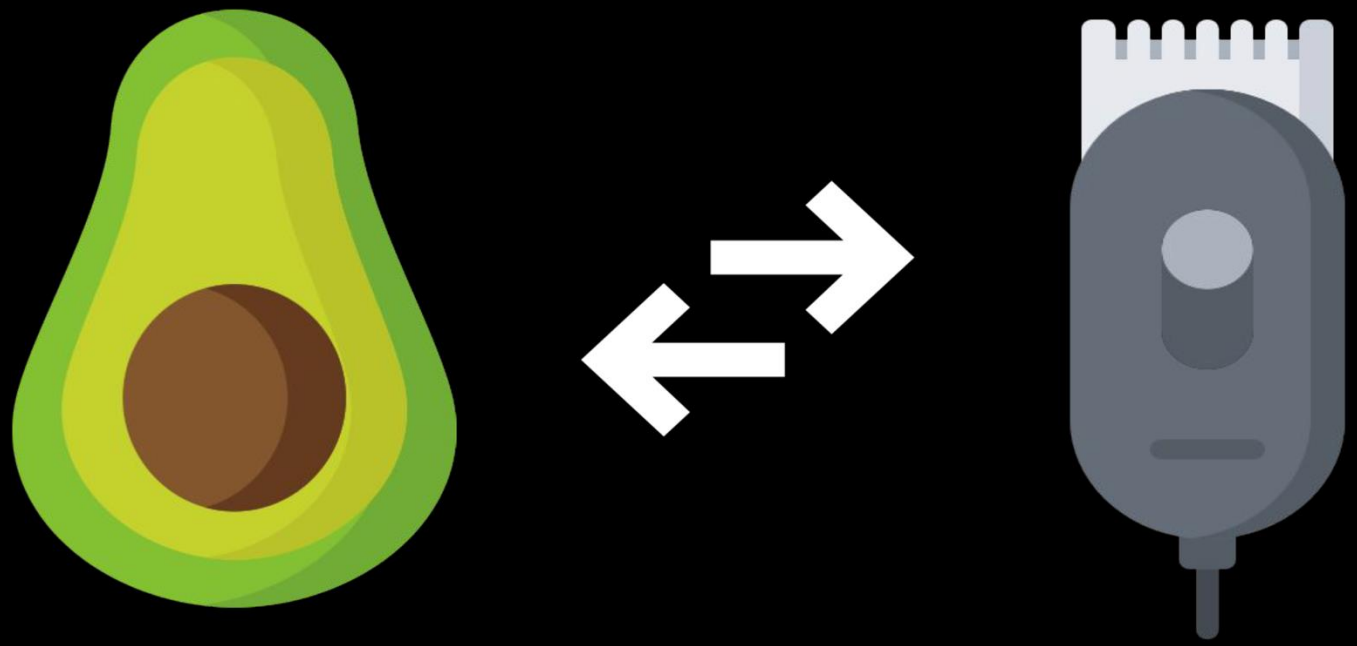
Introdução ao Bitcoin

Um Sistema de Dinheiro Eletrónico Ponto-a-Ponto

O que é o dinheiro?

- O dinheiro serve para facilitar trocas comerciais
- As trocas comerciais existem porque um indivíduo não consegue produzir tudo aquilo que quer consumir

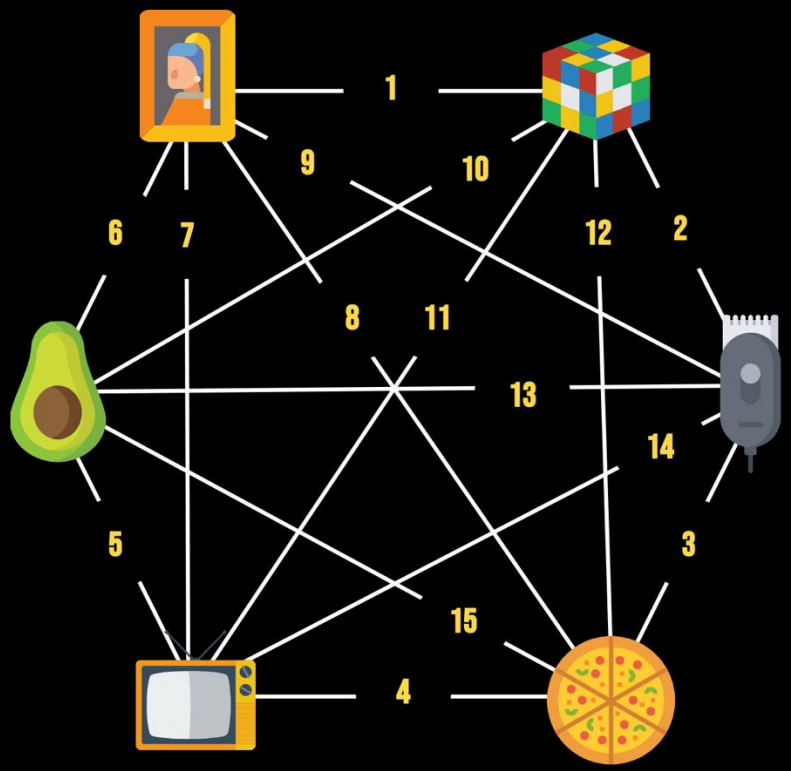


Trocas diretas, ou escâmbio, permitem especialização na produção de um determinado bem






O escâmbio pode funcionar em pequenas escalas. Vejamos um exemplo com 6 produtos.



n(n-1)/2

2 produtos = 1 taxa de câmbio

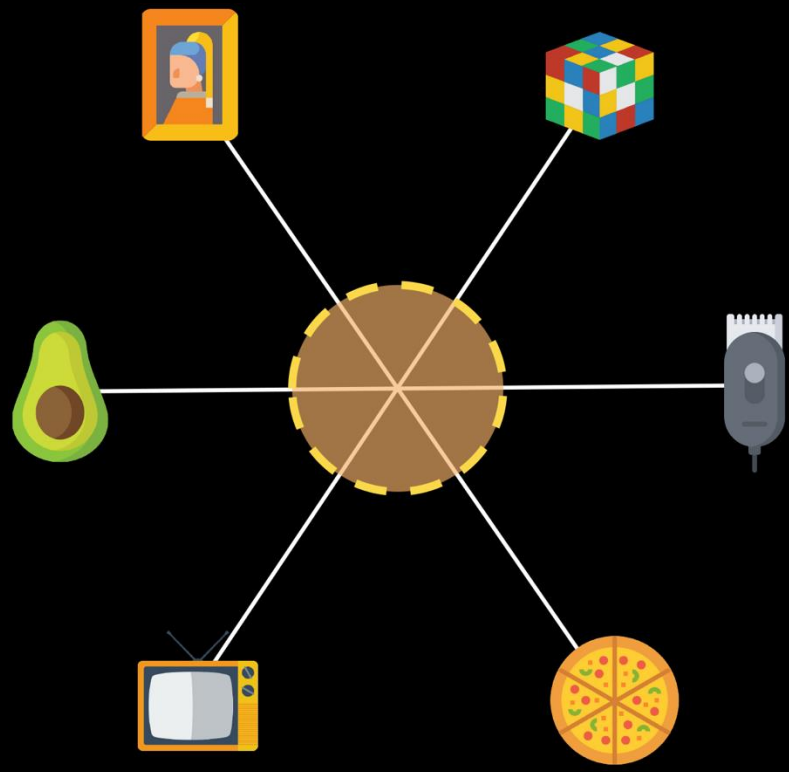
6 produtos = 15 taxas de câmbio

500 produtos = 124 750 taxas de câmbio

Estes 6 produtos traduzem-se em 15 taxas de câmbio.

Este problema de coincidência de vontades é resolvido usando um único bem como meio de troca entre todos os produtos.

Frequentemente, o bem mais comercializável numa economia é denominado de dinheiro.



Funções do dinheiro

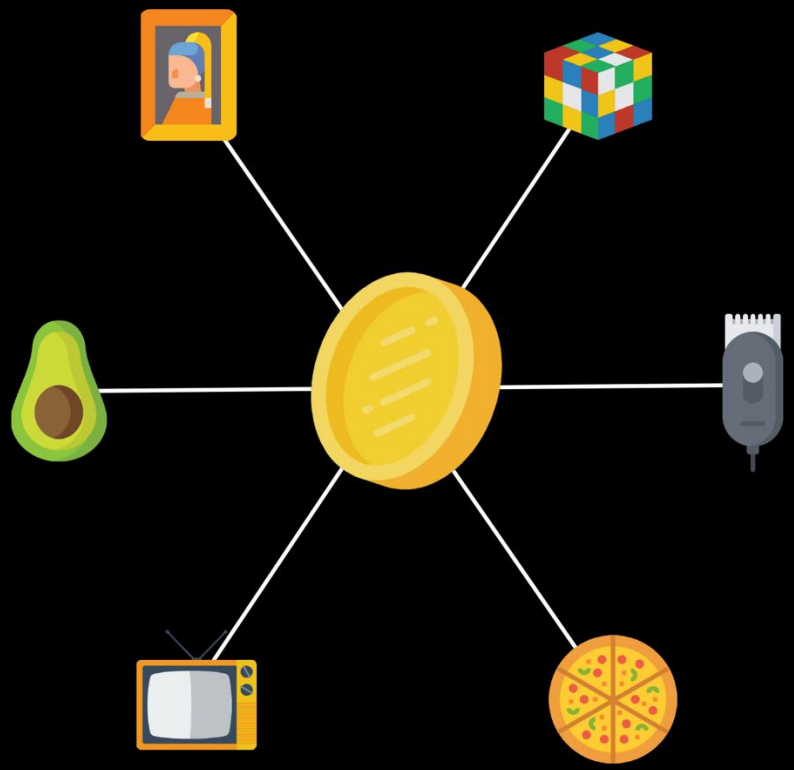
Reserva de Valor

Meio de troca

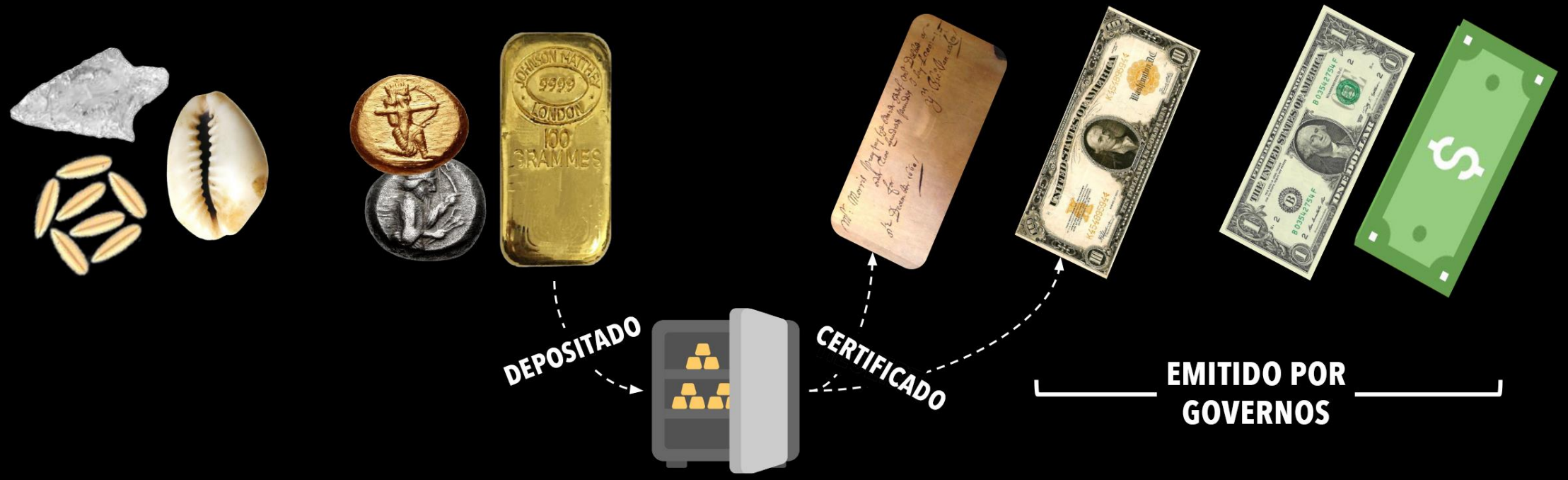
Unidade de conta

Propriedades desejáveis no dinheiro

- Escassez
- Divisibilidade
- Fungibilidade
- Durabilidade
- Portabilidade
- Reconhecibilidade
- Verificabilidade



História do dinheiro



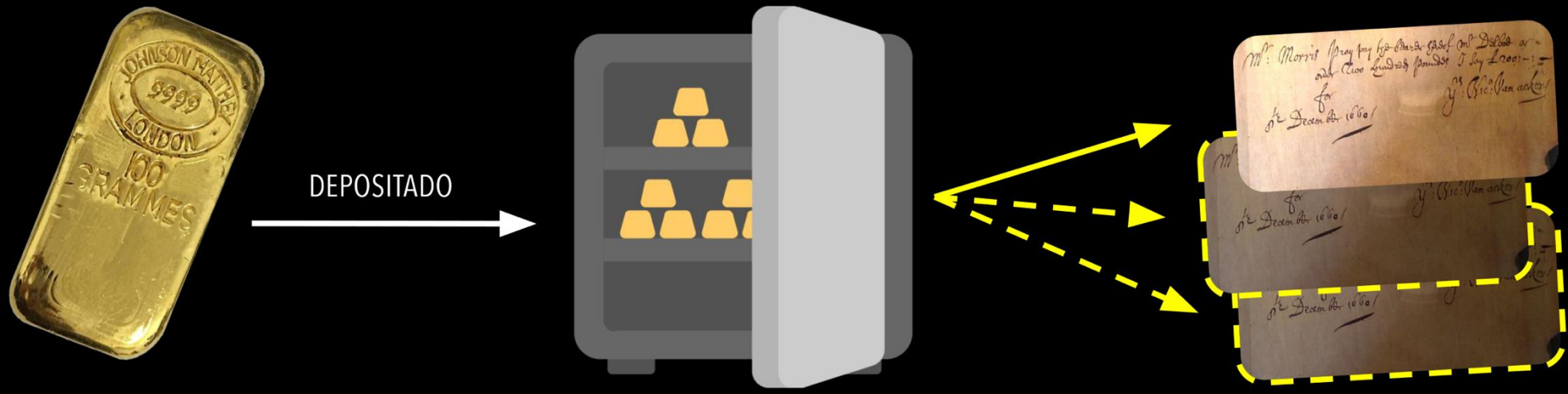
Conchas, utensílios, mercadorias

Metais preciosos

Representações do ouro

Dinheiro hoje

Banca de reserva fracionária



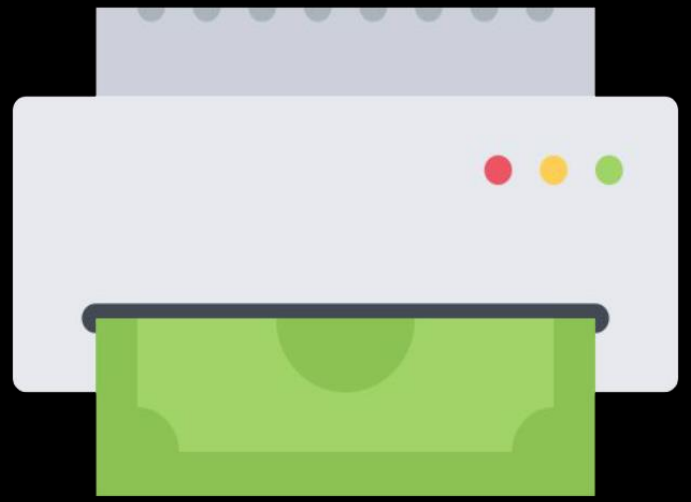
Como as pessoas não levantavam o seu ouro todas as mesmo tempo, os bancos perceberam que podiam emitir mais certificados do que o ouro que guardavam.

Do ouro para o dinheiro fiduciário

WTF happened in 1971?

Como o dinheiro fiduciário não está vinculado a nenhum bem, não há restrição à sua emissão.

Existe um incentivo a criar dinheiro arbitrariamente para suprir necessidades de curto prazo, criando um problema futuro.



$2.90

2004

$5.80

2022

fonte: The Economist Big Mac Index

8 557 BTC

iPhone 4 (2010)

0,04 BTC

iPhone 15 (2023)

O que é o Bitcoin?

Bitcoin: Um Sistema de Dinheiro Eletrónico Ponto-a-Ponto

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Translated in Portuguese from bitcoin.org/bitcoin.pdf
by @rhlinden

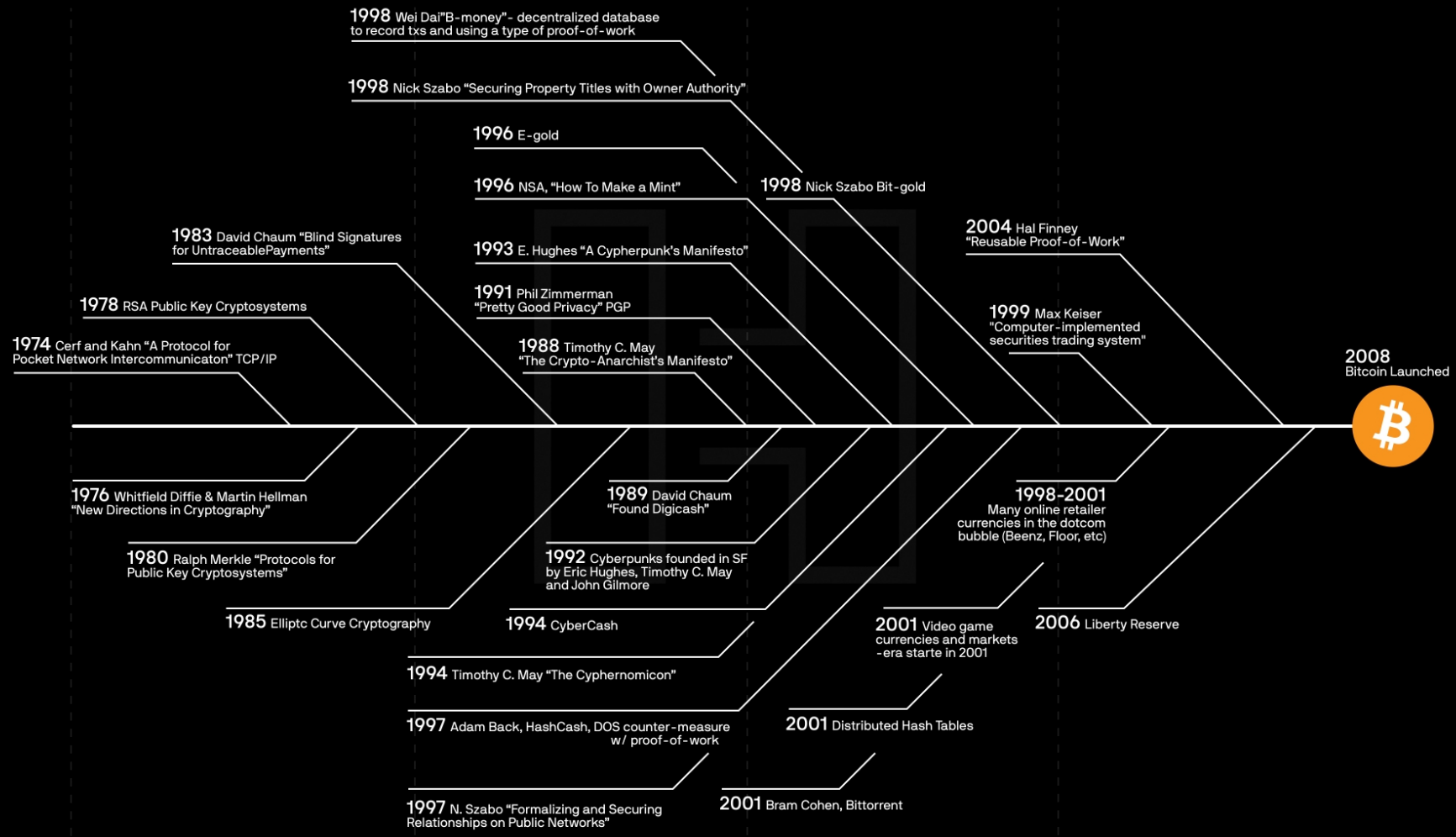
Sinopse. Uma versão puramente ponto-a-ponto de dinheiro eletrónico permitiria o envio de pagamentos interativos diretamente de um interveniente para outro sem passar por uma instituição financeira. Assinaturas digitais proporcionam parte da solução, mas os principais benefícios perdem-se se continuar a ser necessária uma terceira entidade de confiança para evitar gastos duplos. Propomos uma solução para o problema do gasto duplo usando uma rede ponto-a-ponto. A rede marca a hora nas transações codificando-as numa cadeia continua de provas-de-trabalho baseada em *hash*, formando um registo que não pode ser alterado sem refazer a prova-de-trabalho. A cadeia mais longa, não só serve de prova da sequência de acontecimentos testemunhados, mas prova que tem origem no grupo de maior capacidade de processamento. Desde que a maioria da capacidade de processamento seja controlada por nós que não estejam conjugados para atacar a rede, eles produzirão a cadeia mais longa e prevalecerão sobre atacantes. A própria rede necessita uma estrutura mínima. As mensagens são difundidas numa base do melhor esforço, e os nós podem abandonar e reintegrar a rede à vontade, aceitando a cadeia mais longa de provas-de-trabalho como prova do que aconteceu enquanto estiveram fora.

1. Introdução

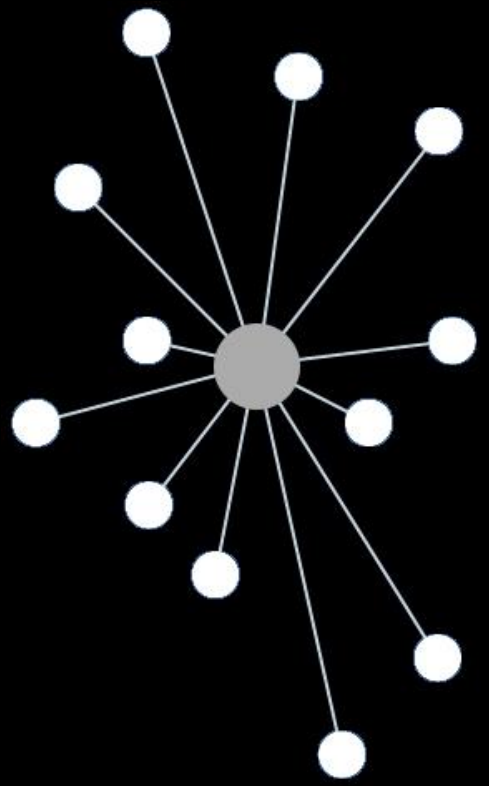
O comércio na Internet vem dependendo quase exclusivamente de instituições financeiras atuando como terceira parte de confiança para o processamento de pagamentos eletrónicos. Embora o sistema funcione suficientemente bem para a maioria das transações, continua a sofrer das fraquezas inerentes ao modelo baseado na confiança. Transações completamente irreversíveis não são possíveis, uma vez que as instituições financeiras não podem evitar a mediação de disputas. O custo da mediação aumenta os custos da transação, limitando o tamanho mínimo praticável e restringindo a possibilidade de pequenas transações casuais, e há um custo mais alargado na perda da capacidade de efetuar pagamentos irreversíveis de serviços irreversíveis. Com a possibilidade de reembolso, a necessidade de confiança aumenta. Os comerciantes devem ser cuidadosos com os seus clientes, exigindo mais informação que a de outra forma seria necessária. Uma certa percentagem de fraude é aceite como inevitável. Estes custos e incertezas do pagamento podem ser evitadas usando moeda física em pessoa, mas não existe mecanismo para fazer pagamentos sobre um canal de comunicações sem uma terceira parte de confiança.

O que é necessário é um sistema eletrónico de pagamento baseado em prova criptográfica e

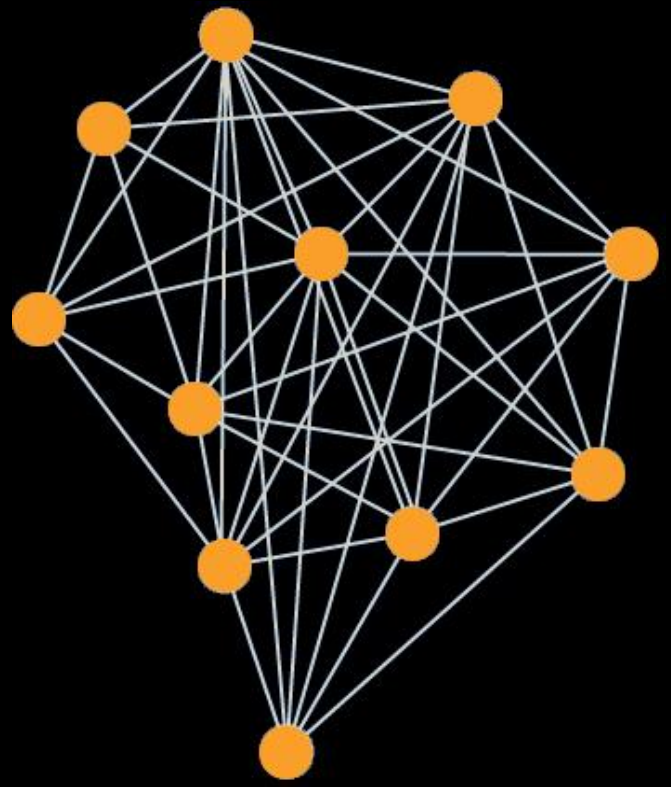
A Pré-história do Bitcoin – o resultado de 40 anos de investigação, desenvolvimento e procura



Created by: @danheld
Inspired by: @anselLinder @btcmrkts

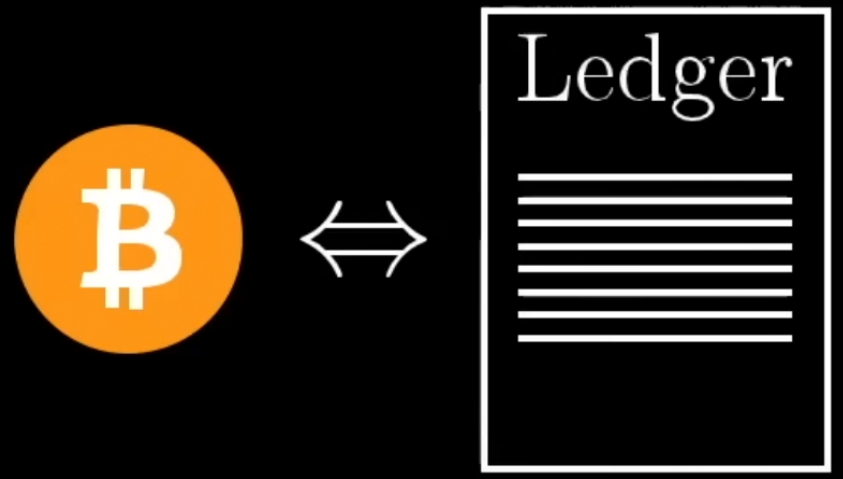


Centralizado

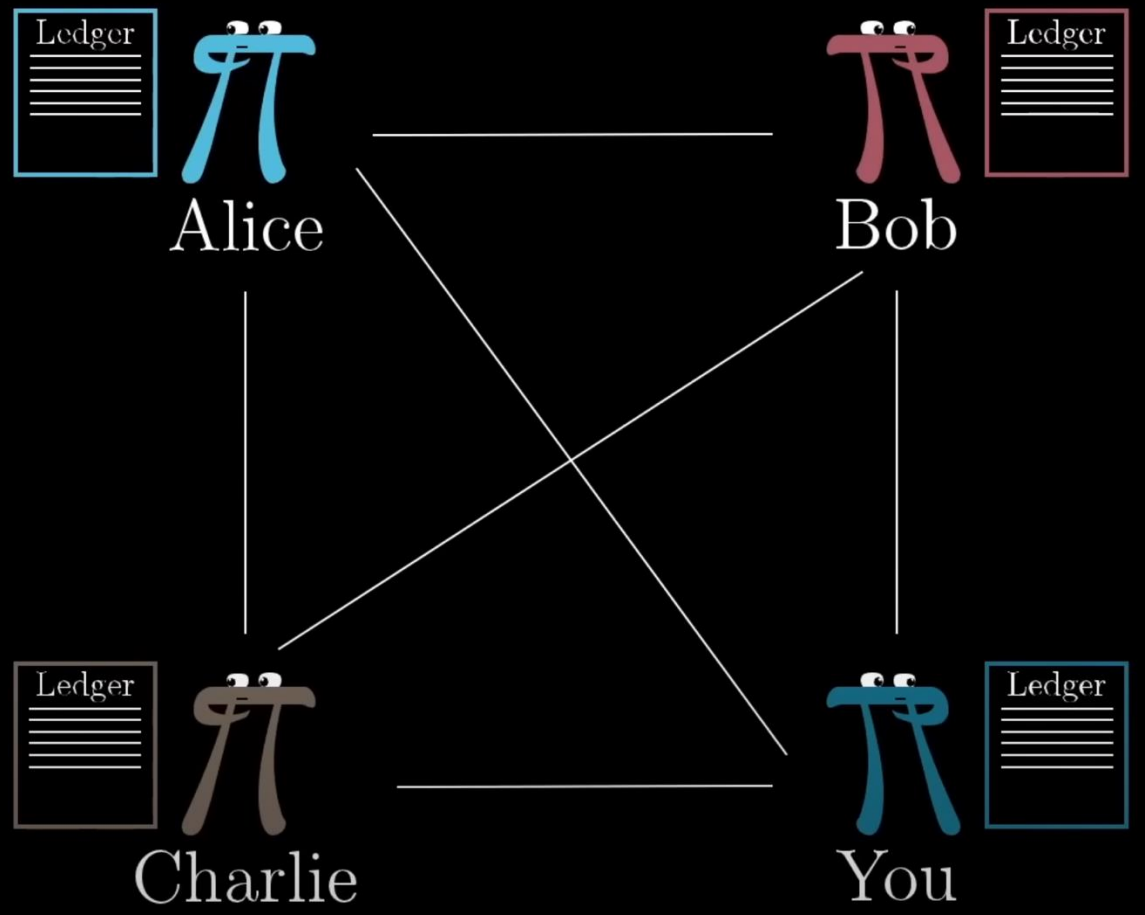


Descentralizado

Registo de quem é dono do quê, através de um livro-razão (*ledger*) distribuído por todos os participantes da rede, de forma a não depender de nenhuma entidade central.



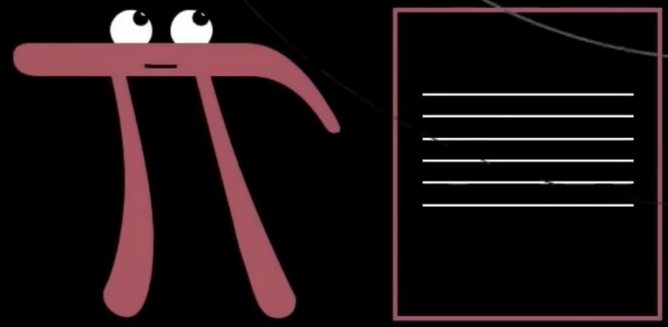
As alterações ao livro-razão são verificadas e registadas por todos os participantes.



Como funciona o Bitcoin?

Transações

Quando alguém quer enviar bitcoin, compõe uma transação que assina com a sua chave privada. Esta transação é propagada por toda a rede. No entanto, só é incluída no livro-razão quando fizer parte de um bloco minerado.



Alice paga ao Bob 0.1 BTC Alice

Charlie paga à Alice 0.3 BTC Charlie

Bob paga ao Charlie 0.5 BTC Bob

Criptografia de chave pública

Sistema criptográfico que usa pares de chaves: chave pública, que pode ser partilhada com terceiros, e chave privada que é conhecida apenas pelo proprietário.

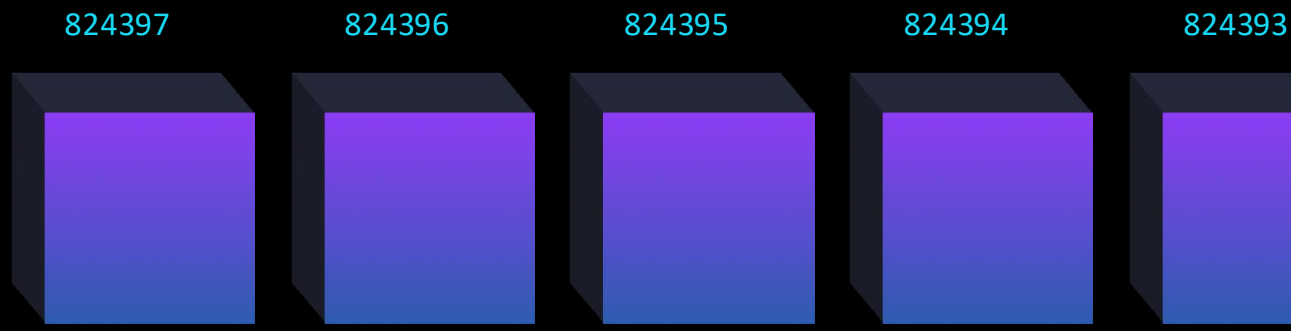
Bloco

Um bloco serve para agrupar transações, de modo a não ter que conciliar os livros-razão de todos os participantes cada vez que há uma nova transação.

Timechain

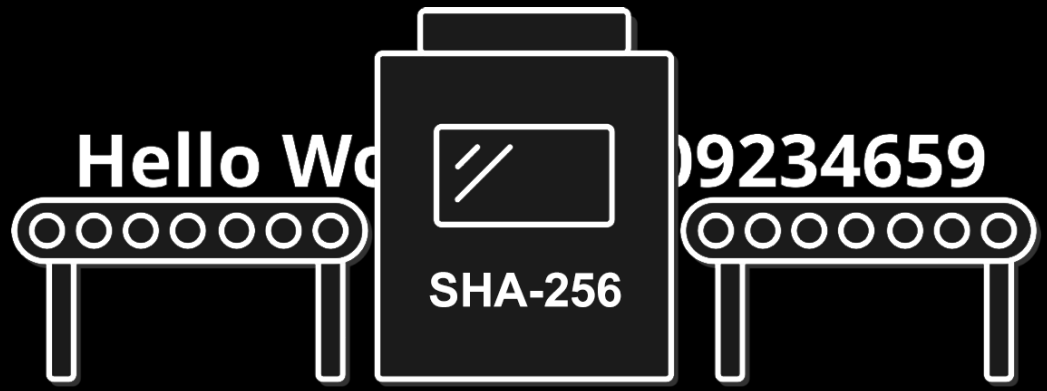
A timechain é uma cadeia de blocos (block chain) ordenados cronologicamente.

Para além de transações, um bloco inclui uma referência ao bloco anterior de modo a provar que este lhe sucede. Isto é importante para manter a integridade cronológica das transações.



Mineração

Um bloco é produzido (minerado) colocando o seu conteúdo como variável numa função criptográfica (SHA-256) cujo resultado é um número imprevisível.



Para o bloco ser válido este número tem de ser inferior a um alvo definido no protocolo.

Prova de trabalho

Visto que o número é imprevisível, não é possível ajustar criteriosamente a variável de modo a obter o resultado desejado. Assim, não há alternativa senão a tentativa e erro.

Este processo repetitivo consome energia, provando que deu trabalho chegar ao resultado desejado. A este processo chama-se prova de trabalho (*proof-of-work*).

Recompensa de bloco

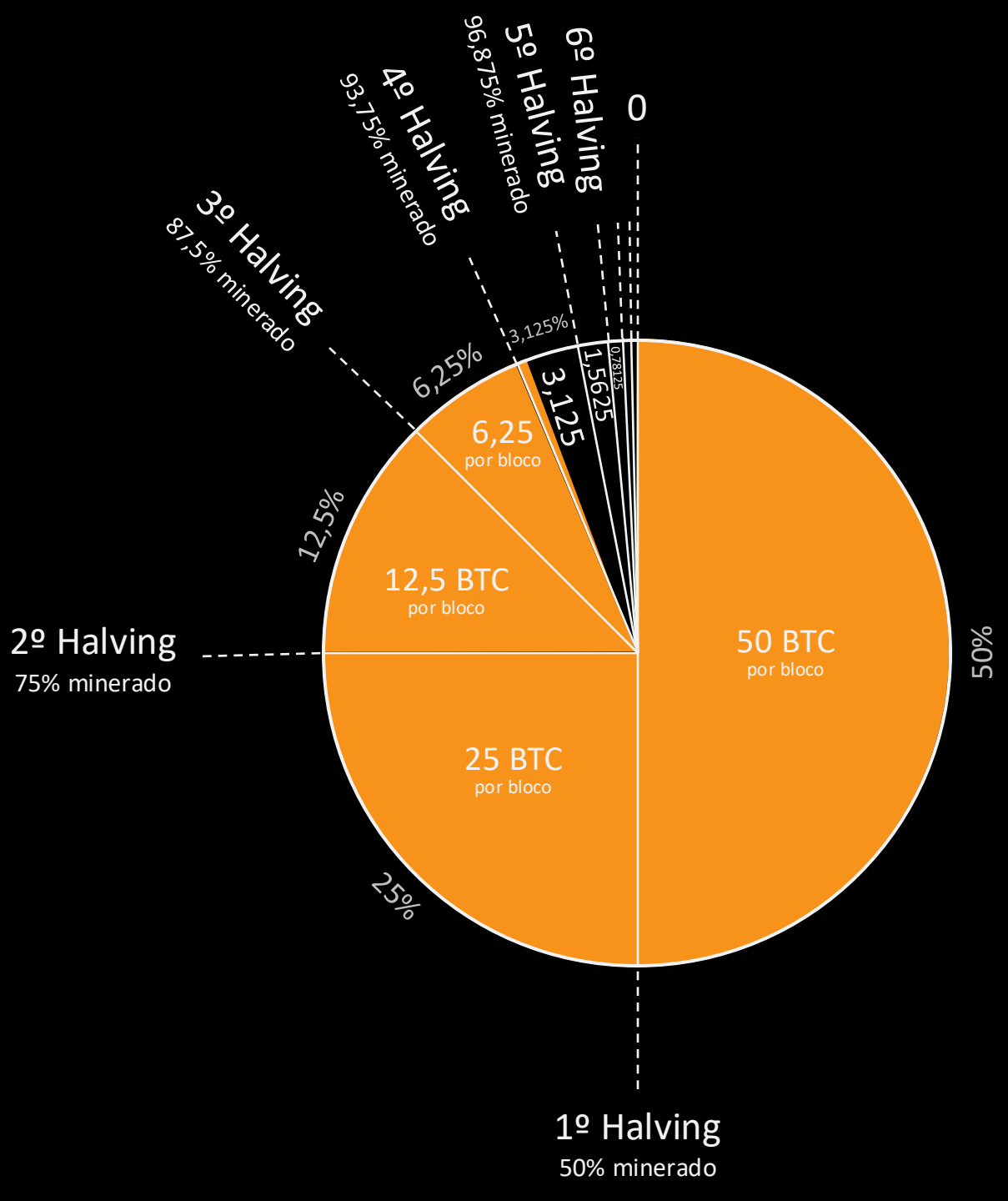
Como incentivo a despender a energia necessária à produção de um bloco, é dado a quem o produz o privilégio de incluir uma transação especial que atribui novos bitcoins.

É assim que novas moedas são criadas.

Recompensa de bloco

Esta recompensa reduz para metade a cada 210 000 blocos (~4 anos), um acontecimento conhecido como *halving*.

Este valor começou por ser 50 bitcoins por bloco.


6º Halving
0
5º Halving
96,875% minerado
4º Halving
93,75% minerado
3º Halving
87,5% minerado
3,125%
6,25%
12,5%
50%
25%
0,78125
1,5625
3,125
6,25
por bloco
12,5 BTC
por bloco
50 BTC
por bloco
25 BTC
por bloco
2º Halving
75% minerado
1º Halving
50% minerado

número total de "halvings" que irão ocorrer

número de novos bitcoins criados por bloco

$$\sum_{i=0}^{32} 210\,000 \left\lfloor \frac{50}{2^i} \right\rfloor$$

número de blocos entre halvings

número de halvings até ao momento

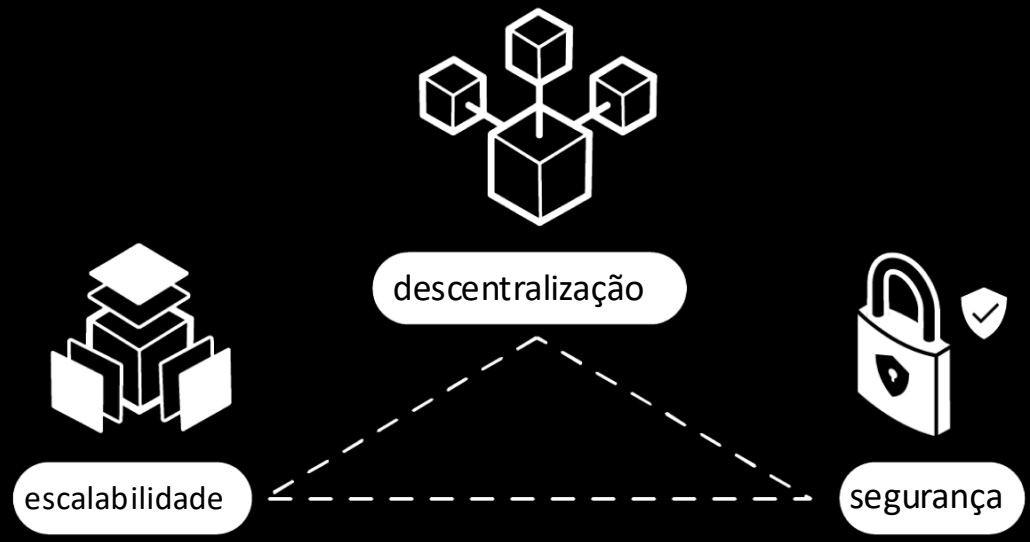
21M

(na verdade, 20 999 999.99755528)

Trilema

Ter estas três propriedades em simultâneo é um problema sem solução.

Sendo necessário sacrificar uma delas, a escolha recai sobre a escalabilidade, que pode ser resolvida em segundas camadas, em cima da rede base (*on-chain*).

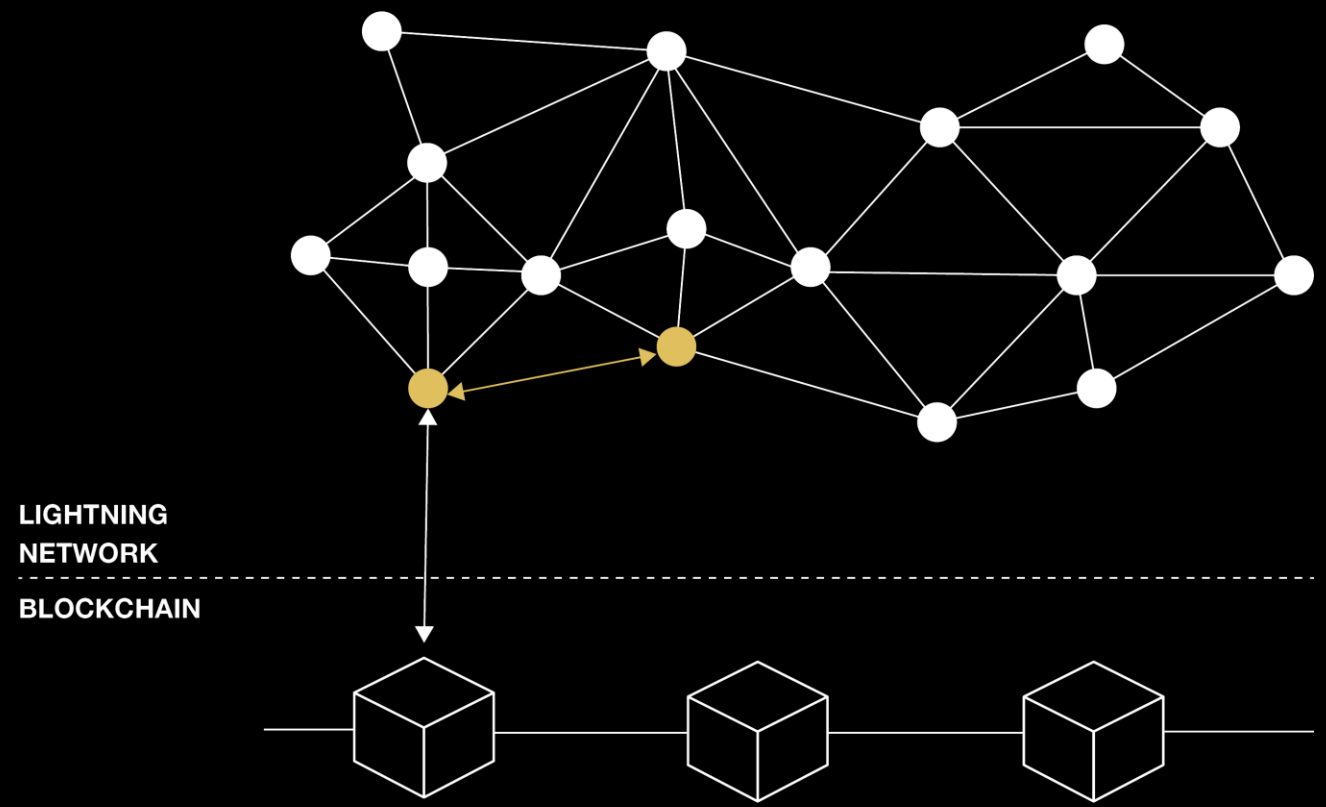


Lightning Network

A Lightning Network é uma rede ponto-a-ponto construída em cima da rede base de Bitcoin que permite fazer transações rápidas e baratas *off-chain*. Isto permite resolver o problema da escalabilidade.

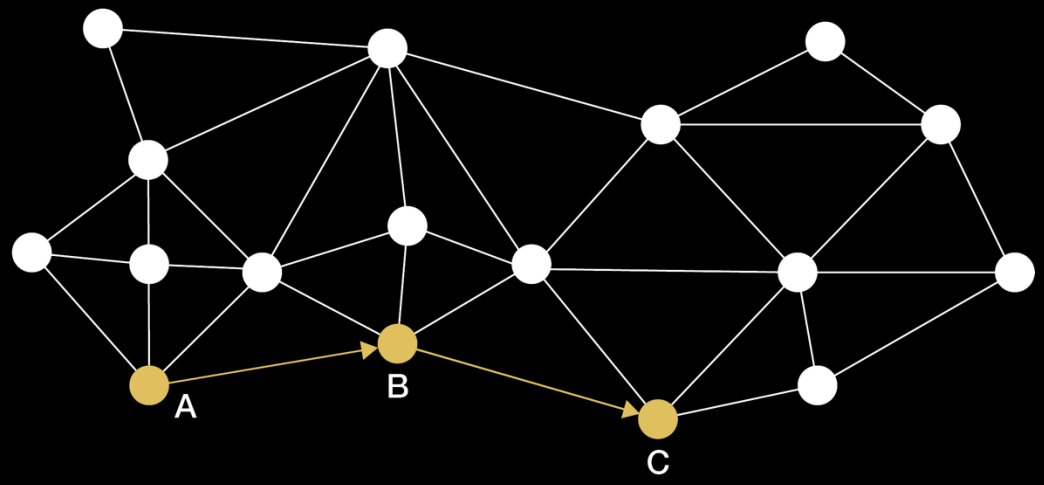
Lightning Network

Dois utilizadores podem abrir um canal entre si, permitindo enviar bitcoin de um para o outro instantaneamente.



Lightning Network

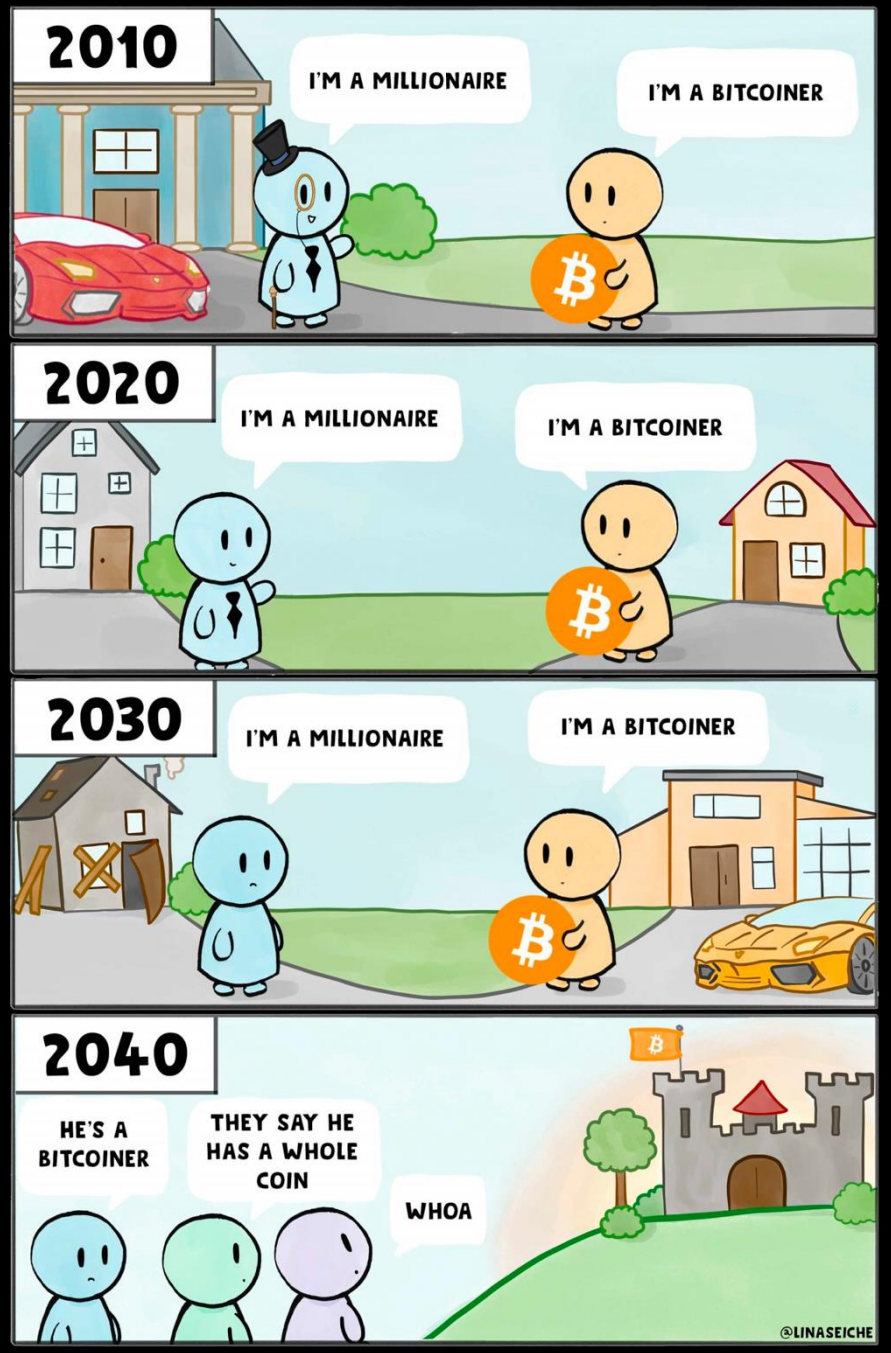
Se dois utilizadores não tiverem um canal, a rede encontra um caminho usando os canais existentes para rotear o pagamento.



Conclusão

	Bitcoin	Ouro	Fiat
Duradouro	B	A+	C
Portátil	A+	D	B
Fungível	B	A	B
Verificável	A+	B	B
Divisível	A+	C	B
Escasso	A+	A	F
Historicamente reconhecido	D	A+	C
Resistente à censura	A	C	D

THE LITTLE HODLER



Conteúdo:

Henrique Albuquerque (@liberspace)

Inês Louro (npub1yaz...8qwyhh3p)

Imagens:

Anil (@anilsaidso)

Grant Sanderson (@3blue1brown)

Yan Pritzker (@skwp__)

Lina Seiche (@linaseiche)


FÓRUM REGIONAL EDUCAÇÃO ECONÓMICA
FREE
MADEIRA