IMD0913

O PROTOCOLO BITCOIN: VISÃO GERAL

Definições

Criptomoeda: *Uma forma de moeda que é armazenada digitalmente e não é emitida por uma autoridade central. Sua segurança é baseada em criptografia, consenso distribuído e alinhamento de incentivos econômicos. Bitcoin é uma criptomoeda.*

Blockchain: *A estrutura de dados utilizada para representar uma criptomoeda (entre outras aplicações). Armazena os dados de uma forma que permite que várias partes os acessem de forma confiável, sem a necessidade de confiar uma nas outras.*

Características fundamentais de uma **moeda**

Durabilidade: a moeda não perde valor e não é destruída ou tornada irresgatável facilmente.

Portabilidade: a moeda é fácil de transportar de um lugar para outro.

Divisibilidade: a moeda pode ser facilmente trocada em diferentes denominações.

Uniformidade: todas as unidades da moeda são idênticas em valor.

Oferta limitada: a oferta da moeda não pode ser inflacionada arbitrariamente.

Aceitabilidade: a moeda deve ser suficientemente aceita.

Características fundamentais de um **blockchain**

Controle descentralizado: o consenso comunitário, ao invés da decisão de uma única parte, dita quem acessa ou atualiza o *blockchain*.

Evidência de adulteração: é imediatamente óbvio se os dados armazenados no *blockchain* forem adulterados.

Consenso de Nakamoto: é preciso comprovadamente gastar recursos ao atualizar o *blockchain*.

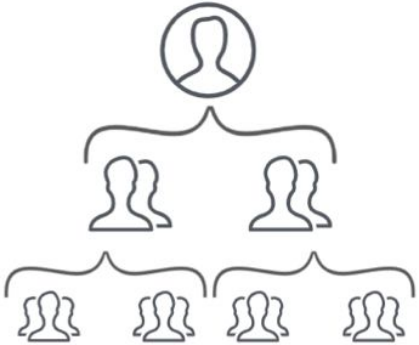
O que é centralização?

Autorização/administração tratada por **uma única parte**

Os dados são armazenados por uma única parte

Imagine:

- Arquitetura cliente-servidor
- Organograma hierárquico
- Dinastia política
- Banco tradicional



Centralização: vantagens e desvantagens

+ VANTAGENS

Eficiência

Dados são armazenados em um lugar, programas são executados uma vez

Fácil atualização dos dados

Atualizações nos dados só precisam de uma aprovação e pode ser forçado para os demais usuários

– DESVANTAGENS

Falta de soberania

Uma entidade central “manda” nos dados

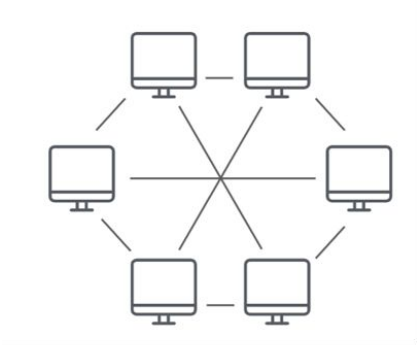
Único ponto de falha

Qualquer ataque ou falha só precisa ocorrer em um lugar

O que é **des**centralização?

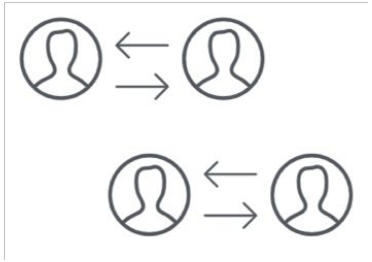
Autorização de acordo com um **protocolo/acordo amplamente conhecido**

Os dados são armazenados pelos participantes



Imagine:

- Arquitetura *peer-to-peer* (P2P)
- Organograma plano
- Democracia pura
- Comunidade



Descentralização: vantagens e desvantagens

+ VANTAGENS

Soberania

Você sabe exatamente como seus dados serão usados

Tolerância a falhas

Toda a rede tem que ser derrubada, em contraste com uma única parte

– DESVANTAGENS

Ineficiência

Dados são duplicados e programas são re-executados através da rede

Difícil atualização dos dados

Atualizações devem ser deliberadamente adotadas pelos participantes da rede

O que é Bitcoin?

Bitcoin é uma **criptomoeda** criada por **Satoshi Nakamoto** em 2008

> **Criptomoeda**: *uma moeda baseada em ciência da computação, criptografia e economia*

Uso original da estrutura de dados conhecida agora como ***blockchain***

100% digital e **não é controlada por entidade central**

Motivada pelo movimento ***Cypherpunk***

Open-source: https://github.com/bitcoin

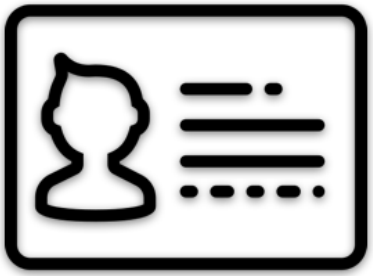
Motivação

Confiamos aos bancos alguns serviços bastante críticos:

- Transferir e resgatar dinheiro
- Registrar corretamente o histórico da conta e transações
- Armazenar nossa informação pessoal

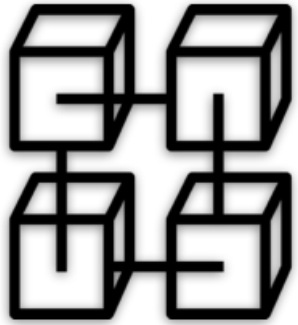
Como fazemos um sistema descentralizado que faz o mesmo o que um banco faz?

Componentes do protocolo Bitcoin



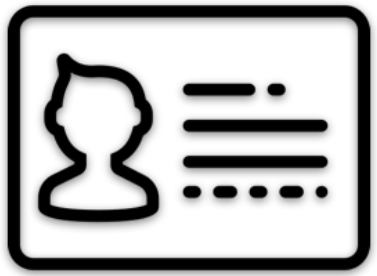
IDENTIDADE
Criando uma conta no sistema

TRANSAÇÕES
Enviar e receber bitcoin com segurança



REGISTRO DISTRIBUÍDO
Registro histórico de transações

CONSENSO *TRUSTLESS*
Concordar com as mudanças do livro-razão



IDENTIDADE

O que torna uma **identidade** sua?

Identidade

Qual o papel da identidade no contexto de moedas?

- **Receber** dinheiro
- **Reivindicar/gastar** dinheiro
- **Não-repúdio**

Identidade no cotidiano:

- Residências têm endereços e chaves para a caixa de correio
- Emails tem aliases e senhas
- Bitcoin tem chaves públicas e chaves privadas

Identidade nos bancos

Identidade é confirmada através de informações pessoais:

- CPF
- Nome
- Data de nascimento
- Endereço

Login e senha são emitidos por gerente central:

- O banco garante que os *logins* são únicos

Identidade: chaves públicas e privadas

Cada identidade é representada com uma **chave pública** única

Uma **chave privada** correspondente atua como a chave para “destrancar” a chave pública... e o seu dinheiro!

Chaves privadas são escolhidas aleatoriamente, chaves públicas são geradas a partir da chave privada

Chave pública para receber, **chave privada** para resgatar

Identidade: chaves públicas e privadas

Alguns detalhes:

Informações pessoais não são necessárias

Isso significa que o Bitcoin é anônimo?

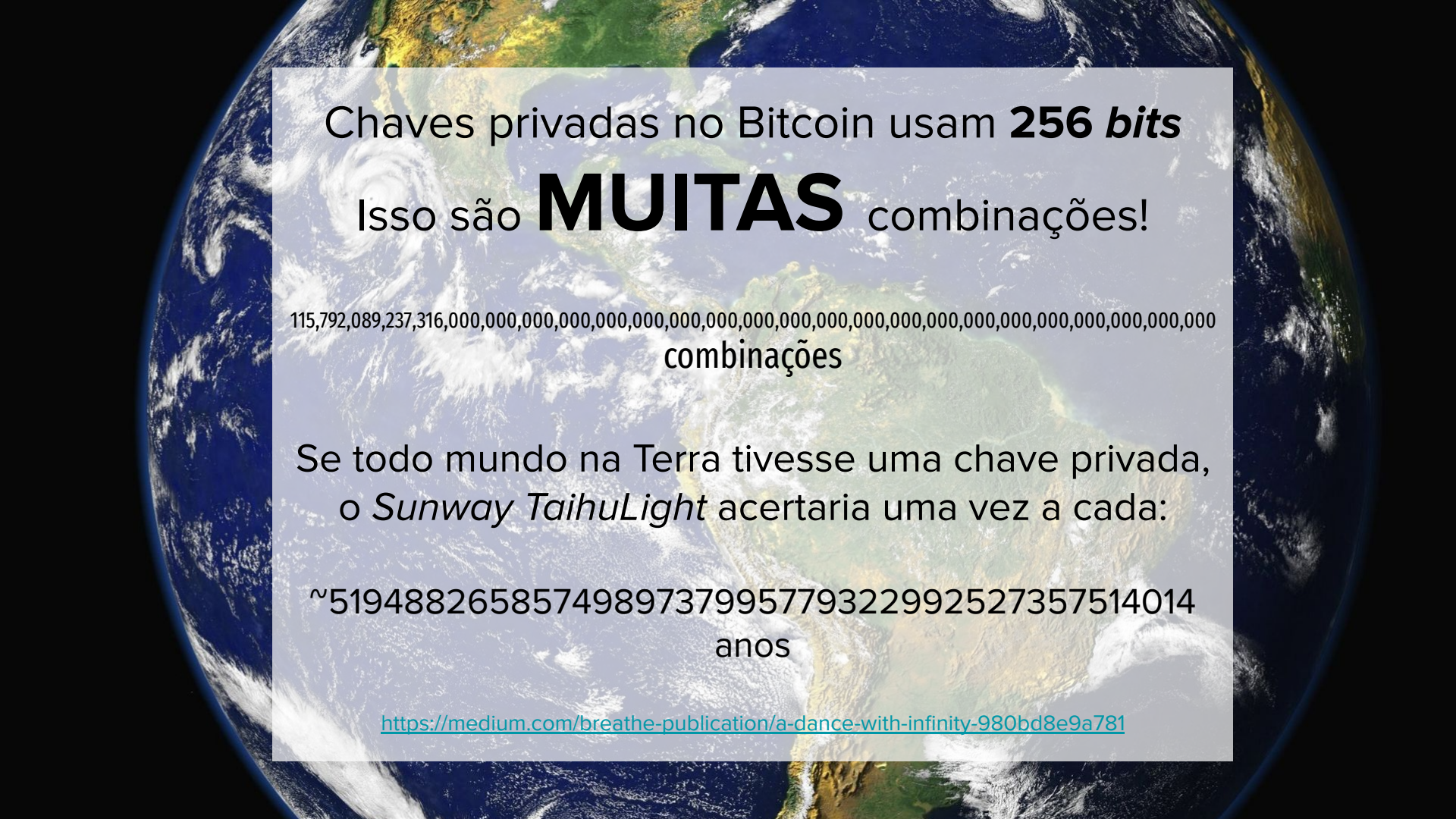
Sem limite para a quantidade de contas que você pode ter

Isso afeta a segurança do Bitcoin?

Sem restrições para chaves que foram tomadas

Isso significa que alguém pode ter a mesma chave privada que eu?


E se alguém **adivinhar** minha **chave privada**?!



Chaves privadas no Bitcoin usam **256 *bits***

Isso são **MUITAS** combinações!

115,792,089,237,316,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000
combinações

Se todo mundo na Terra tivesse uma chave privada, o *Sunway TaihuLight* acertaria uma vez a cada:

~5194882658574989737995779322992527357514014
anos

https://medium.com/breathe-publication/a-dance-with-infinity-980bd8e9a781

TRANSAÇÕES

O que torna uma **transação** válida?

Transações

O que torna uma transação válida?

Proof-of-ownership (uma assinatura)

Saldo disponível

Nenhuma outra transação usando o mesmo recurso

Transações: modelo tradicional

Gerente central mantém o registro do saldo das contas e verifica se as transações são válidas

Cada conta tem um **saldo disponível**

Para gastar, dinheiro é subtraído do total

Para receber, dinheiro é somado ao total

Daniel	Alice
Saldo:	Saldo:
$100,00	$250,00
-10,00	+10,00

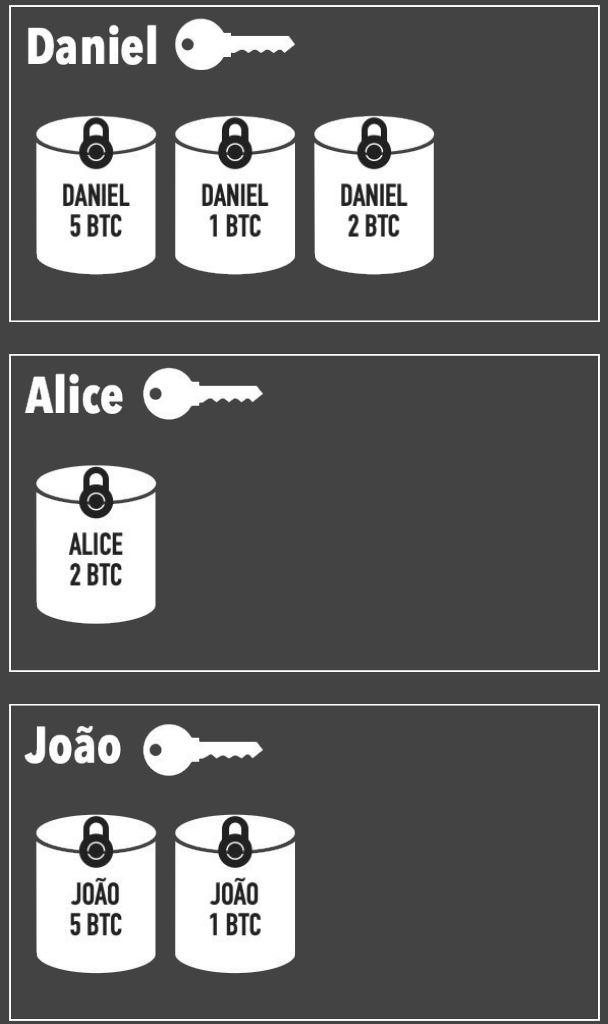
Transações: modelo UTXO

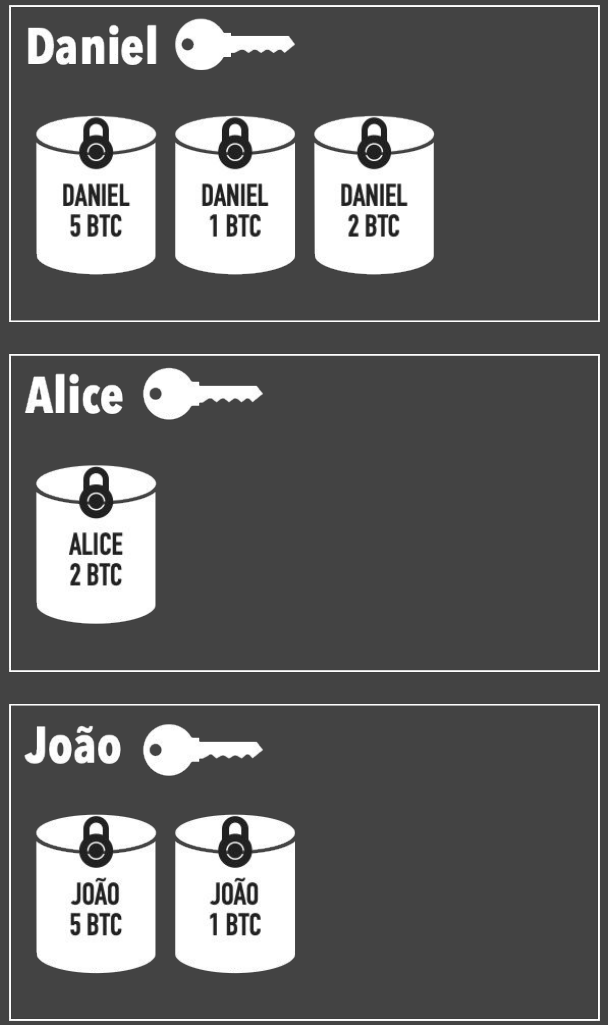
Blockchain do Bitcoin mantém o registro de moeda não gasta

- Cada conta tem um conjunto de **Unspent Transaction Outputs (UTXOs)**
  - Quantidades de bitcoin enviadas para a conta que ainda não foram utilizados

Um UTXO pode conter qualquer quantidade de bitcoin, e eles são gastos inteiramente

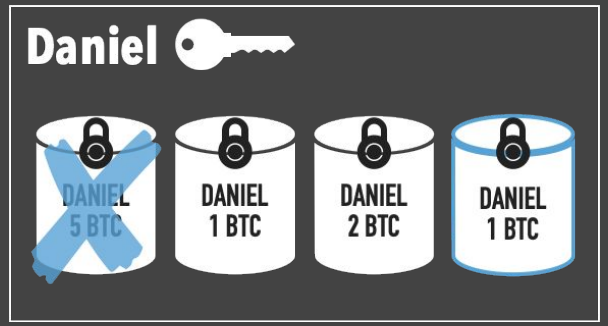
UTXOs só podem ser utilizados uma vez

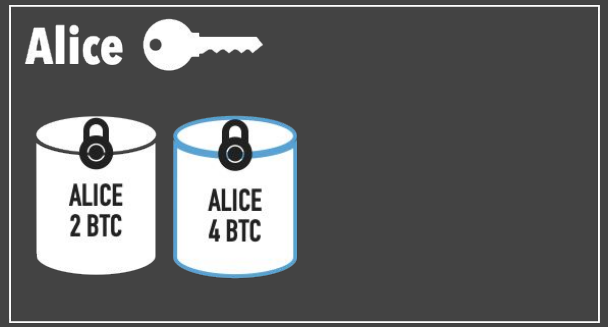

Daniel
DANIEL
5 BTC
DANIEL
1 BTC
DANIEL
2 BTC
Alice
ALICE
2 BTC
João
JOÃO
5 BTC
JOÃO
1 BTC

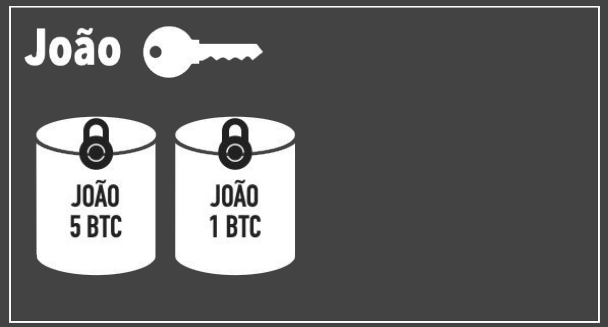


Daniel envia 4 BTC para Alice:

- Resgatando seu UTXO contendo 5 BTC
- Enviando 4 BTC para Alice
- e enviando 1 BTC de volta para ele mesmo

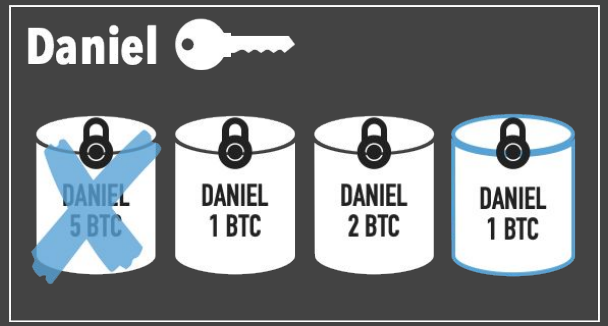


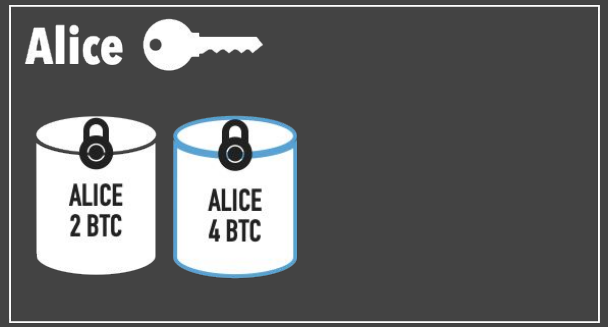


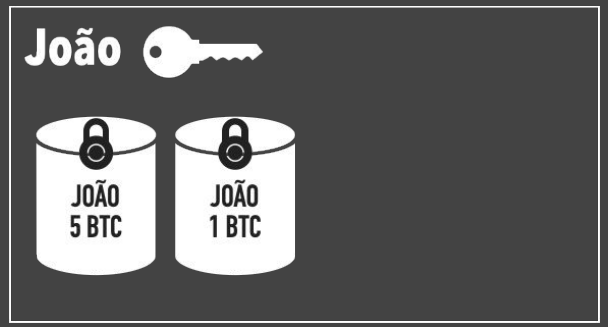


Daniel envia 4 BTC para Alice:

- Resgatando seu UTXO contendo 5 BTC
- Enviando 4 BTC para Alice
- e enviando 1 BTC de volta para ele mesmo

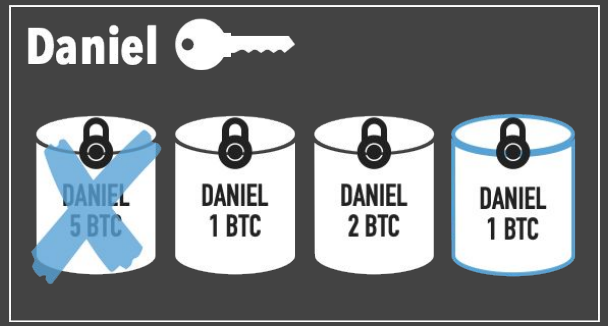


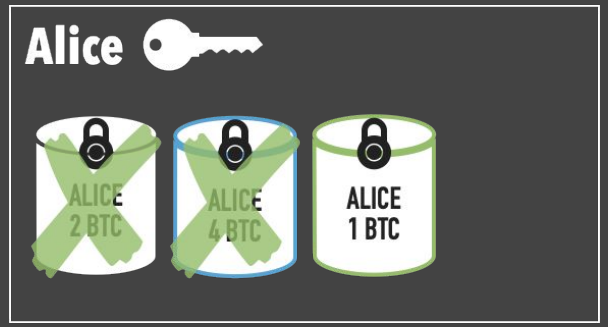


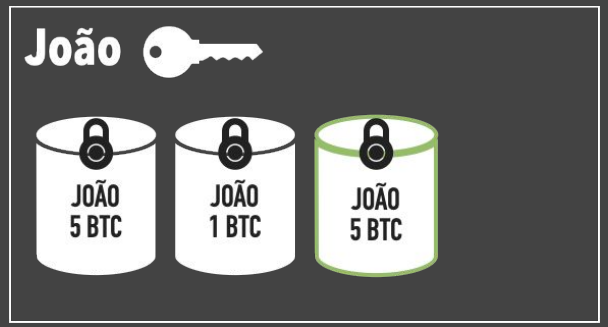


Alice envia 5 BTC para João:

- Resgatando seus UTXOs contendo 2 BTC e 4 BTC
- Enviando 5 BTC para João
- e enviando 1 BTC de volta para ele mesmo







Alice envia 5 BTC para João:

- Resgatando seus UTXOs contendo 2 BTC e 4 BTC
- Enviando 5 BTC para João
- e enviando 1 BTC de volta para ele mesmo

Resumindo, não existem bitcoins,
somente **UTXOs**

Validade

Proof-of-ownership

Assinatura gerada pela chave privada

Saldo disponível

UTXOs são usados diretamente como entrada de uma transação

Nenhuma outra transação usando o mesmo recurso

Falamos disso daqui a pouco...

No protocolo Bitcoin...

A rede Bitcoin pode operar com valores fracionários de Bitcoin

Até a ordem de grandeza de **10^{-8}** (0,00000001)

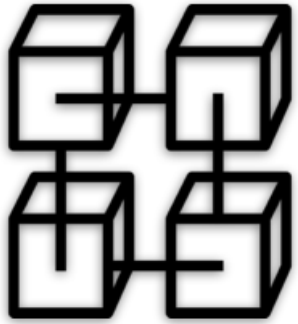
Alguns nomenclaturas comuns:

1 bitcoin (BTC)

1 milibitcoin ou milibit (mBTC) = 1/1.000 BTC = 0,001 BTC

1 microbitcoin ou microbit (µBTC) = 1/1.000.000 BTC = 0,000001 BTC

1 satoshi = 1/100.000.000 BTC = 0,00000001 BTC



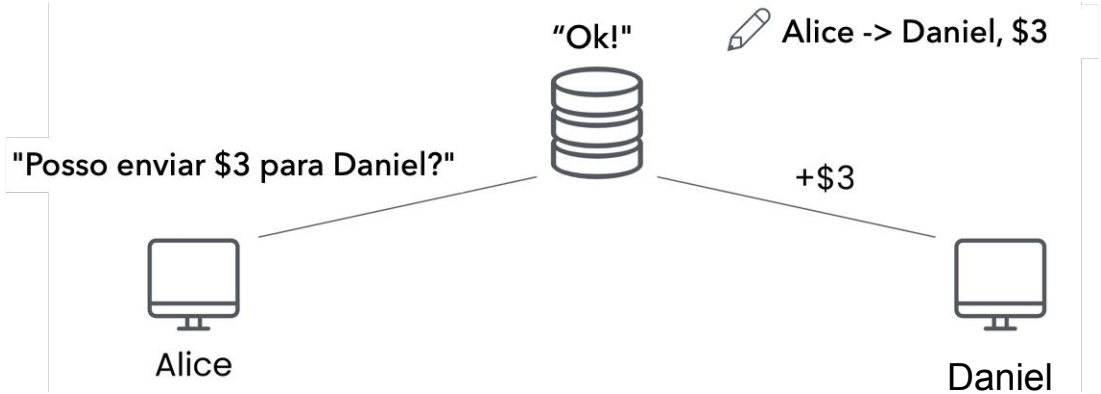
REGISTRO DISTRIBUÍDO

Registro: modelo tradicional

Entidade centralizada armazena todos os dados

Gerência central atualiza os dados através de *updates*

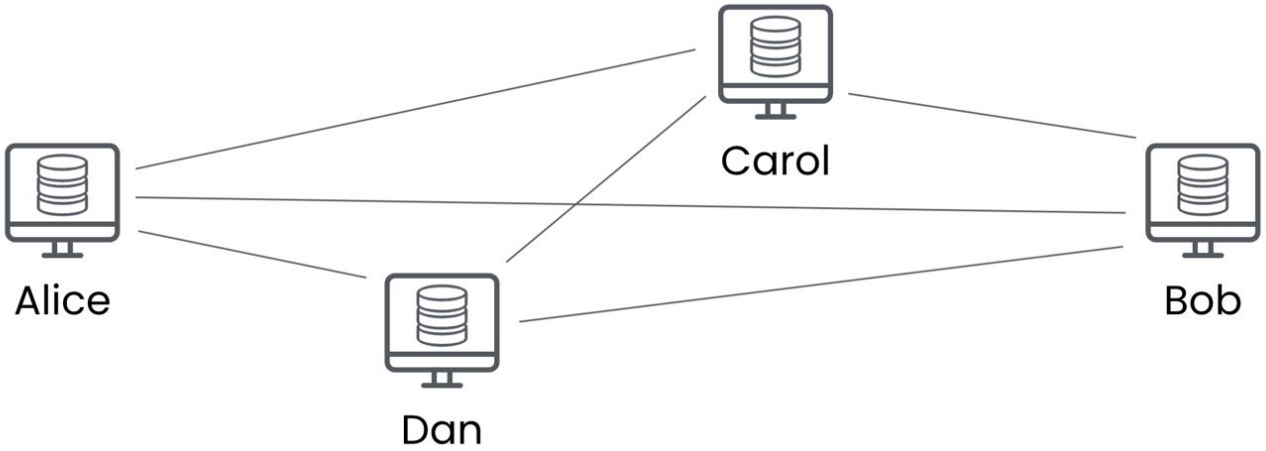
Medidas de segurança para prevenir *hackers* e falhas



Registro distribuído: blockchain

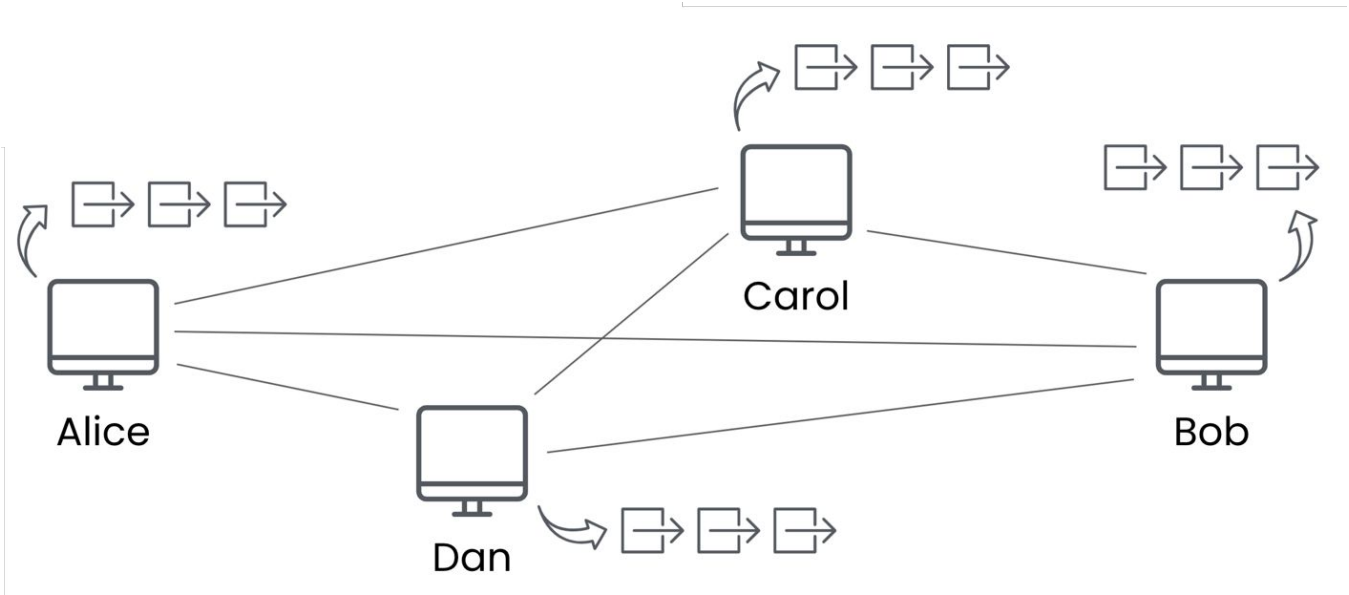
Os dados são armazenados e as atualizações são transmitidas a **todos**

Transparente e tolerante a falhas por natureza



Registro distribuído: blockchain

Transações são compiladas em “**blocos**" com referências para impor uma ordenação



CONSENSO *TRUSTLESS*

O que é consenso?

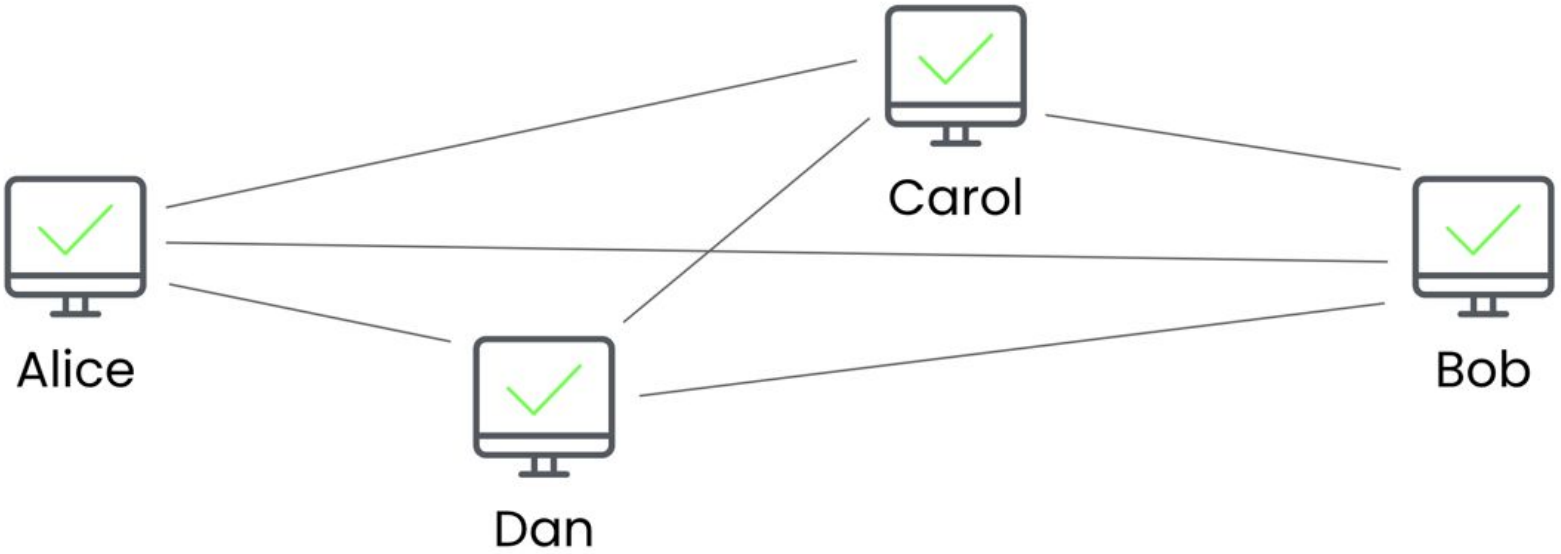
Consenso é o processo pelo qual os participantes de uma rede chegam a um **acordo** sobre alguma decisão a ser tomada.

Em nosso caso, concordar com alterações em um livro-razão de transações.

Tradicionalmente muito simples: confiamos 100% no banco!

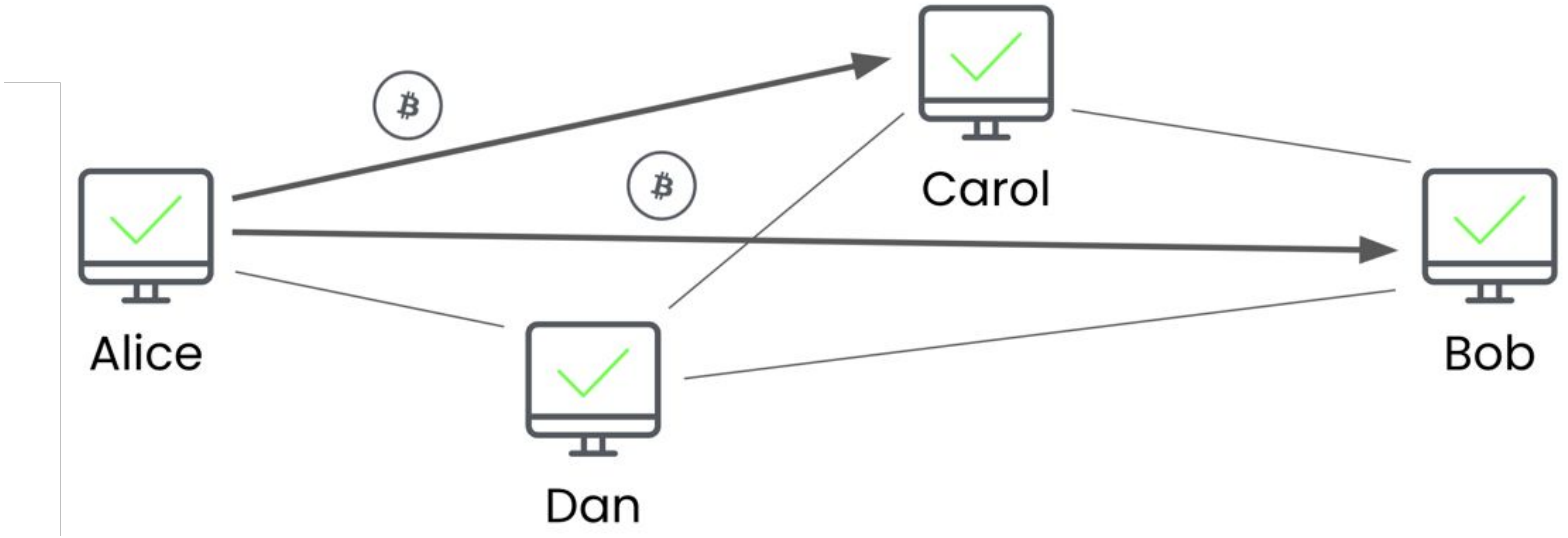
Consenso "ingênuo"

Todos aceitam transações como válidas à medida que acontecem, sem “discussão"



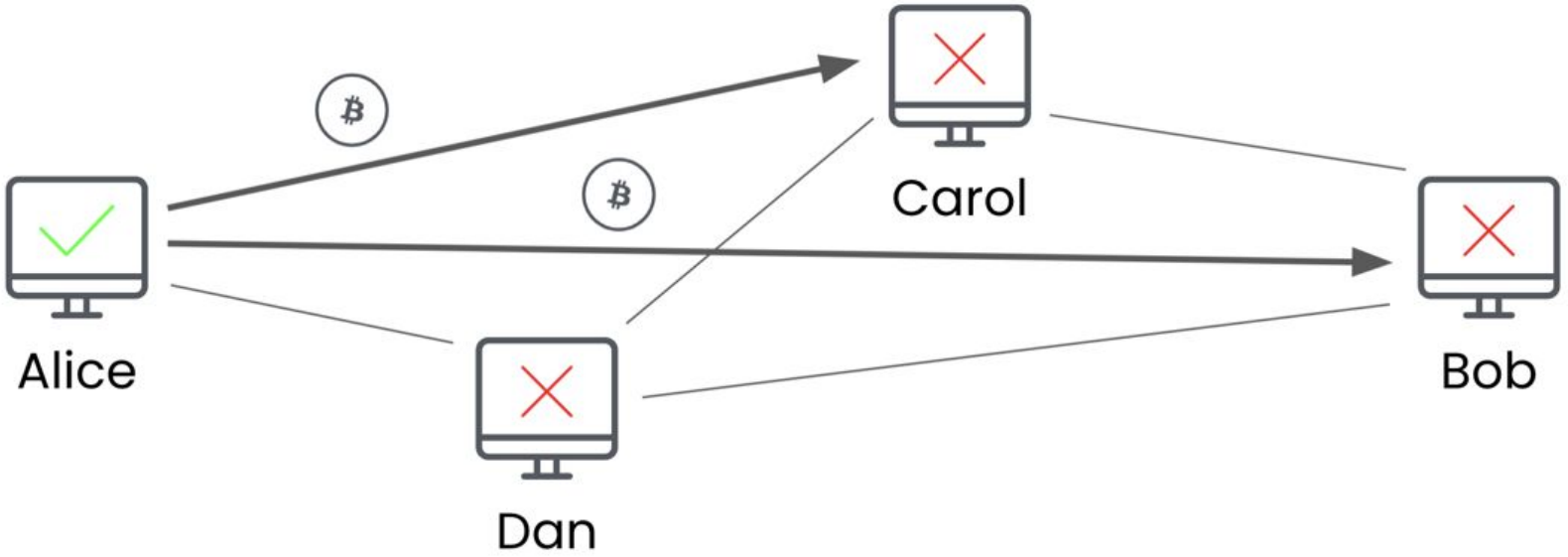
Consenso "ingênuo": **ataque de gasto duplo**

Alice promete 1 BTC para Bob em uma transação, e **o mesmo 1 BTC** para Carol em outra transação. Isso é uma **ataque de gasto duplo** (*double spend attack*)



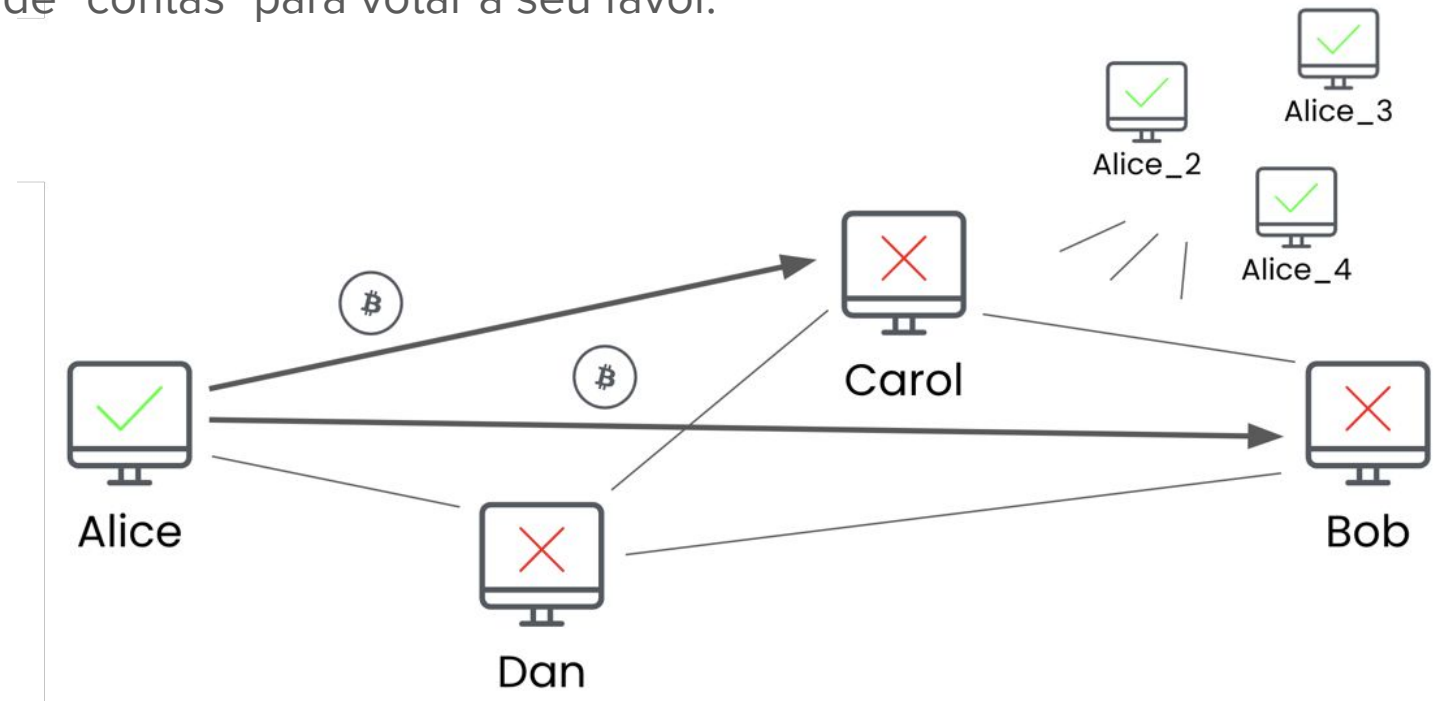
Consenso "democrático"

Em vez disso, vamos ter proponentes que transmitam as transações e eleitores que escolhem se querem ou não incluí-las.



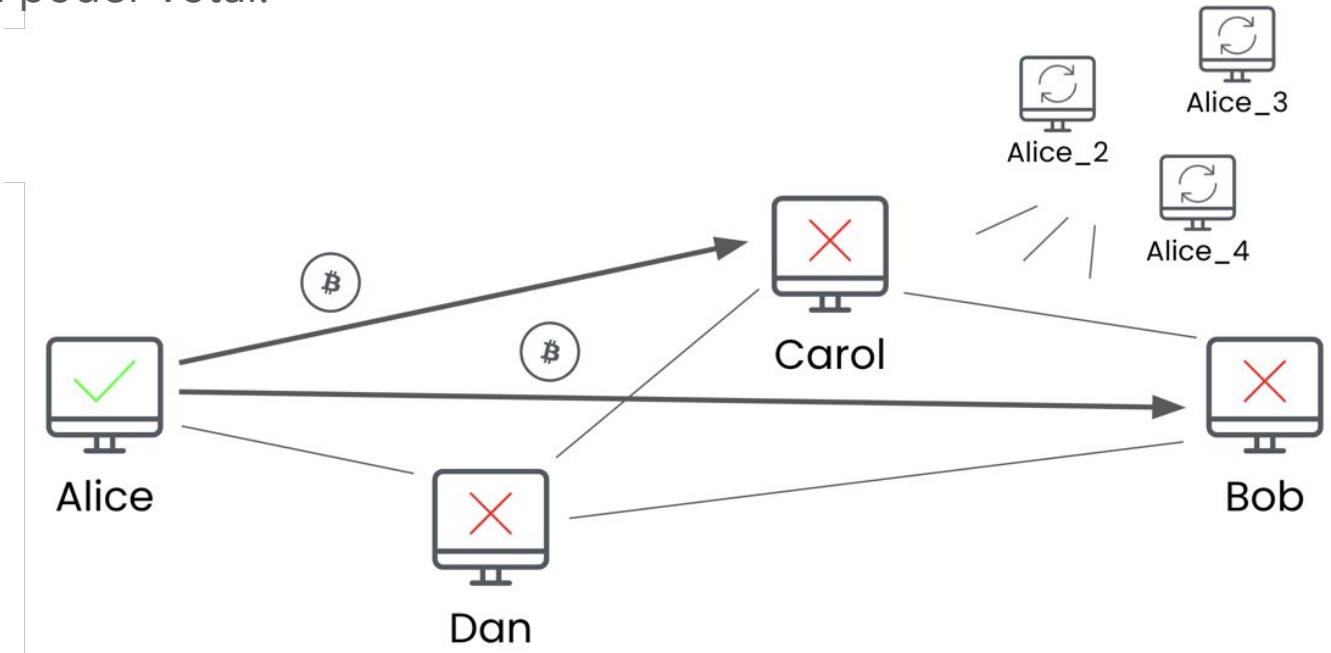
Consenso "democrático": ataque *sybil*

Criar pares de chaves pública/privada não **custa nada**, então Alice pode fazer um monte de "contas" para votar a seu favor.



Consenso de Nakamoto

Agora, vamos fazer os eleitores fazerem um monte de **cálculos inúteis de força bruta** para poder votar.



O Bitcoin pode ser uma moeda?

Durabilidade: persistido para sempre no *blockchain*.

Portabilidade: pode manter todo o seu saldo em seu bolso.

Divisibilidade: permutável em quantidades arbitrárias tão pequenas quanto 0,00000001 BTC.

Uniformidade: sem características distintivas que fariam 1 BTC valer mais do que outro.

Oferta limitada: limite finito de 21.000.000 BTC.

Aceitabilidade: particularmente aceitável porque você não precisa confiar em mais ninguém para resgatar seu dinheiro.

Resumindo o Bitcoin...

Identidade: usamos nossa chave pública para receber Bitcoin e usamos nossa chave privada para resgatá-lo;

Transações: você possui um conjunto de UTXOs que você pode usar como entrada de novas transações;

Registro: cada parte armazena uma cópia do *blockchain*, o livro-razão distribuído;

Consenso: transações são aprovadas via *proof-of-work*, um processo de votação custoso, para evitar ataques de gasto duplo.