Bitcoin: Blockchain e pagamentos digitais peer-to-peer

Sistemas Distribuídos 2023/24

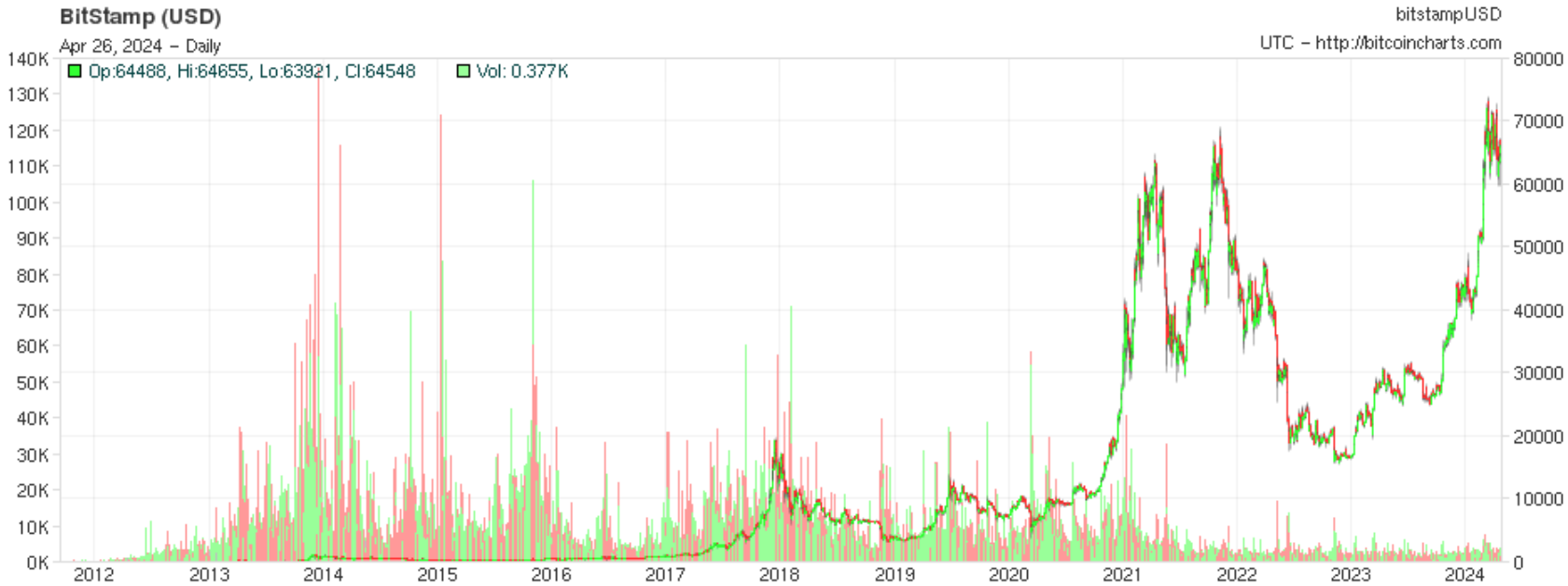
O que é uma moeda e para que serve?

- Para algo ser uma moeda, deve ter as seguintes características:
  - ser um meio de trocas comerciais (pagamentos);
  - ser uma unidade convertível de conta (preço de bens e serviços);
  - armazenar valor ao longo do tempo.
- Pode ser um registo ou um objeto físico, desde que verificável:
  - moeda fiduciária (notas de Euro),
  - moeda mercadoria (metais preciosos),
  - *etc.*

Moedas digitais (ou criptomoedas)

- Na última década surgiram várias *moedas digitais*, que procuram ter todas as características de uma moeda "real".
  - Exemplos: bitcoin, litecoin, worldcoin, zetacoin, novacoin...
- Têm em comum o facto de não usarem uma entidade central.
- Servem, em particular, para realizar *pagamentos digitais*.
- A mais popular em valor de mercado é o bitcoin (BTC, XBT).

Bitcoin



Preço de 1 bitcoin em US dollar nos últimos 5 anos (CC BY-SA 3.0)

O que é o Bitcoin?

Dinheiro eletrónico inteiramente **peer-to-peer**.

- É um sistema de software para pagamentos eletrónicos.
- Funciona com base numa rede peer-to-peer, sem qualquer entidade administrativa (banco ou governo).
- Elimina-se o custo da entidade central (taxas), mas também a capacidade de mediação (apoio ao consumidor, seguros, *etc.*).

Duas entidades efetuam transações diretamente, sem terceiros.

Exemplo de realização de pagamento

A Alice entrou na loja do Bob, que aceita pagamentos em bitcoin, e viu uma máquina fotográfica nova.

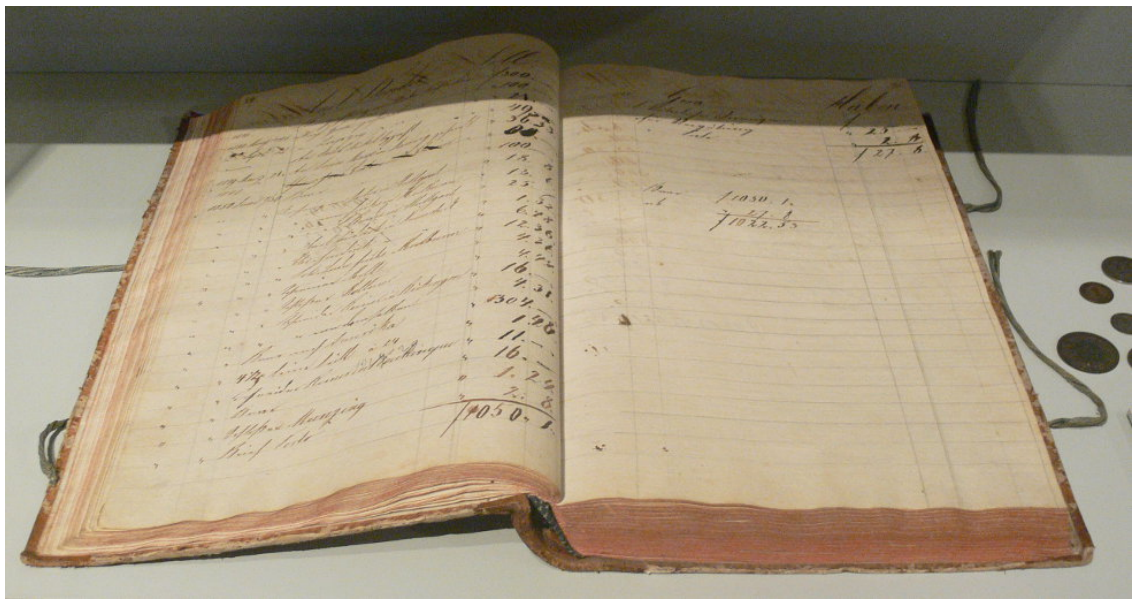
- Na caixa, aceita-se 559EUR ou 0.75BTC (valor de mercado).

- O código QR gerado na caixa tem um URL que identifica o endereço, a quantia, uma etiqueta opcional (nome do beneficiário), e uma mensagem opcional.
- Usando uma carteira instalada num telemóvel, a Alice lê o código e autoriza o pagamento.

Soluções para o problema de *double spending*

Garantir que quem paga não pode gastar a dobrar.

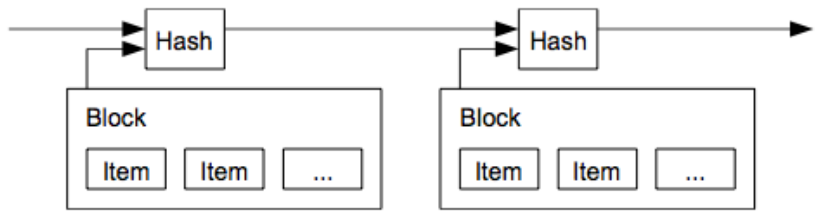
- Introduzindo uma autoridade central de confiança, através da qual passam todas as transações (um banco).



- Sem uma entidade central, as transações devem ser *anunciadas publicamente*, e a maioria dos nós da rede bitcoin mantém-se de acordo quanto ao histórico.

Ideia geral: *block chain*

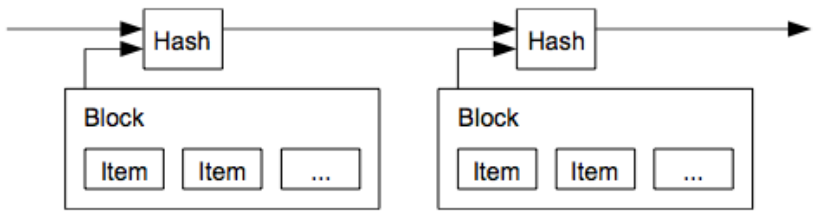
1. Todas as transações (a nível global) são registadas por toda a rede bitcoin, sendo **agrupadas em blocos** sucessivamente.
   - Esses blocos são um "livro de balanços" público.
2. Cada bloco inclui o *hash* do bloco que o antecede.
   - Forma-se uma **cadeia de blocos** para assegurar integridade.
   - Para alterar um bloco no passado ter-se-ia de alterar **todos** os blocos seguintes até ao presente.



3. Criar cada bloco exige também realizar uma operação computacionalmente demorada (*proof-of-work*).
   - Se parte da rede tentasse criar um *branch* na cadeia, nunca conseguiria realizar toda a prova de trabalho.
   - A cadeia de blocos mais longa é a cadeia correta.

Ideia geral: *block chain*

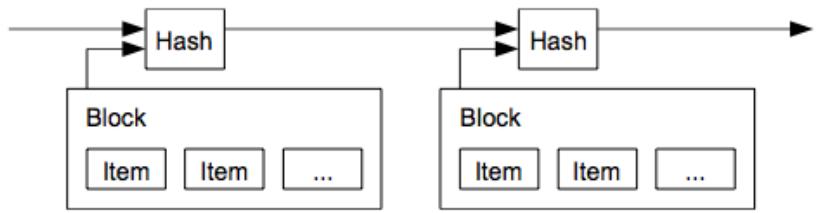
1. Todas as transações (a nível global) são registadas por toda a rede bitcoin, sendo **agrupadas em blocos** sucessivamente.
   - Esses blocos são um "livro de balanços" público.
2. Cada bloco inclui o *hash* do bloco que o antecede.
   - Forma-se uma **cadeia de blocos** para assegurar integridade.
   - Para alterar um bloco no passado ter-se-ia de alterar **todos** os blocos seguintes até ao presente.



3. Criar cada bloco exige também realizar uma operação computacionalmente demorada (*proof-of-work*).
   - Se parte da rede tentasse criar um *branch* na cadeia, nunca conseguiria realizar toda a prova de trabalho.
   - A cadeia de blocos mais longa é a cadeia correta.

Ideia geral: *block chain*

1. Todas as transações (a nível global) são registadas por toda a rede bitcoin, sendo **agrupadas em blocos** sucessivamente.
   - Esses blocos são um "livro de balanços" público.
2. Cada bloco inclui o *hash* do bloco que o antecede.
   - Forma-se uma **cadeia de blocos** para assegurar integridade.
   - Para alterar um bloco no passado ter-se-ia de alterar **todos** os blocos seguintes até ao presente.

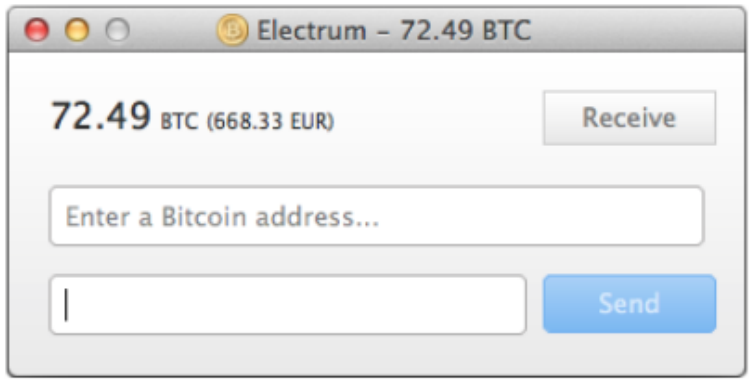


3. Criar cada bloco exige também realizar uma operação computacionalmente demorada (*proof-of-work*).
   - Se parte da rede tentasse criar um *branch* na cadeia, nunca conseguiria realizar toda a prova de trabalho.
   - A cadeia de blocos mais longa é a cadeia correta.

Carteiras de bitcoin

As bitcoins são armazenadas em carteiras.

- Um computador, telemóvel, ou tablet pode ter uma carteira.
- Existem também dispositivos de hardware e serviços na Web.



- Ao criarmos uma carteira (por exemplo, instalando uma aplicação) é gerado o nosso primeiro endereço.
- Podemos dar esse endereço a quem quisermos que nos envie bitcoins, e *vice versa*.

Carteiras de bitcoin

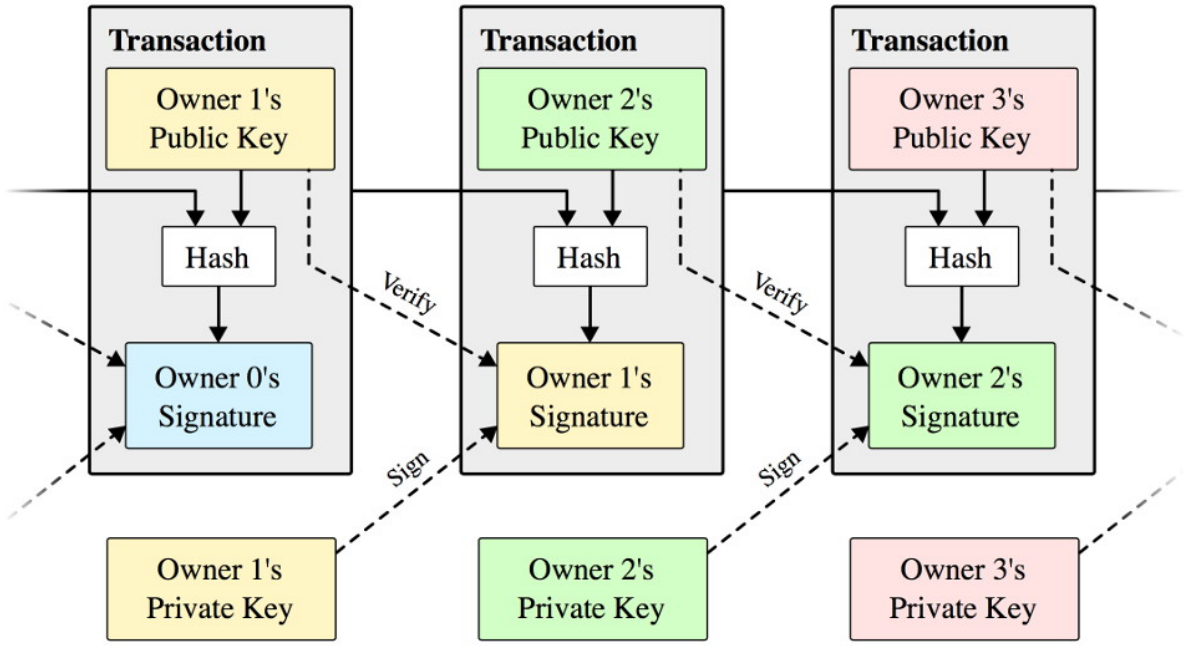
- O bitcoin usa encriptação de chave pública – é gerado um par de chave pública e chave privada.
  - Endereço bitcoin: é o *hash* da chave pública.
  - Credenciais de acesso: a chave privada.
- Uma carteira pode ser vista como um repositório das chaves privadas, devendo também executar pagamentos e verificações.
- Implementações:
  - Bitcoin-Qt e Bitcoin Core são o software de referência.
  - Há carteiras online, como blockchain.info ou coinbase.
  - Pode-se armazenar chaves privadas em papel, metal, *etc.*

Quem perder uma chave privada, perde todas as bitcoins associadas.

Transações eletrónicas

Uma moeda eletrónica forma uma cadeia de assinaturas digitais.

- Transferência: assinatura digital do *hash* da transação anterior e da chave pública do beneficiário (o bitcoin usa SHA-256).
- Verificação: confirmação da cadeia de proprietários.



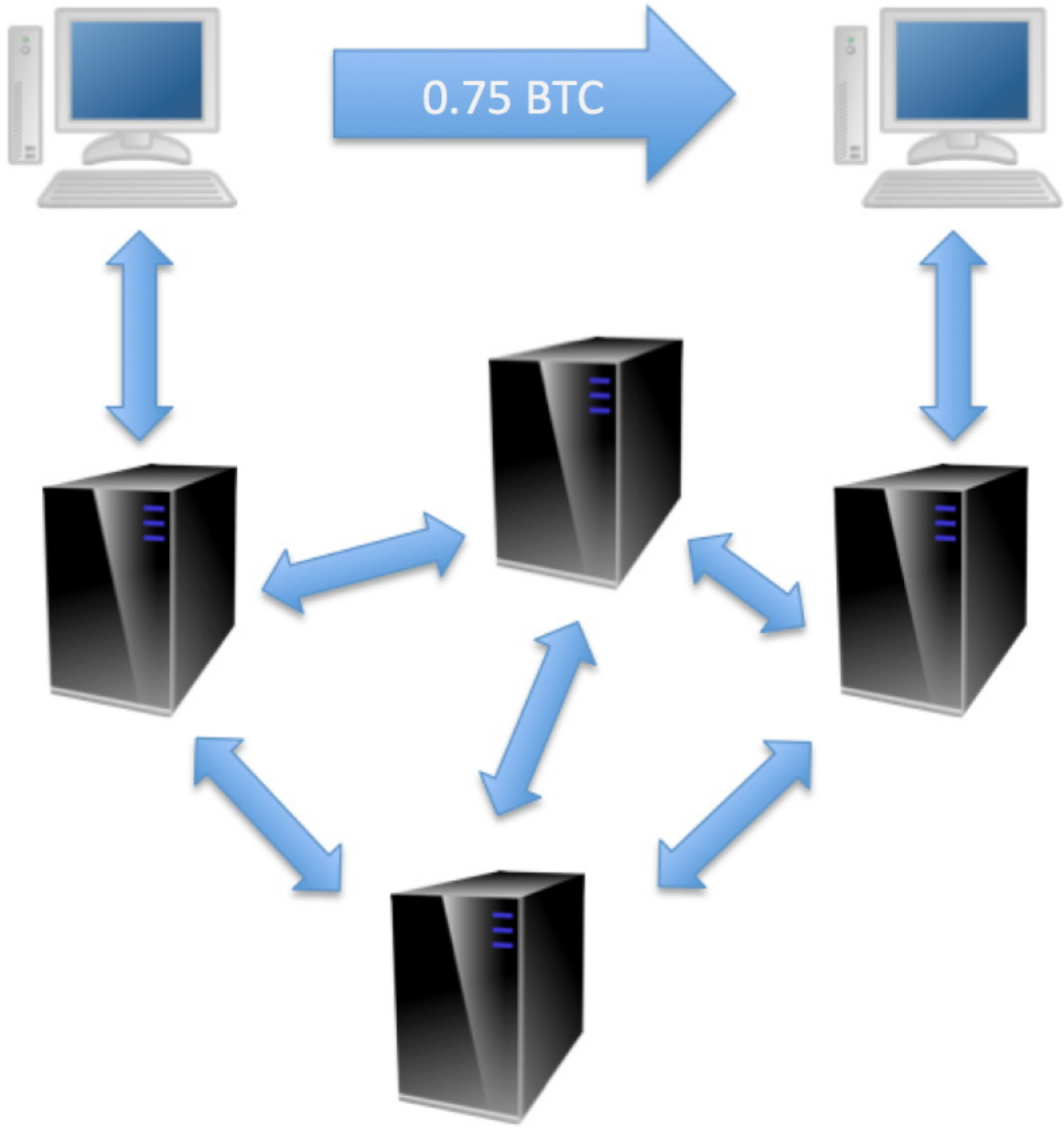
Fonte: 'Bitcoin: A peer-to-peer electronic cash system', Satoshi Nakamoto, 2008.

Como verifica um *beneficiário* que o *ordenante* não gastou a dobrar (double spending)?

Balanços de conta – *block chain*

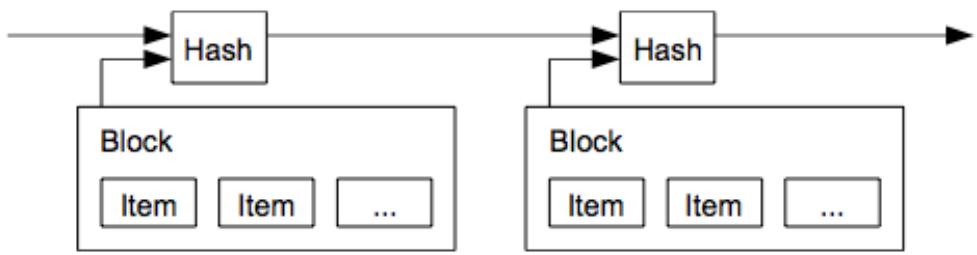
- As transações confirmadas de bitcoin ficam registadas num livro de balanços distribuído, designado por *block chain*.
- Através da *block chain* sabe-se a cadeia de pertença das moedas de bitcoin (cada cliente pode saber o balanço).
- Block chain = livro de balanços público e partilhado.
- Aproximadamente de 10 em 10 minutos, um novo bloco de transações aceites é adicionado à *block chain*.
- Nós que pertençam à *rede bitcoin* armazenam uma cópia da block chain (descartam-se transações antigas).
- *Double spending* solucionado usando puramente peer-to-peer.

A rede bitcoin



A rede bitcoin

1. Uma nova transação é enviada a todos os nós (broadcast).
2. Cada nó junta num bloco as transações novas.
3. Cada nó executa uma prova de trabalho para esse bloco.
4. Assim que a obtenha, cada nó envia a prova de trabalho a todos os outros nós (broadcast).
5. Os nós aceitam um bloco se e só se todas as transações forem válidas (sem *double spending*).
6. Quando aceitam um bloco, usam o seu *hash* e assumem-no como predecessor do próximo bloco.
7. A cadeia mais longa é sempre considerada a cadeia correta.



Prova de trabalho

A "prova de trabalho" impede que um adversário lance inúmeros processos para criar uma *block chain* aceite pela maioria da rede.

- Novo bloco = Tx1, Tx2, ..., TxN, hash do predecessor, nonce.
- Hash(novo bloco) = 0000000000000010101011101101...
- É necessário incrementar iterativamente o *nonce* e calcular um *hash* até obter um *hash* com zeros suficientes (*proof of work*).
- Verificar que esse trabalho foi feito é trivial.
- O bloco não pode ser modificado sem se refazer o trabalho, e seria também necessário refazer todos os blocos seguintes.

Se pelo menos 51% do poder computacional da rede bitcoin for detido por nós honestos, a cadeia honesta será sempre a mais longa.

Incentivo à participação na rede

- A primeira transação de um bloco é, por convenção, uma nova moeda para quem criou o bloco.
- Além de ser um incentivo para os nós, é a única forma de fazer circular novas moedas de bitcoin (designam-se mineiros).
- Minar bitcoin torna-se progressivamente mais difícil, de forma a que encontrar um *nonce* demore sempre $\sim$10 minutos.
- Cada novo bloco vale 12.5 bitcoins desde julho de 2016.
- Este incentivo reduz-se a metade a cada 210 000 blocos ($\sim$4 anos) e termina em 2140 quando existirem 21M BTC.

A mineração funciona como um sistema de consenso distribuído.

Conclusão

- Soluciona o problema de *double spending* de forma descentralizada, utilizando um esquema de prova de trabalho.
- Todas as transações são registadas numa cadeia de blocos pública.
- Um adversário pode apenas tentar gerar uma cadeia de blocos maior do que o resto da rede, e mesmo que o consiga só poderá reaver o dinheiro que o próprio gastou.
- A confirmação final, para o vendedor, pode demorar 1 hora (a transação deve ficar a 6 blocos de profundidade).

Começa a ser aceite, mas terá todas as características de uma moeda?

Material adicional

- `https://bitcoin.org/en/developer-documentation`

Bitcoin: Blockchain e pagamentos digitais peer-to-peer

Sistemas Distribuídos 2023/24