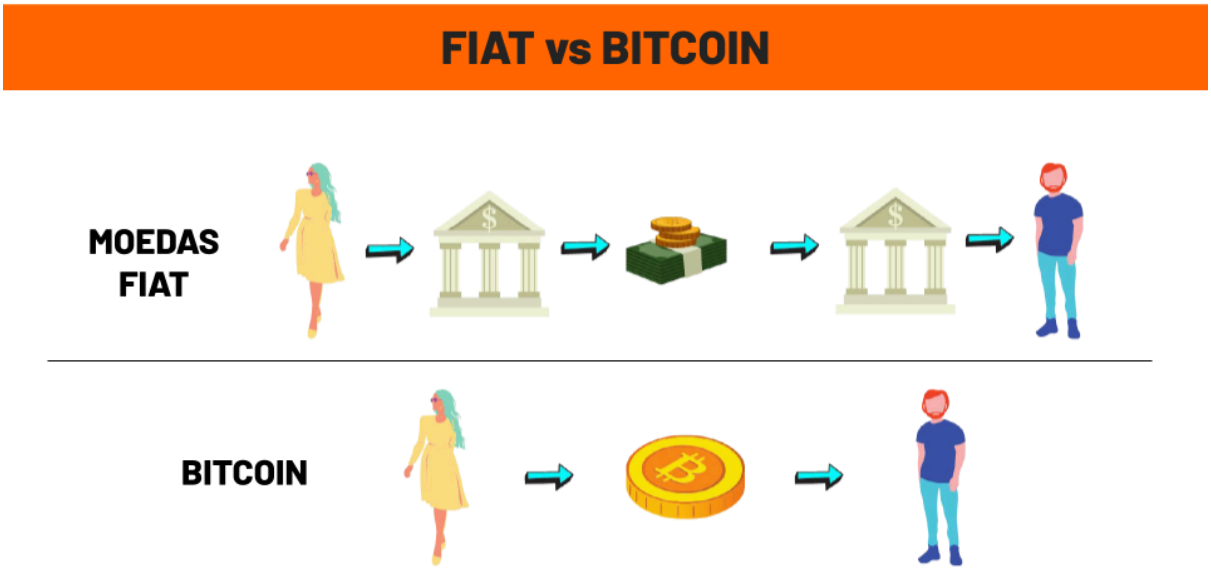
A descentralização do Bitcoin acontece porque ele é uma rede P2P, ponto a ponto. É formada por computadores que se conectam entre si e seguem regras com as quais todos concordam. Não existe um servidor central coordenando ou armazenando os dados, como acontece em redes centralizadas. Também quer dizer que não há um único ponto de falha. Se qualquer computador conectado à rede cair, for destruído ou atacado, a rede sobrevive e segue funcionando porque existem milhares de outros cumprindo a mesma função de forma independente.



(Slide 91) - Bitcoin 4 All

Na prática significa que não existem intermediários no Bitcoin. Cada pessoa pode se conectar à rede sem depender de ninguém, sem precisar pedir permissão e sem a possibilidade de ser impedida por terceiros. Ao contrário do dinheiro fiat que é centralizado e que você depende de inúmeras entidades, ministro da economia, diretor do banco central, instituições de pagamento, casa da moeda, bancos e etc para ter acesso ao sistema.

Bancos centrais determinam as políticas monetárias e você não tem a opção de não seguir as regras, você é forçado a seguir. Daí vem a expressão “curso forçado”. Já os bancos comerciais dão acesso ao sistema. Para participar você precisa pedir permissão para eles e, se você não preenche os requisitos, você pode não ter uma conta bancária ou podem até fechar a sua conta.



(Slide 92) - Bitcoin 4 All

Outra grande diferença é na hora de fazer as transações.

Atualmente, quando você faz uma transação digital, você tem que pedir para o seu banco enviar um valor para o banco de outra pessoa, e depois o banco dessa pessoa deposita o valor na conta correspondente. Em uma transação entre duas pessoas usando o sistema bancário fiat, existe pelo menos um intermediário, um banco, entre duas pessoas. Se essas duas pessoas tiverem conta em bancos diferentes, então vão ser dois bancos intermediando a transação.

Já através do Bitcoin é como fazer uma transação de dinheiro físico, igual quando você compra algum produto e você entrega as notas direto na mão da outra pessoa. Com o bitcoin você envia o valor direto para a carteira de outra pessoa sem passar necessariamente por algum tipo de intermediário fiat ou banco. A não ser que você queira que passe, que você escolha transacionar através de exchanges por exemplo, mas é uma escolha, não uma via obrigatória. Isso muda completamente a forma como o sistema financeiro funciona, porque hoje o sistema fiat depende desses intermediários para transferir valores online.

Foi através de criptografia, timestamps, redes p2p e um mecanismo de consenso robusto que Satoshi Nakamoto conseguiu digitalizar o sistema financeiro como um todo, só que sem precisar de governos ou bancos.

(Slide 93) - Bitcoin 4 All

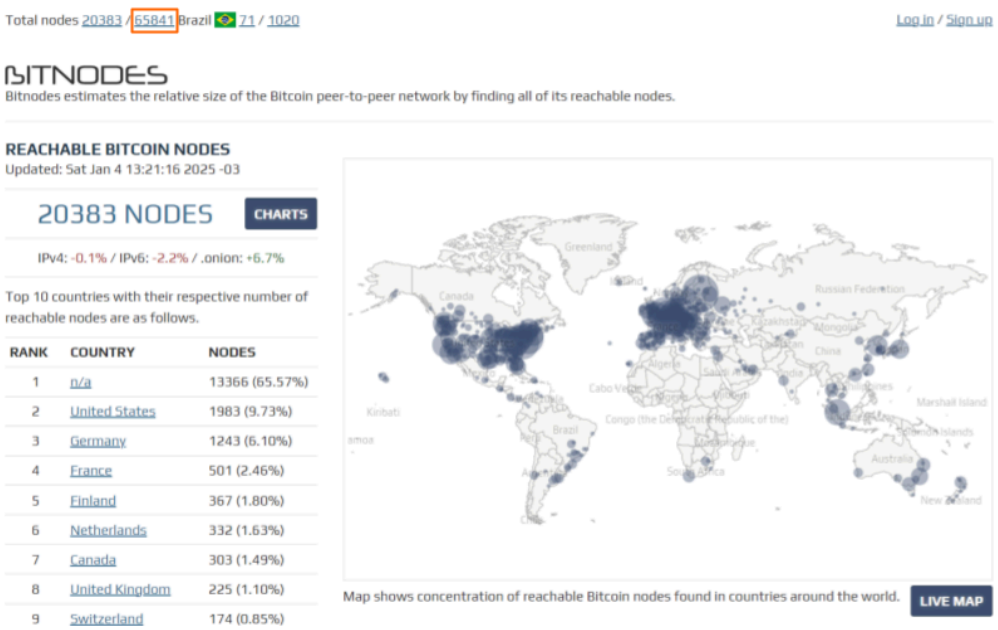
A rede Bitcoin é formada pelo código, pelos mineradores e pelos nodes. O código é um conjunto de regras em forma de códigos computacionais e criptografia que guiam os participantes para se coordenarem entre si. Ele determina como os registros serão feitos e como a rede bitcoin deve funcionar. O código é público e qualquer pessoa pode sugerir modificações, auditar para encontrar bugs e até copiar. É esse código que é dificil de modificar e monopolizar, ele é rodado por milhares de participantes e para modificar ele de forma válida é necessário que praticamente toda a rede concorde em rodar uma versão modificada.

Você pode conferir o github do Bitcoin, onde os desenvolvedores debatem atualizações e onde você também pode contribuir se quiser. Eu vou deixar o link do Github do Bitcoin aqui embaixo da aula. O código funciona através de softwares e o mais usado é o Bitcoin Core, uma implementação da versão original criada por Satoshi Nakamoto.

Já os mineradores são os participantes que propõem os blocos, inserem as transações e defendem a rede de ataques através de poder computacional. São eles os primeiros a receber Bitcoin da rede a cada bloco minerado.

E o terceiro tipo de participante da rede são os nodes. Nodes são os nós, são computadores comuns que verificam se os mineradores estão seguindo o consenso determinado pelo código. Os nodes são agentes potentes de descentralização, porque é a partir deles que qualquer pessoa pode ter uma cópia da blockchain Bitcoin no seu próprio computador, decidir qual versão do código rodar e fazer parte da rede bitcoin com autonomia para enviar suas próprias transações sem depender de ninguém. Inclusive se os

mineradores se juntarem para atacar o Bitcoin, são os nodes que têm poder de impedir que esse ataque seja efetivo. Isso inclusive já aconteceu na chamada guerra de blocos que aconteceu em 2016.



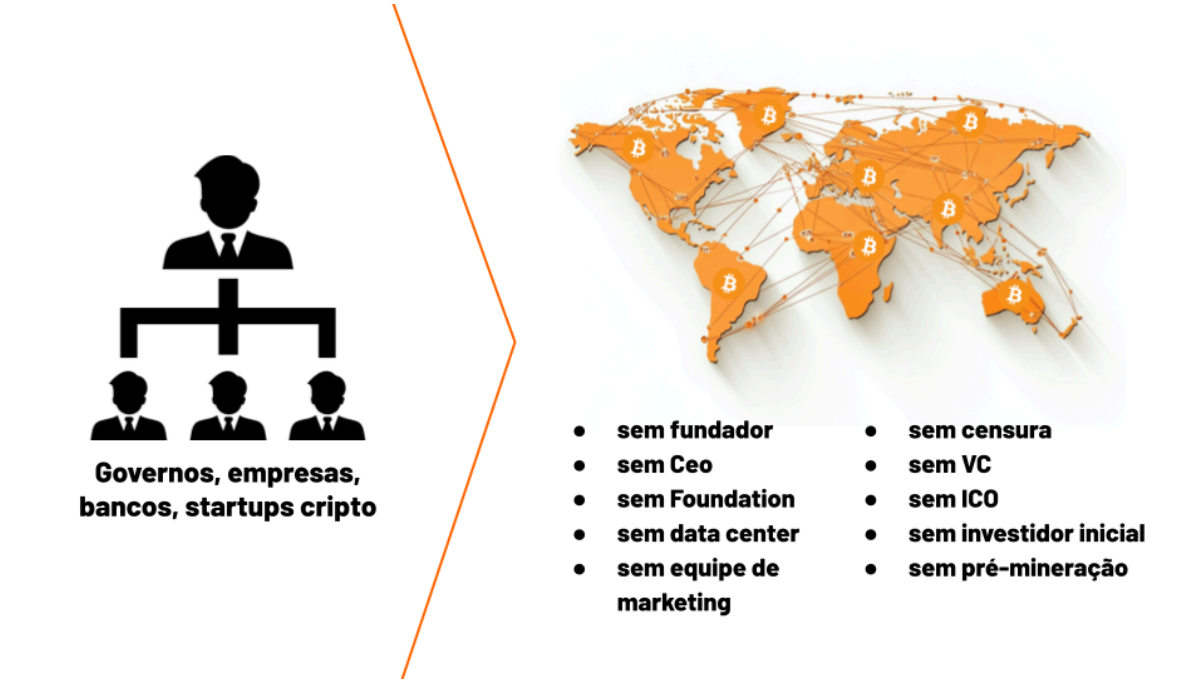
(Slide 94) - Bitcoin 4 All

Segundo o site Bitnodes, existem mais de 65 mil nodes Bitcoin funcionando globalmente e a maioria deles, 65%, não tem uma localização exata identificada. São esses milhares de nodes em computadores comuns conectados entre si que tornam a rede Bitcoin o sistema computacional mais forte, resistente e acessível para qualquer pessoa em qualquer lugar do mundo verificar. Qualquer pessoa pode rodar um node e o custo é baixo, você pode rodar um node inclusive em um computador velho que você tem em casa.

Os nodes verificam o tempo todo os registros. É por isso que a contabilidade da rede Bitcoin é redonda, porque os nodes verificam constantemente se as transações fecham e se o número de moedas circulando está correto. É um sistema de registros distribuído, em que a contabilidade sempre bate certinho, isso também é algo poderoso e único.

(Slide 95) - Bitcoin 4 All

Bancos centrais não permitem que você olhe as contas internas deles ou opine diretamente nas reuniões. A contabilidade dos bancos centrais é privada e feita à portas fechadas. A população depende dos dados fornecidos pelo Banco Central e não pode verificar de forma independente ou opinar diretamente nas políticas monetárias. A população sequer escolhe quem vai presidir o Banco Central! Já no Bitcoin qualquer pessoa pode auditar a rede e sugerir melhorias, porque ela é de livre acesso.



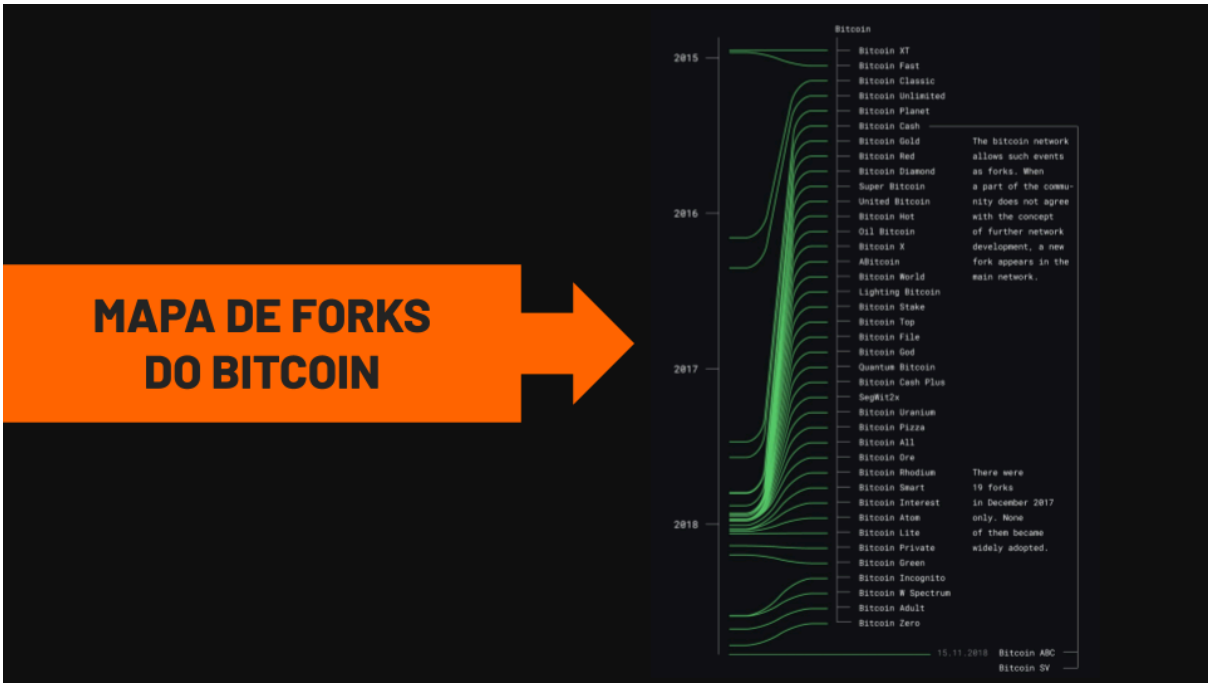
(Slide 96) - Bitcoin 4 All

Estruturas centralizadas são hierárquicas, como uma empresa: tem CEO, alguém tomando as decisões sobre os próximos passos, tem equipe de marketing, de desenvolvimento de pesquisa e funcionam através dessa hierarquia de poder. Empresas competem entre si para ganhar mercado. Criptomoedas são como empresas e competem entre si por market share vendendo utilidade, como empresas fazem.

Já o Bitcoin é horizontal, é colaborativo, ele simplesmente existe e permite que qualquer pessoa usufrua e participe da rede. Não tem ninguém determinando para onde o protocolo vai e qual a próxima atualização. É o coletivo de usuários, nodes e mineradores que definem quais versões do protocolo vão rodar sem que nem eles concordem entre si. É por isso que Bitcoin não tem competidor, nada funciona como ele. Bitcoin abraça o pensamento adversário e usa esses incentivos individuais para fortalecer o todo.

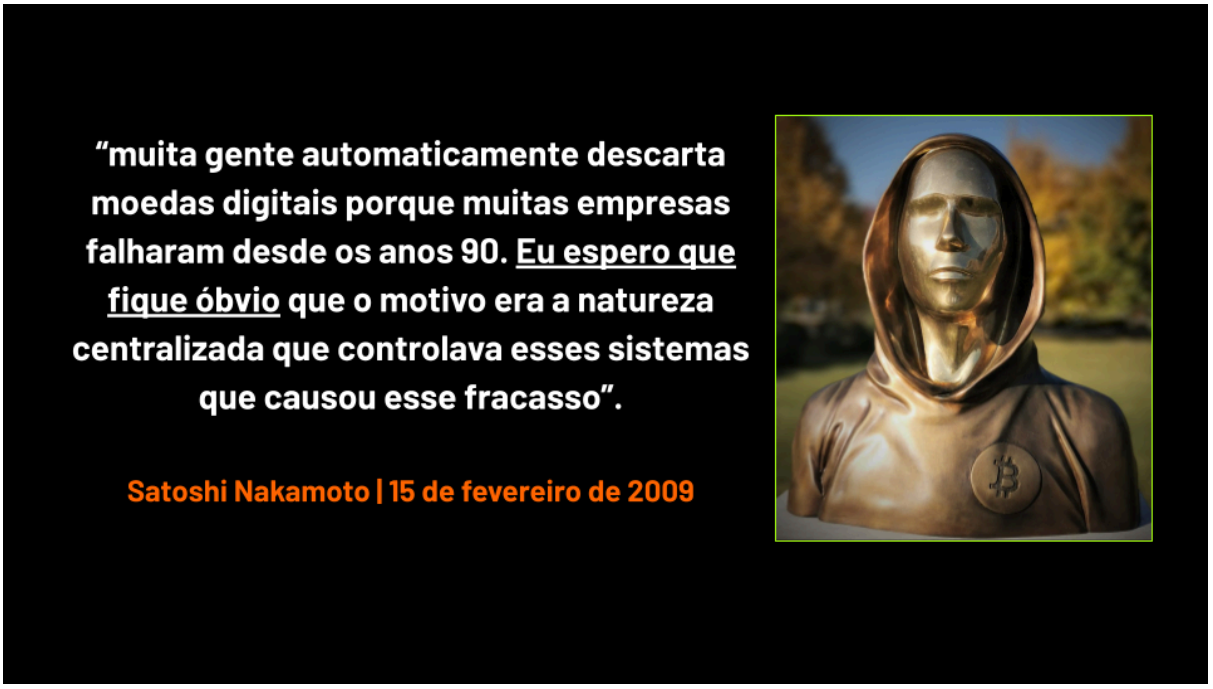
É por isso que Bitcoin é tão resiliente. Não tem como censurar ou evitar que as pessoas acessem, mesmo que elas discordem umas com as outras. Ao contrário dos bancos que o tempo todo fecham contas de usuários e mudam as regras constantemente.

Inclusive muitos protocolos se dizem descentralizados, mas quando você analisa profundamente são o oposto: são como empresas. Tem líderes, tem concentração do poder de decisão, são facilmente censuráveis e não sobreviveriam a ataques hackers ou censura governamental. Já Bitcoin tem sido atacado constantemente e segue rodando sem parar há mais de 10 anos por essa estrutura resiliente e descentralizada.



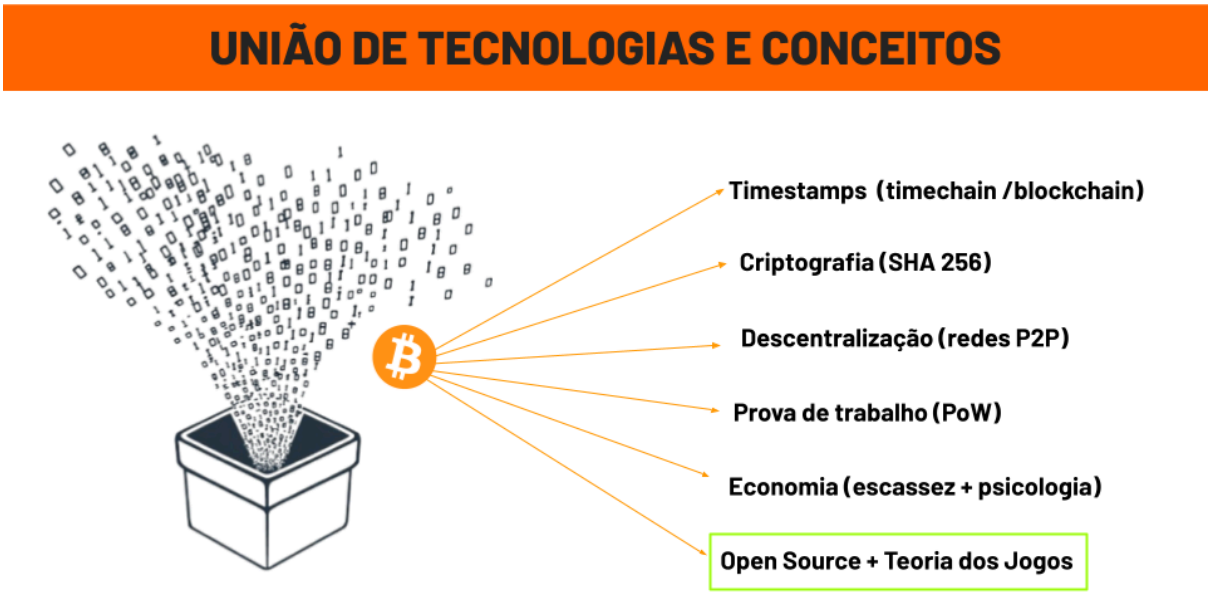
(Slide 97) - Bitcoin 4 All

Mesmo existindo centenas de cópias, nenhuma delas conseguiu ultrapassar o Bitcoin, nem mesmo qualquer outra criptomoeda que surgiu depois. Essa imagem mostra os forks, as cópias que já foram feitas do Bitcoin de 2015 a 2018. Muitos se intitulam como “o verdadeiro bitcoin” e tentaram roubar narrativa, visibilidade e liquidez, mas nenhuma de fato conseguiu. Nenhum projeto consegue roubar as propriedades e o efeito de rede que Bitcoin tem. Qualquer nível de centralização já é um ponto de mutabilidade, de monopólio do poder de decisão e também um potencial ponto de falha que pode ser explorado por atacantes.



(Slide 98) - Bitcoin 4 All

Satoshi sabia desde o princípio que a descentralização era o ponto chave do Bitcoin e um dos principais motivos de projetos anteriores de dinheiro digital não vingarem. Ele inclusive escreveu em 2009: “muita gente automaticamente descarta moedas digitais porque muitas empresas falharam desde os anos 90. Eu espero que fique óbvio que o motivo era a natureza centralizada que controlava esses sistemas que causou esse fracasso”.



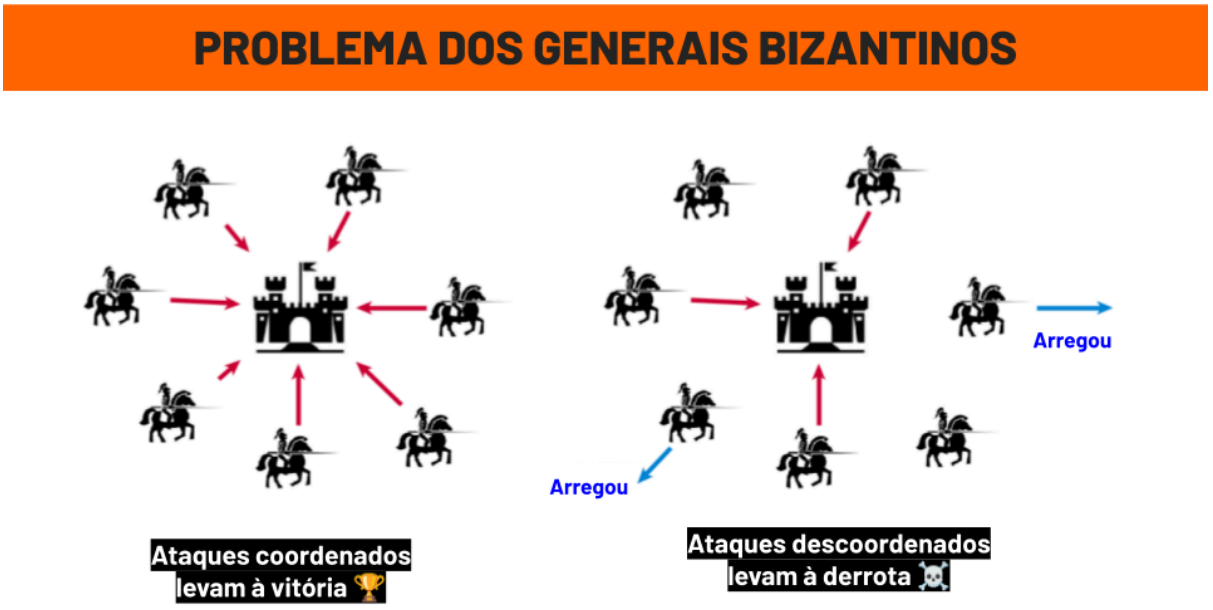
(Slide 99) - Bitcoin 4 All

A descentralização do Bitcoin é resultado de uma combinação única de fatores que trabalham em conjunto para proteger a rede. Para comprometer o sistema, seria necessário um ataque que exigisse coordenação extrema, enormes recursos financeiros e uma quantidade colossal de energia. Essa barreira quase intransponível é sustentada pela aplicação prática da teoria dos jogos, que incentiva os participantes a colaborar entre si para fortalecer a rede em vez de tentar hackear ou enganar uns aos outros.

Na teoria dos jogos do Bitcoin, a colaboração é sempre mais lucrativa do que a sabotagem. Os mineradores, validadores e outros participantes têm incentivos financeiros e estruturais para atuar a favor da rede, já que qualquer tentativa de ataque seria extremamente cara e, na maioria dos casos, inútil.

Além disso, para que essa colaboração seja possível e confiável, o Bitcoin opera com transparência total. Seu código é open source, ou seja, aberto e acessível a todos, permitindo auditoria contínua e garantindo que nenhuma regra seja alterada sem o consenso da rede. Esse alinhamento entre descentralização, incentivos econômicos e transparência é o que torna o Bitcoin a rede monetária mais robusta e segura já criada.

Satoshi conseguiu unir esses ponto resolvendo um dos problemas mais antigos: o problema dos generais bizantinos.



(Slide 100) - Bitcoin 4 All

Essa analogia tenta responder, através de uma situação de guerra, como sistemas de computador poderiam se comunicar de forma descentralizada. Até antes do Bitcoin surgir esse problema não tinha uma resposta.

Você assistiu Game of Thrones? Se você assistiu, imagina agora uma cena de invasão de uma cidade tipo a do seriado. Essa cidade se chama Bizâncio e tem vários generais querendo atacar esse lugar. Eles cercaram a cidade e devem decidir juntos quando atacar. Se todos atacarem ao mesmo tempo vencem a batalha porque houve coordenação. Se eles atacarem em momentos diferentes, eles perdem porque ficaram descoordenados e suscetíveis a serem atacados.

Os generais não têm canais de comunicação seguros uns com os outros para criar essa ação coordenada. Primeiro porque eles estão em posições diferentes ao redor da cidade, e segundo porque eles não conseguem ter garantias de que a mensagem vai chegar, as chances de um mensageiro ser interceptado pelo inimigo é muito grande.

Então, eles precisam achar uma forma de se comunicar, de entrar em consenso sobre a hora certa de atacar. O primeiro general pode começar enviando uma mensagem de ataque às 9h, mas ele não tem como saber se o mensageiro entregou a mensagem ou não. Essa incerteza pode levar o primeiro general a desistir de atacar. Dilemas como esse geraram muitas falhas nos dinheiros digitais anteriores ao Bitcoin.

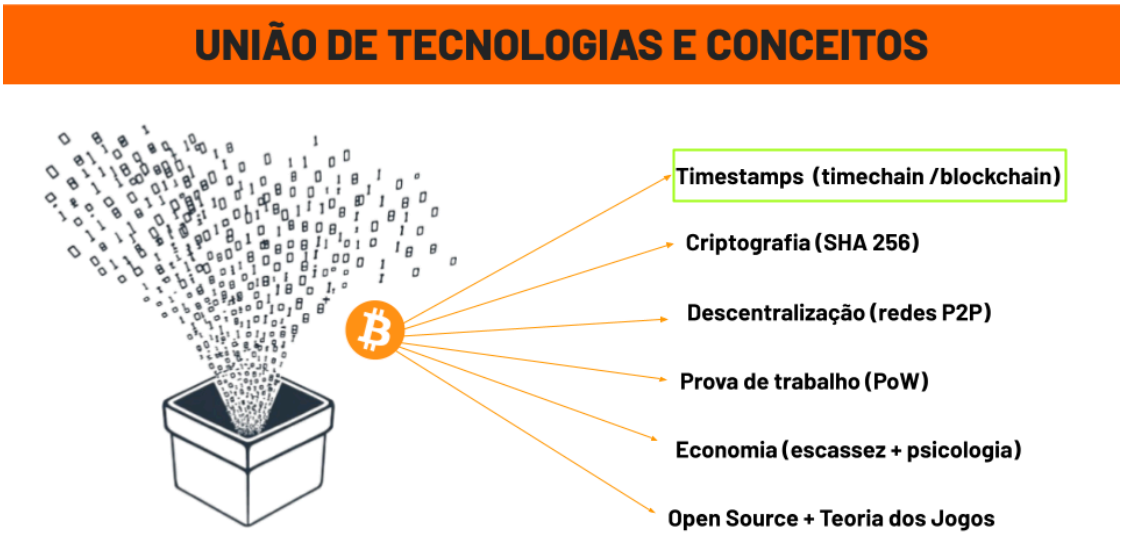
O Bitcoin conseguiu resolver o problema dos generais bizantinos tendo: coordenação completa através de Proof of Work, que estabelece um conjunto de regras de

processamento da rede que coordena todo mundo; através de redes P2P que conectam todos os participantes ao mesmo sistema; e através de blockchain, um sistema de registros criptográficos encadeados que todos podem verificar sem depender de nenhum “mensageiro” de fora do sistema.

Através desse sistema todos os generais conseguiriam se coordenar sobre o momento certo de atacar Bizâncio sem depender de terceiros, de forma sincronizada, segura e sem ninguém hesitar ao ataque.

(Slide 101) - Bitcoin 4 All

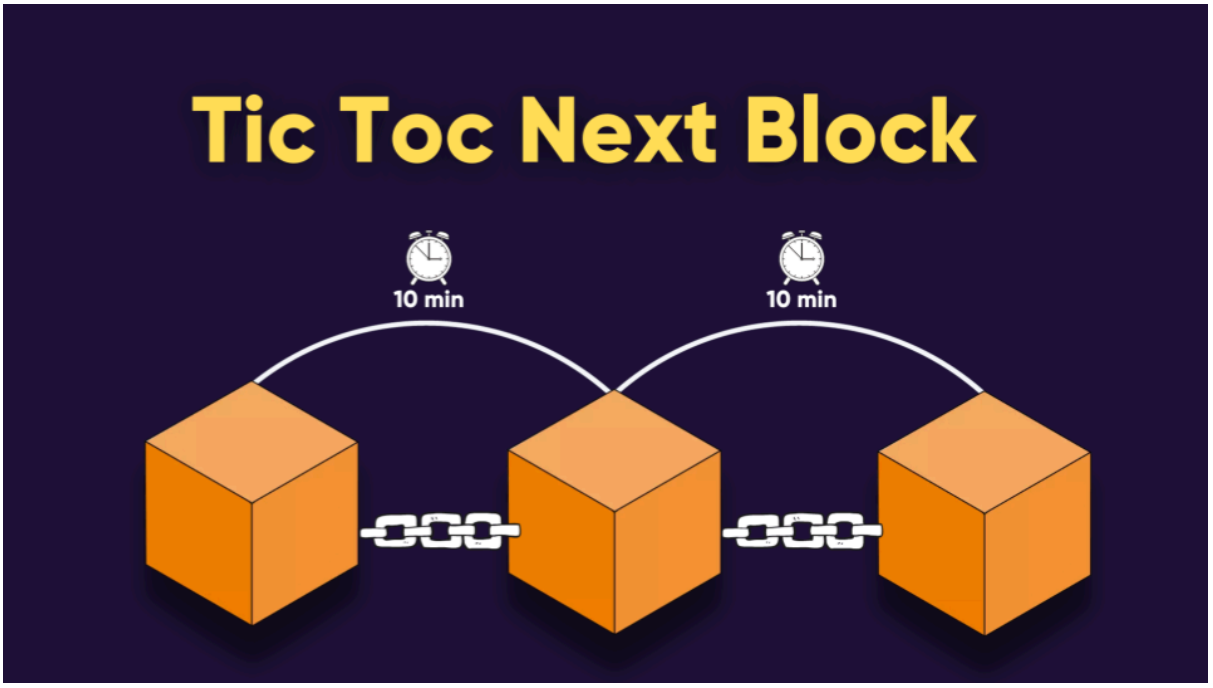
Eu falei agora a pouco sobre Proof of work e mecanismos de consenso, esses termos são as regras que guiam o protocolo. São algoritmos que estabelecem como a rede vai se coordenar. Esse conjunto de regras busca, a partir de uma situação inicial, um input (entrada em portugues), atingir um resultado final, um output (saída em portugues).



(Slide 102) - Bitcoin 4 All

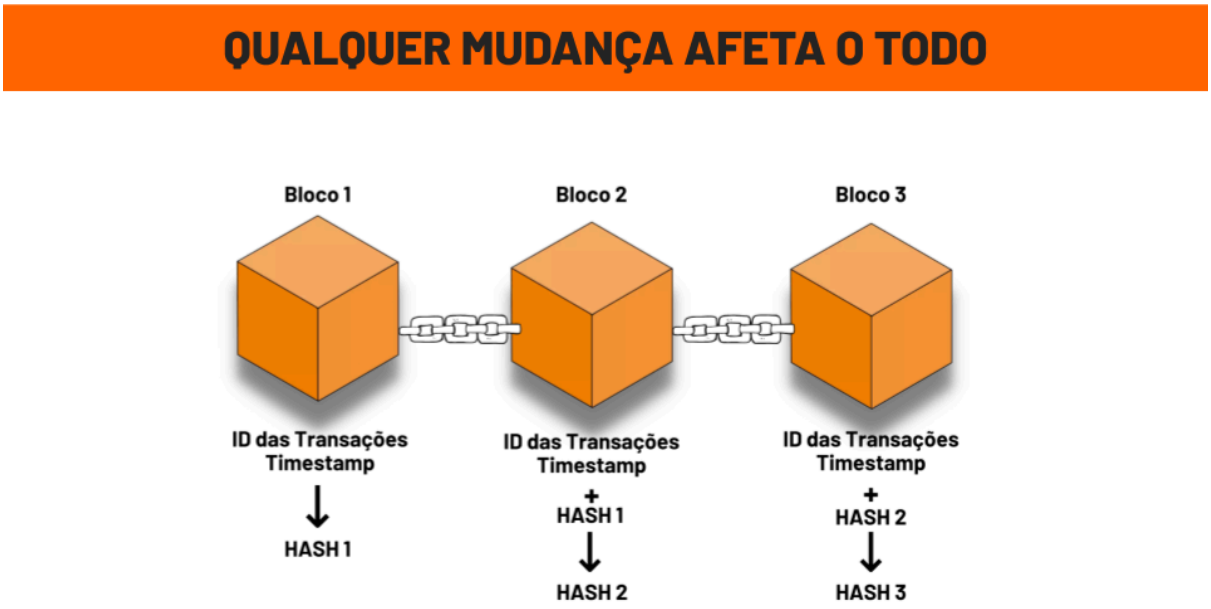
Tudo isso funciona registrando informações em um sistema encadeado, distribuído e que não pode ser apagado chamado blockchain. Satoshi usou timestamps e timechain para descrever esse mecanismo no whitepaper do bitcoin.

Tem gente que fala que blockchain é a verdadeira inovação por trás do Bitcoin, mas isso é a maior bobagem. Blockchain é importante, mas sozinha e sem outras propriedades, ela é só uma base de dados lenta, cara e tão centralizada quanto um Excel de uma empresa!



(Slide 103) - Bitcoin 4 All

Blockchain ou timechain significa corrente de blocos. São blocos de informação atrelados uns aos outros e que são processados pela rede a cada 10 minutos em média. Quer dizer que muitas vezes demora menos de 10 minutos e outras vezes pode levar horas. Depende do poder computacional dos mineradores e da dificuldade da rede.



(Slide 104) - Bitcoin 4 All

A imutabilidade de registros vem no sentido de que não tem como você tirar ou mudar o bloco do meio da cadeia. Se tem 200 blocos e você tentar apagar ou modificar o do meio, os blocos vizinhos vão ser afetados, muda o hash.

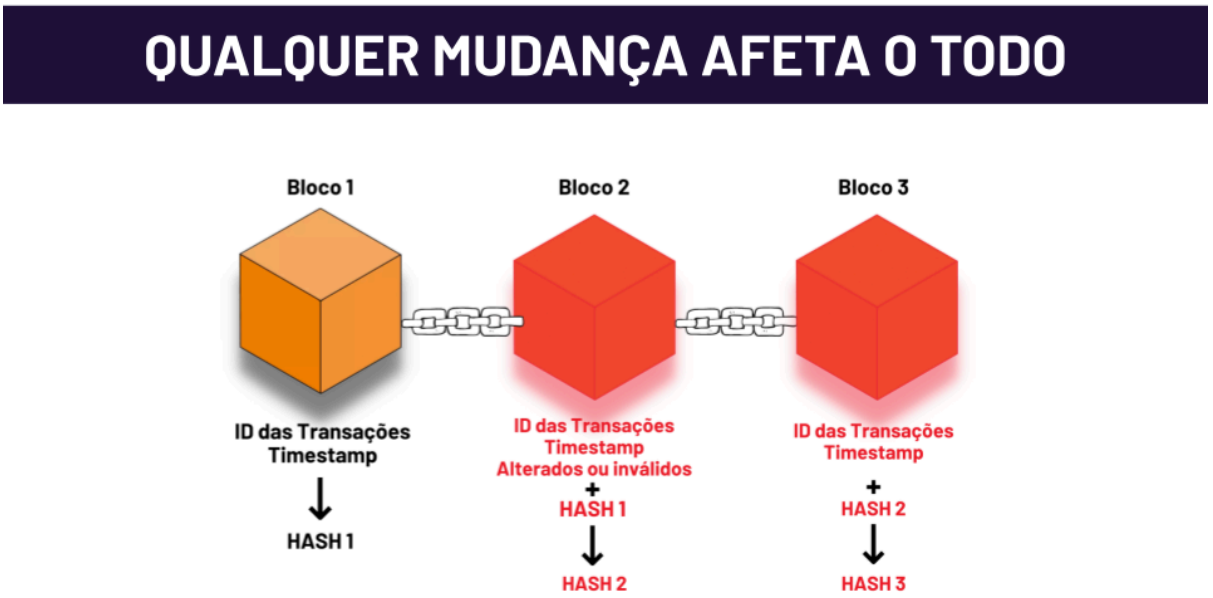
É como se fosse uma costura digital. Se você puxar o fio do meio de uma costura, distorce todos os próximos pontos, não é assim? Com o Bitcoin é muito parecido. Se qualquer informação for alterada em um bloco, acaba distorcendo todos os blocos seguintes.

Então, vamos supor que a gente está olhando agora para a blockchain do Bitcoin. Cada bloco minerado contém informações sobre as transações financeiras feitas na rede e sobre o próprio bloco onde elas foram registradas. Só que a rede resume todas essas formações em um código chamado HASH. O Hash é a frase criptográfica que resume todas as informações que estão dentro do bloco de informação. É a partir do Hash que o encadeamento acontece.

Depois de criado o Hash 1 do bloco 1, ele vai ser inserido junto com o conteúdo do próximo bloco, o bloco 2. Vai ser misturado de forma aleatória e vai formar o Hash 2.

O Hash 2 resume todo o conteúdo do seu bloco e também do bloco anterior, porque o Hash 1 foi inserido dentro do conteúdo do bloco 2 e assim sucessivamente.

O hash 3 vai ser o resumo criptográfico do bloco 3, que contém o hash do bloco 2 anterior. Através dessas funções de hash é que acontece o encadeamento da rede. Ou seja, os blocos seguintes sempre vão ter um resumo dos blocos anteriores. É desta forma que as informações estão sempre correlacionadas.



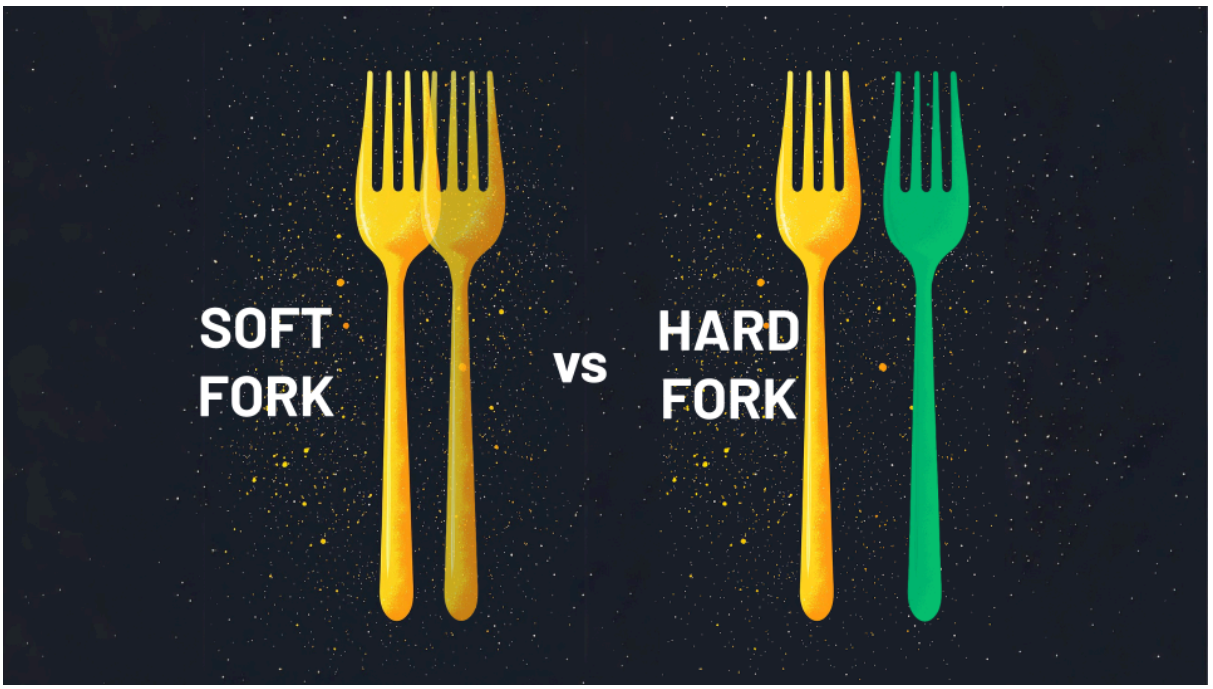
(Slide105) - Bitcoin 4 All

É por causa desse encadeamento de informações que a rede fica sempre confirmando tudo antes de minerar o próximo bloco. Então, se mudar qualquer coisa no bloco 1, o hash de todos os blocos seguintes também mudam. Se mudar uma vírgula, um espaço, uma letra, qualquer coisa, já altera o Hash. Se algo for alterado depois de registrado em blockchain, os mineradores ou os nodes que verificam a rede vão identificar a alteração através do hash e não vão aceitar essa informação como válida.

Esse mecanismo torna absurdamente fácil verificar se houve algum ataque ao histórico de transações ao mesmo tempo que torna muito dificil editar o passado dos registros de forma efetiva. Isso porque, tanto os nodes quanto os mineradores tem cópias da blockchain bitcoin, se qualquer informação do passado for mudada e não bater com as cópias que existem nos seus computadores, eles vão ser facilmente identificados e não vão aceitar aquele bloco como válido.

Esse é um dos fatores de verificação constante que torna a rede Bitcoin muito segura e difícil de “passar a perna” e de hackear. É uma rede que consegue descentralizar a confiança, porque está tudo certinho, não tem nada alterado. Todas as informações batem. Essa facilidade de verificação e dificuldade de manipulação é o que torna os registros na blockchain Bitcoin imutáveis.

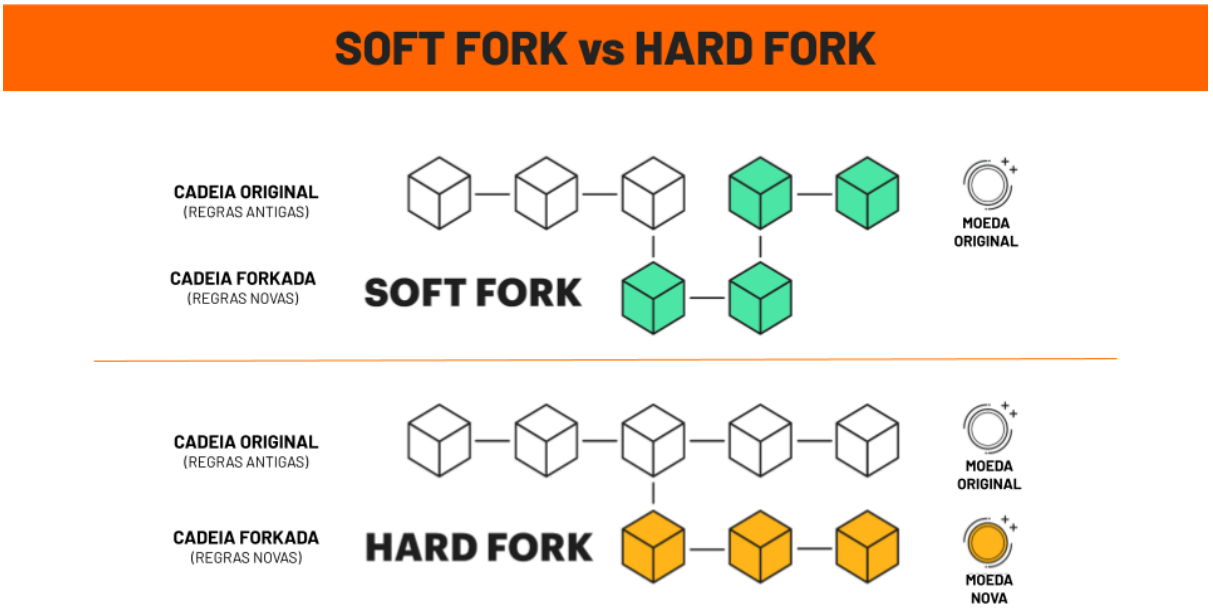
Ainda assim, caso alguém resolva modificar a forma como a rede funciona, essa pessoa pode causar um fork.



(Slide 106) - Bitcoin 4 All

As atualizações de versões de blockchain são chamadas de forks. Existem dois tipos de atualizações: soft forks e hard forks.

Forks vem de ramificação e significa garfo em inglês, por isso você vai ver imagens de garfos quando alguém falar em forks. Forks são versões diferentes das regras iniciais.



(Slide 107) - Bitcoin 4 All

Então qual a diferença entre esses dois tipos de garfos, ou melhor, bifurcações?

Soft forks é quando a rede faz uma atualização de forma que tanto quem roda a versão antiga do código, do software, quanto quem roda a nova versão conseguem se coordenar. É um fork retrocompatível, opcional e que não muda mecanismo de consenso. Segue sendo a mesma rede e a mesma moeda só que com alguns detalhes diferentes nas versões.

Já os hard forks são quando atualizações radicais são feitas, a ponto de mudar consenso do protocolo e quem roda a versão antiga não consegue se coordenar com quem roda a nova versão. Usuários antigos são conseguem participar da nova rede se não atualizarem. Como consequência, uma nova moeda e uma nova rede é criada. Esse tipo de atualização força usuários a atualizarem para a nova versão.

Bitcoin não faz hard forks, apenas soft forks. Porque hard forks são forças centralizadoras, excluem usuários que podem não concordar com a nova versão e acabam com a imutabilidade de rede. Hard forks são mais frequentemente observados em outros protocolos de criptomoedas e em blockchains privadas de empresas.

Bom, nessa aula nós começamos a mergulhar no funcionamento do Bitcoin, mas essa é só uma parte, tem muito mais conteúdo para você aprender. Absorva esse conhecimento, dê uma pausa no seu cérebro e quando estiver pronto para continuar eu te espero na próxima aula.