

IMD0293

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 accessem de forma confiável, sem a necessidade de confiar uma nas outras.

CARACTERÍSTICAS FUNDAMENTAIS DE UM BLOCKCHAIN

- ▶ **Controle descentralizado:** o consenso comunitário, ao invés da decisão de uma das partes, 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

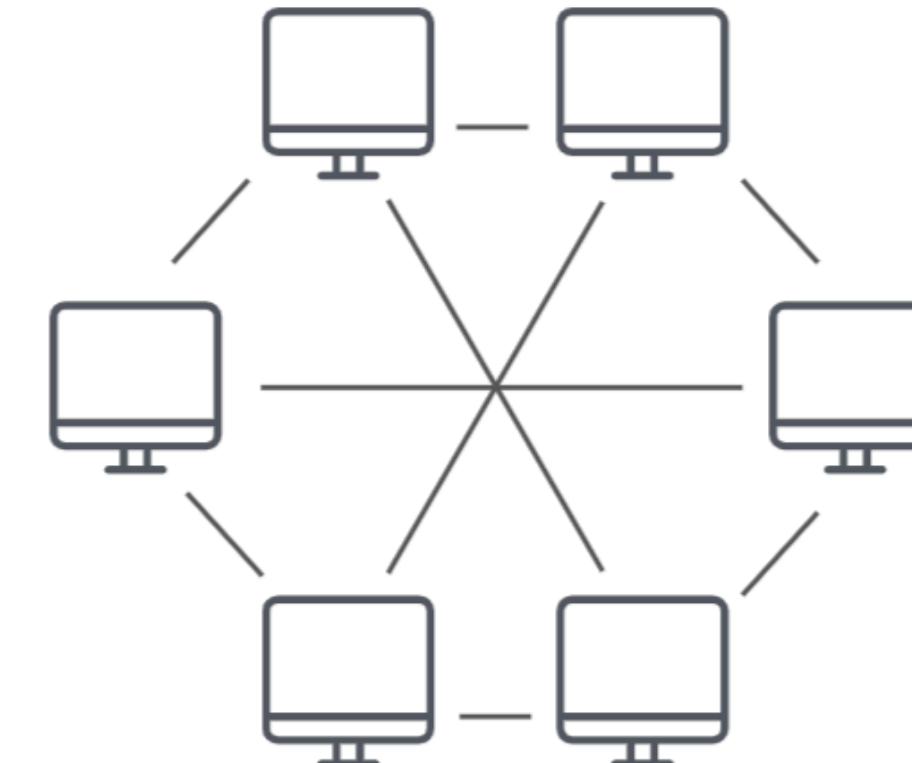
Uma entidade central “manda” nos dados

Único ponto de falha

Qualquer ataque ou falha só precisa ocorrer em um lugar

O QUE É DESCENTRALIZAÇÃO?

- ▶ Autorização de acordo com um **protocolo 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**
- ▶ Movimento Cypherpunk
- ▶ <https://github.com/bitcoin>



MOTIVAÇÃO

Confiamos aos bancos alguns serviços bastante críticos:

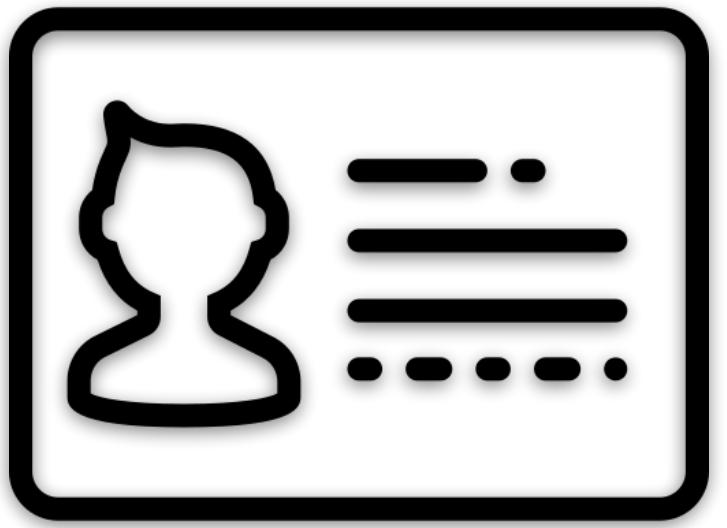
- ▶ Transferir e resgatar dinheiro
- ▶ Registrar corretamente o histórico da conta e transações
- ▶ Armazenar nossa informação pessoal





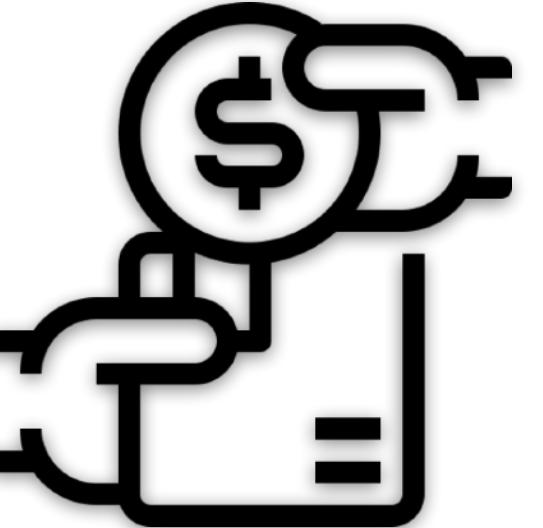
Como fazemos um serviço descentralizado que faz o mesmo o que um banco faz?

COMPONENTES BITCOIN



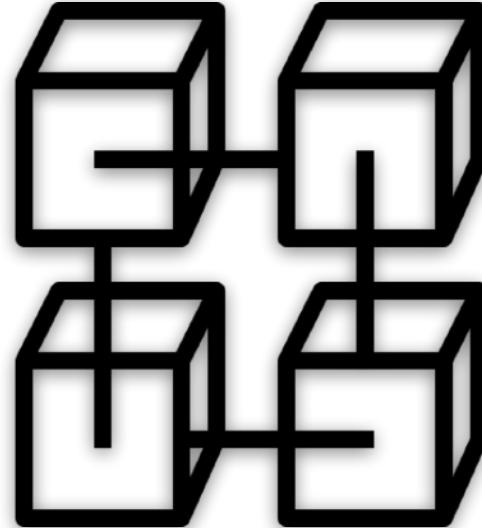
Identidade

Endereços/Contas que podem conter, enviar e receber bitcoin



Transações

Habilidade de enviar e receber bitcoin com segurança



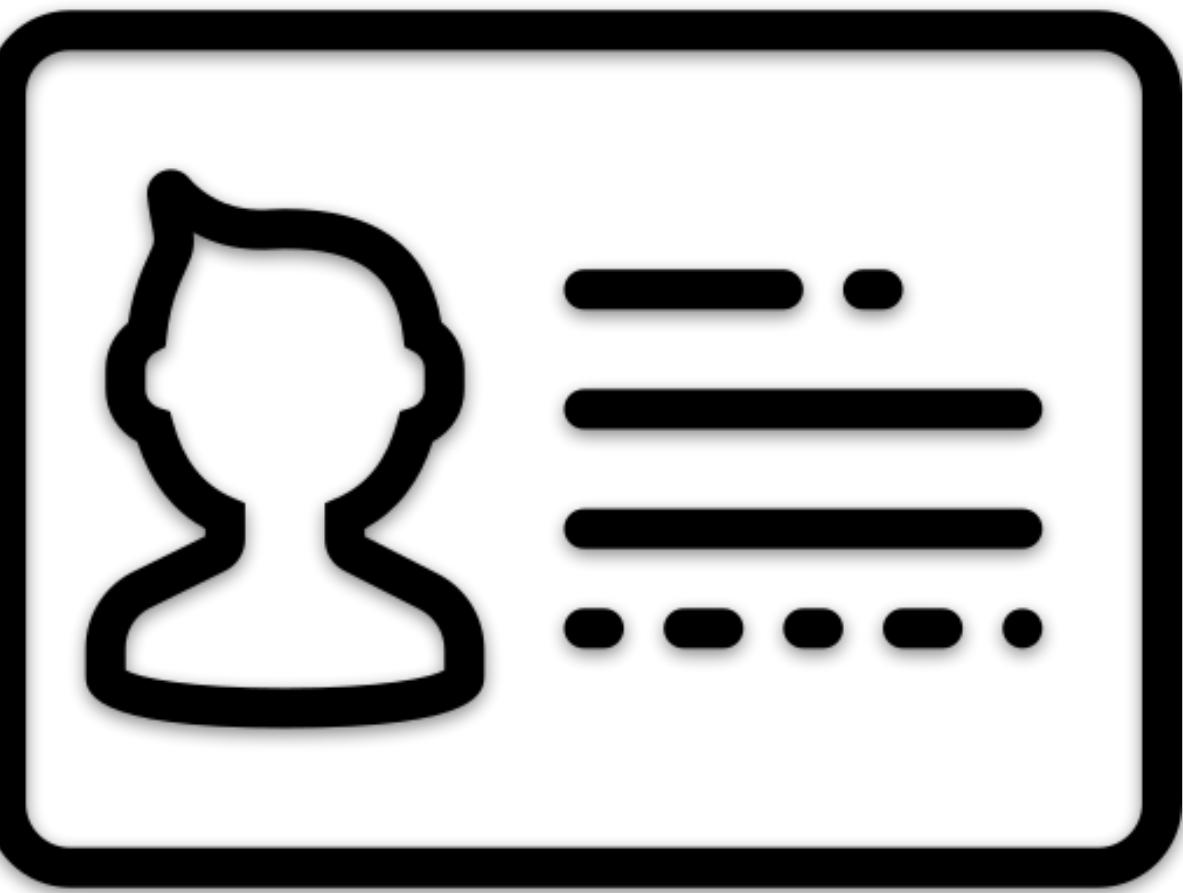
Registro Distribuído

Registros de transações bitcoin são mantidas através da rede



Consenso *trustless*

Concordar com as mudanças do livro-registro



IDENTIDADE

IDENTIDADE

Qual o papel da **identidade** no contexto de moedas?

IDENTIDADE

- ▶ Qual o papel da identidade no contexto de moedas?
 - ▶ **Receber** dinheiro
 - ▶ **Reivindicar/gastar** dinheiro
 - ▶ **Não-repúdio**
- ▶ Identidade no cotidiano:
 - ▶ Residências tem **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 entidade 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

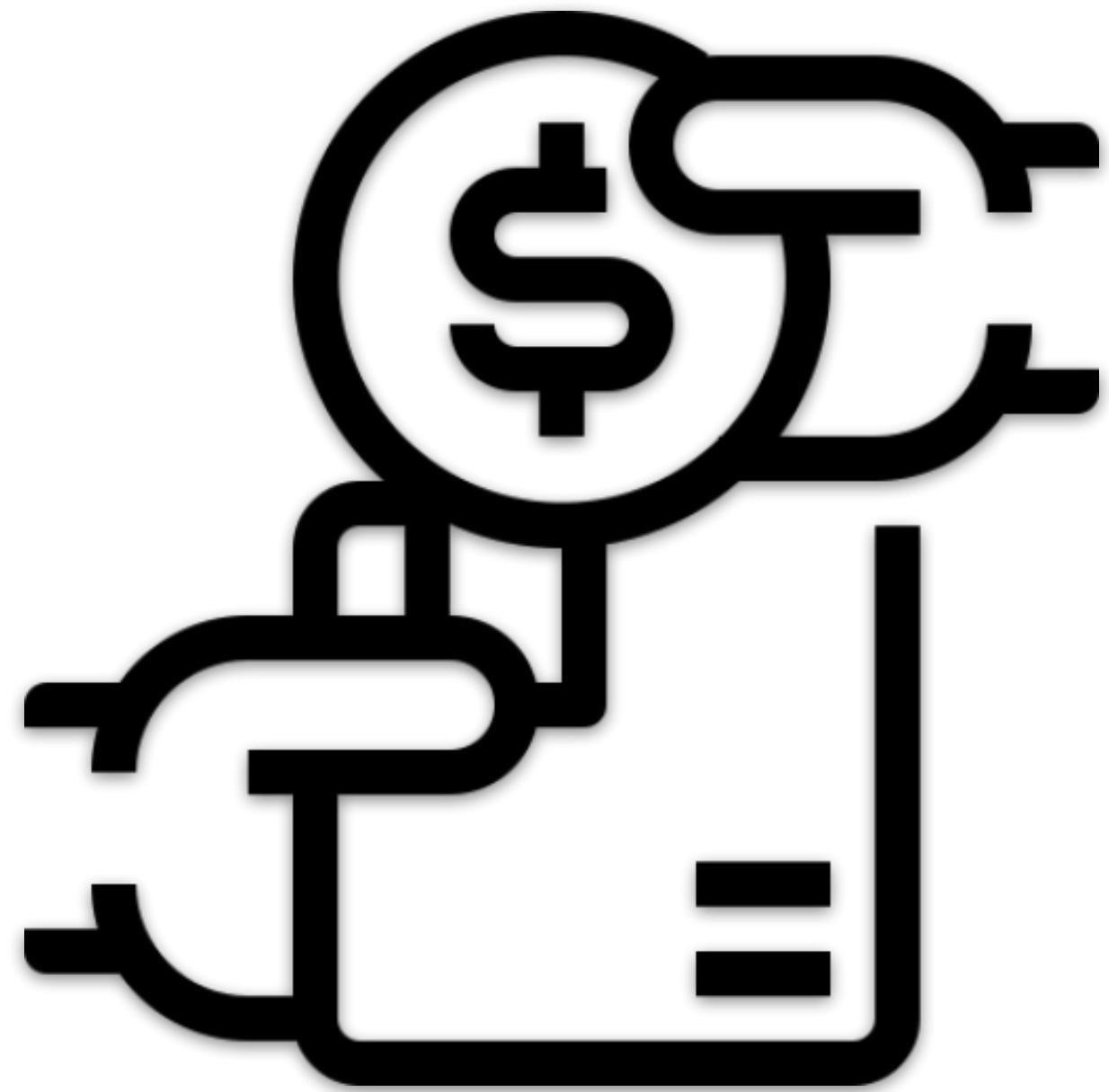
IDENTIDADE: CHAVES PÚBLICAS E PRIVADAS

- ▶ 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?!

IDENTIDADE: SEGURANÇA



TRANSAÇÕES

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

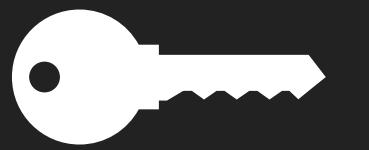
| Daniel |
|-----------------|
| Saldo: \$100,00 |
| -10,00 |

| Alice |
|-----------------|
| Saldo: \$250,00 |
| +10,00 |

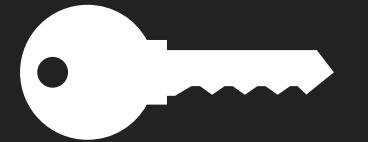
TRANSAÇÕES: MODELO UTXO

- ▶ Blockchain 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



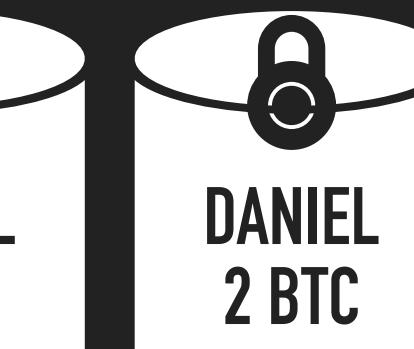
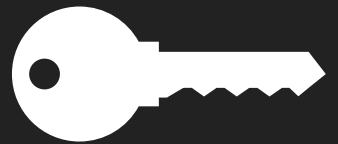
Alice



João



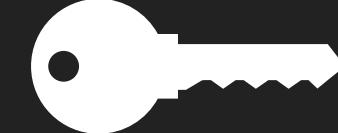
Daniel



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

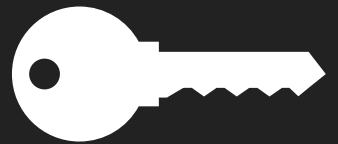
Alice



João



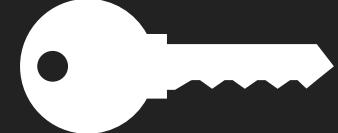
Daniel



Daniel envia 4 BTC para Alice:

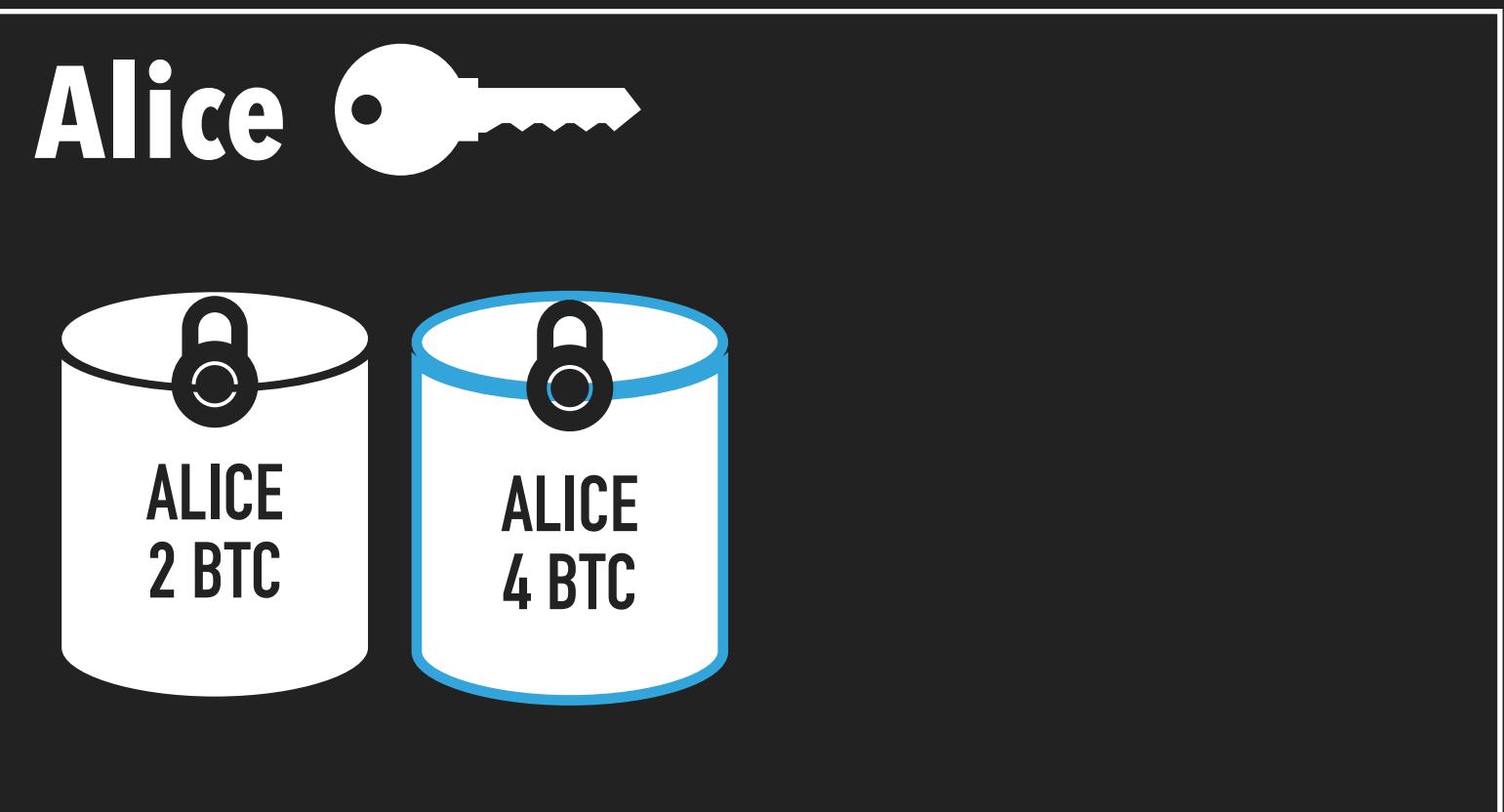
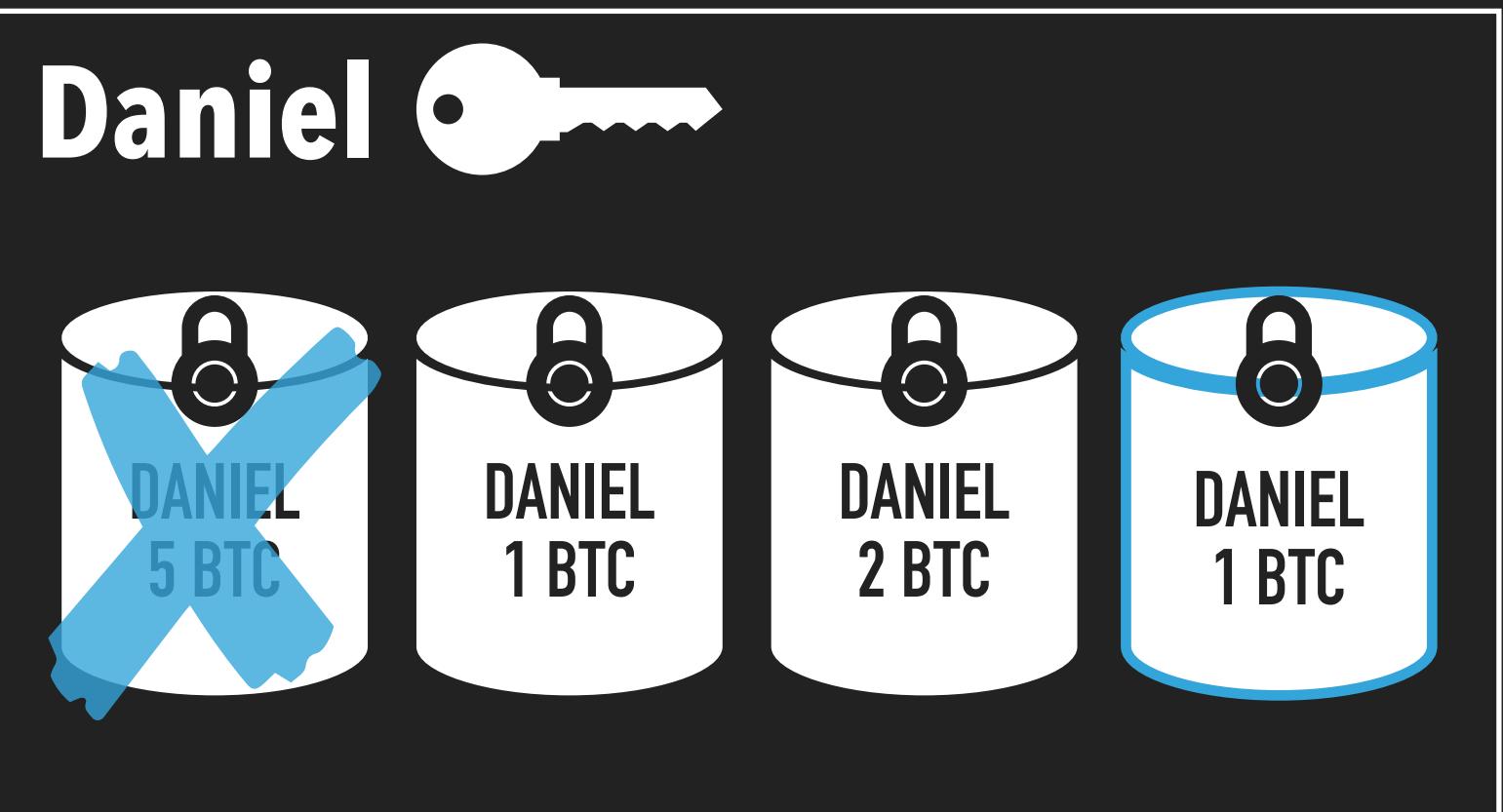
- Resgatando seu UTXO contendo 5 BTC
- Enviando 4 BTC para Alice
- e enviando 1 BTC de volta para ele mesmo

Alice



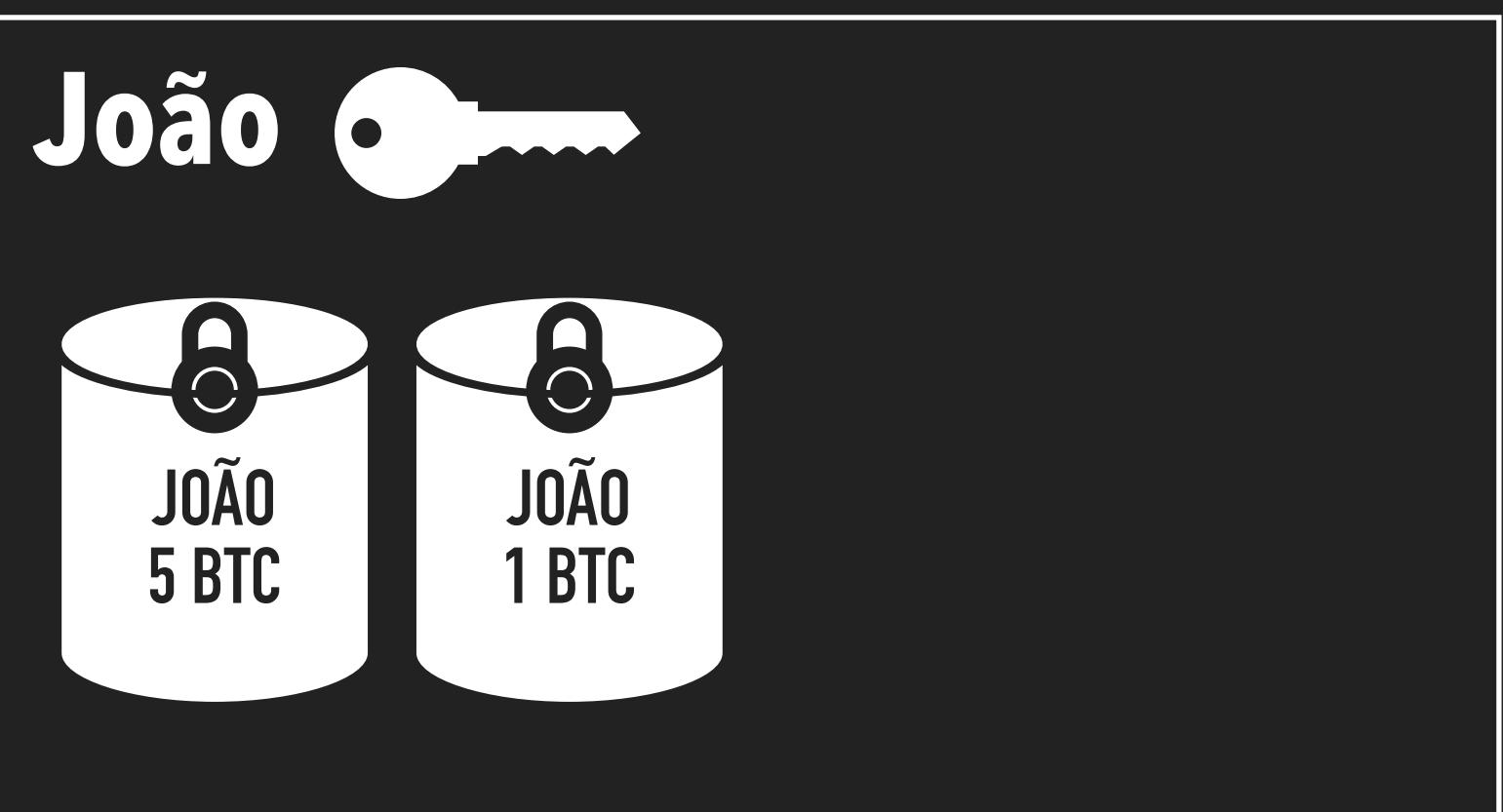
João

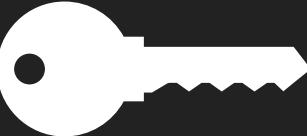




Alice envia 5 BTC para João:

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



Daniel 



Alice 



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

João 

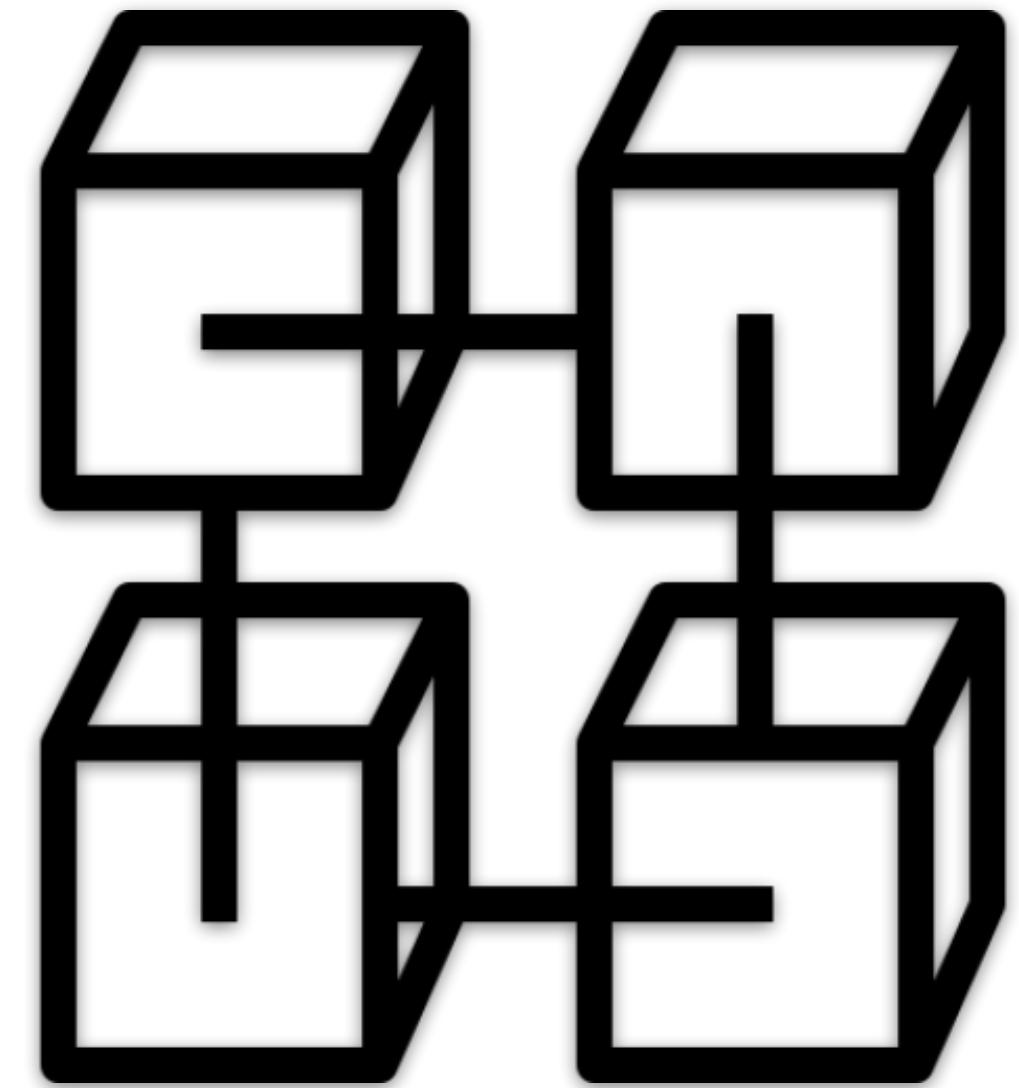


TRANSAÇÕES: MODELO UTXO

Resumindo, não existem bitcoins, somente UTXOs

NO MUNDO BITCOIN...

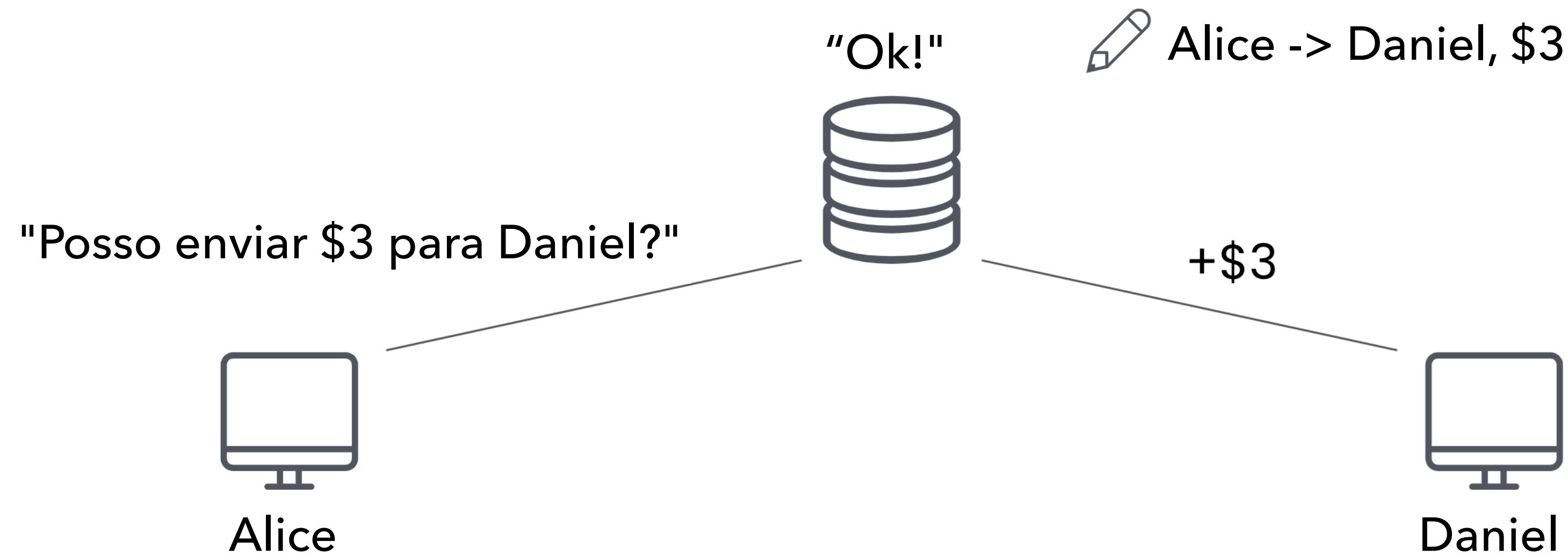
- ▶ A rede Bitcoin pode operar com valores fracionários de Bitcoin
 - ▶ Até a ordem de grandeza de 10^{-8} (0,0000001)
- ▶ Alguns nomenclaturas comuns:
 - ▶ 1 bitcoin (BTC)
 - ▶ 1 milibitcoin ou milibit (mBTC) = $1/1.000$ BTC = 0,001 BTC
 - ▶ 1 microbitcoin ou microbit (μ BTC) = $1/1.000.000$ BTC = 0,000001 BTC
 - ▶ 1 satoshi = $1/100.000.000$ BTC = 0,00000001 BTC



**REGISTROS E
BLOCKCHAIN**

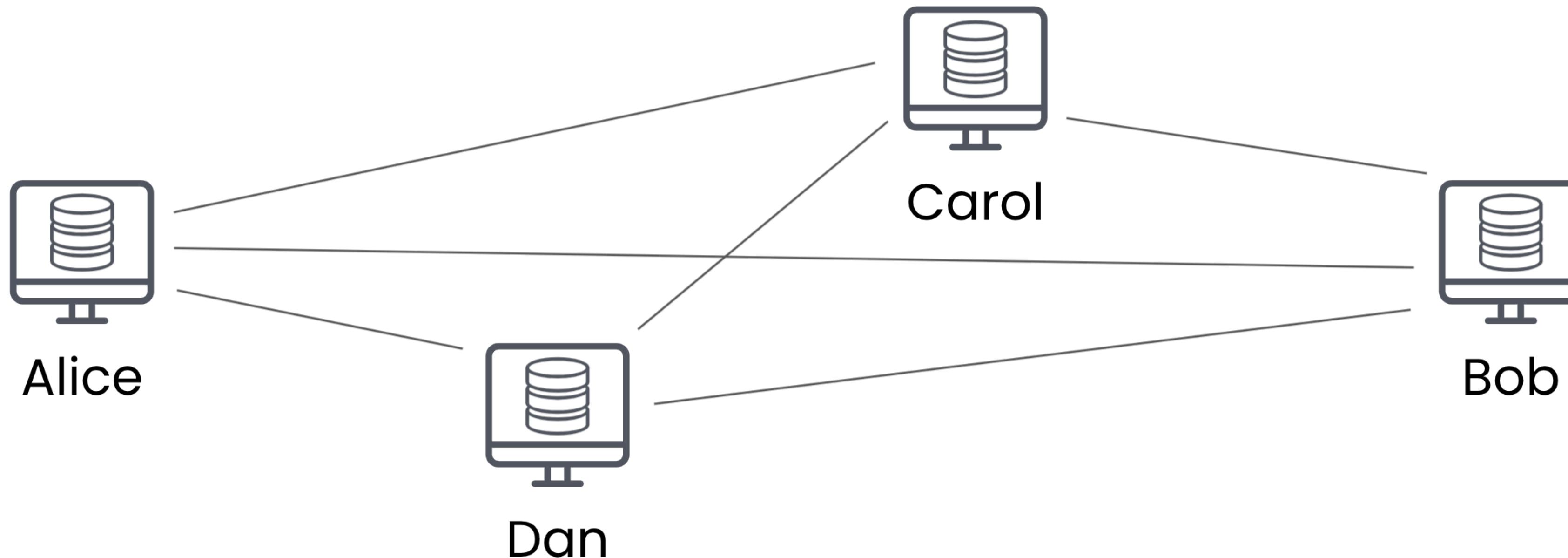
REGISTRO: MODELO TRADICIONAL

- ▶ Banco de dados centralizado armazena todos os dados
- ▶ Gerência central atualiza os dados através de *updates*
- ▶ Medidas de segurança para prevenir *hackers* e falhas



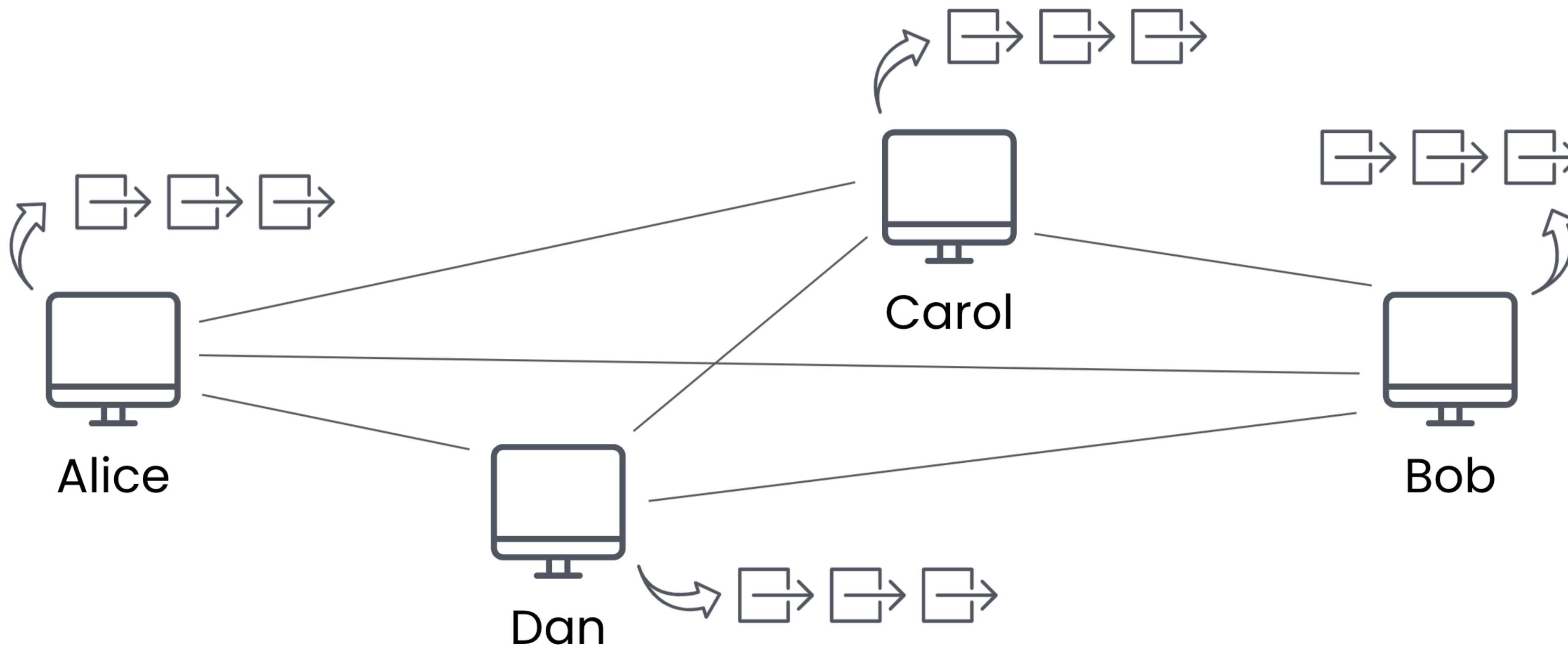
REGISTRO DISTRIBUÍDO: BLOCKCHAIN

- ▶ 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
(PROOF-OF-WORK)**

O QUE É CONSENSO?

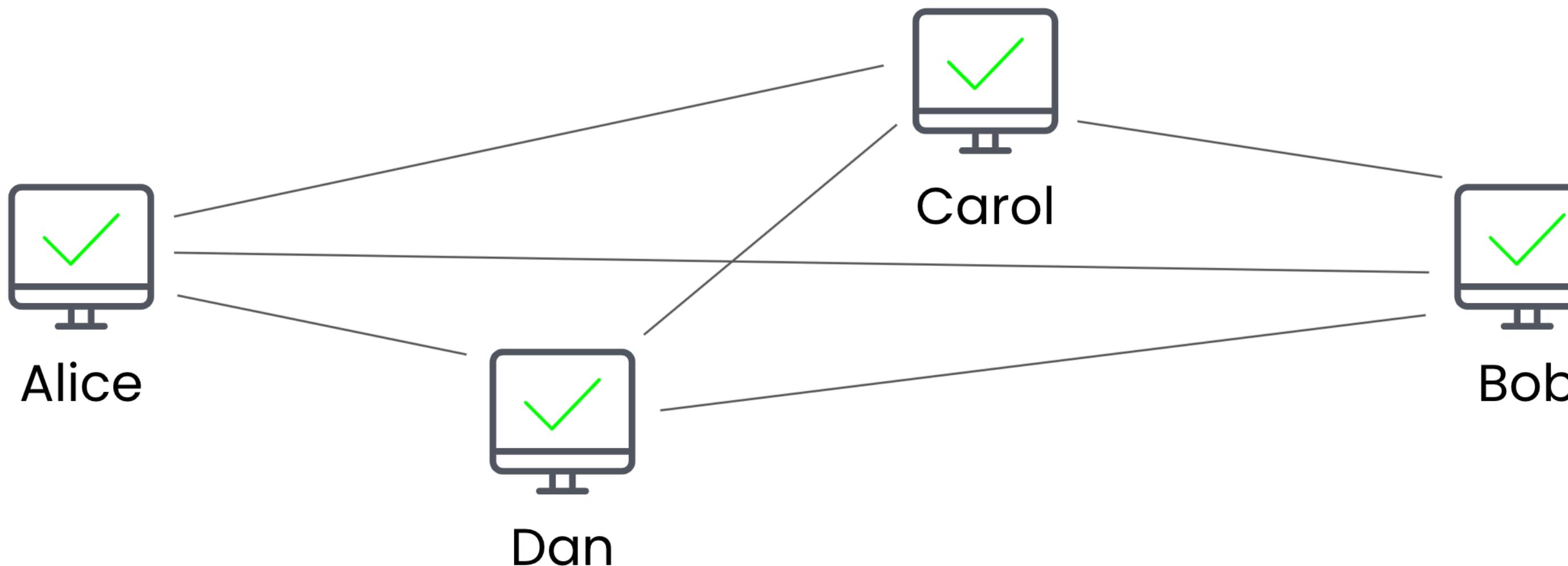
- ▶ **Consenso** é o processo pelo qual os participantes de uma rede chegam a um acordo sobre alguma decisão a ser tomada.
- ▶ Em nosso caso, concordar com alterações em um livro-razão.
- ▶ Tradicionalmente muito simples: confiamos 100% no banco!

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.
- ▶ Tradicionalmente muito simples: confiamos 100% no banco!

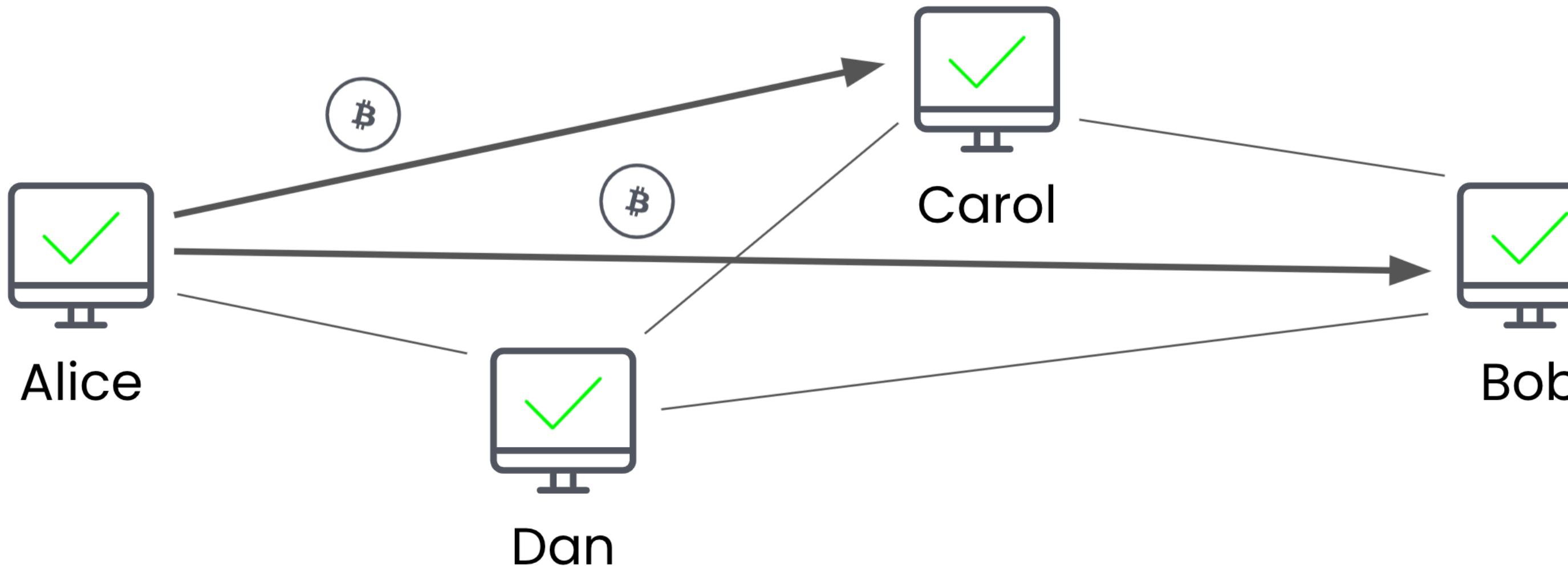
CONSENSO “INGÊNUO”

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



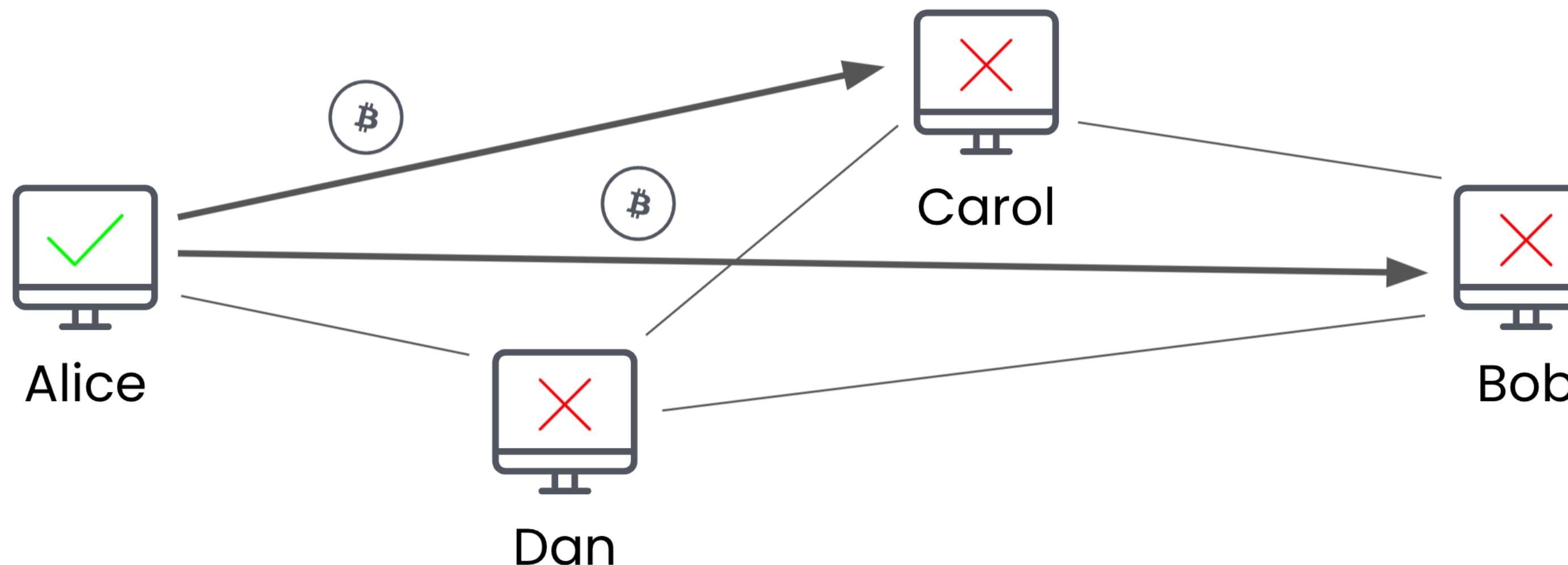
CONSENSO “INGÊNUO”: ATAQUE DE GASTO DUPLO

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



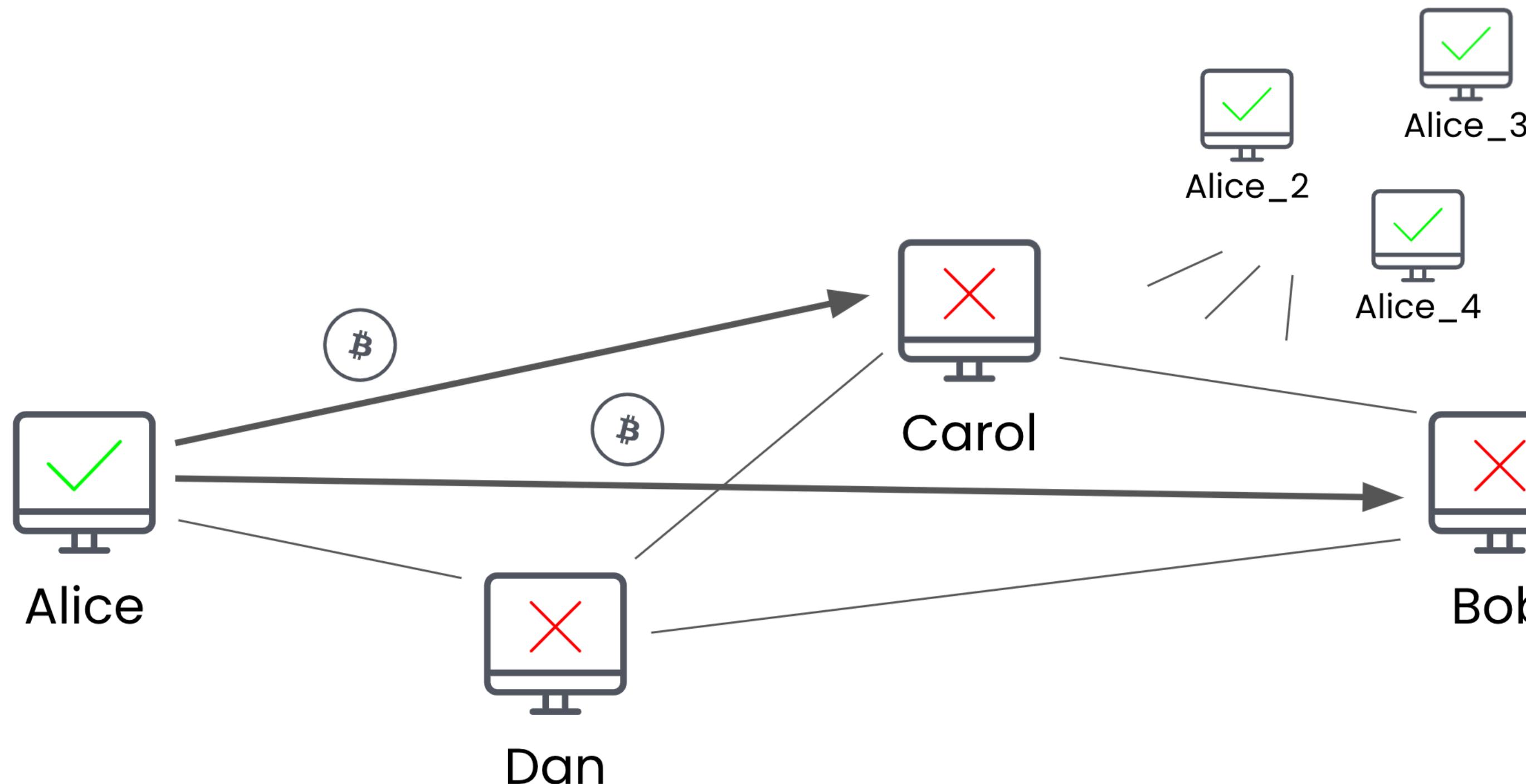
CONSENSO “DEMOCRÁTICO”

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



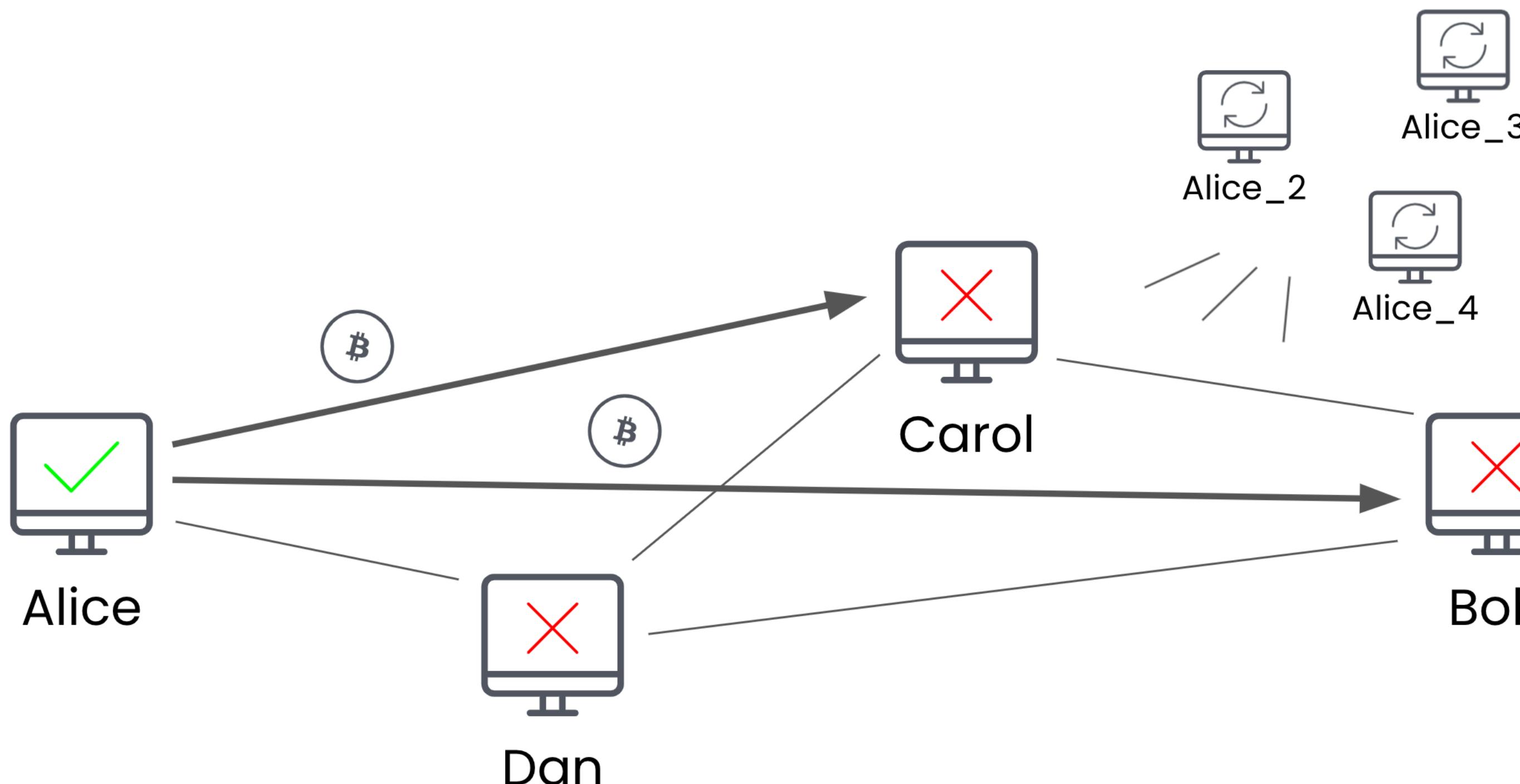
CONSENSO “DEMOCRÁTICO”: ATAQUE SYBIL

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.



RESUMINDO...

- ▶ **Identidade:** Compartilhamos nossa chave pública para transferir Bitcoin e usamos nossa chave privada para resgata-lo;
- ▶ **Transações:** A partir do modelo UTXO, saldos são implicitamente a soma de todos os UTXOs que você pode resgatar;
- ▶ **Registro:** Cada entidade armazena uma cópia do blockchain, o livro-razão distribuído;
- ▶ **Consenso:** Pares lançam propostas via *proof-of-work*, um processo de votação custoso, para evitar ataques de gasto duplo (*double spend*).