

BLOCKCHAIN & GAMES

Mark Joselli
PUCPR
mark.joselli@pucpr.br

MARK JOSELLI

- Professor da PUC-PR e do Apple Developer Academy;
- Consultor pela Mark Joselli Consulting;
- Doutor e mestre em computação;
- Apple Distinguished Educator;
- Criador da primeira especialização em Blockchain do Brasil;
- Escrevendo uma série de livros sobre Blockchain pela editora Casa do Código;

OBJETIVOS

- Compreender a tecnologia
- Introduzir como é o desenvolvimento
- Introduzir como pode ser integrado em um game

MOTIVAÇÕES

- Nova tecnologia
- Não tem muitas aplicações (principalmente em games).

AGENDA

- Valor do dinheiro
- Bitcoin
- Mineração
- Vantagens e desvantagens do blockchain
- Smart Contracts e a rede Ethereum
- Criação de Games usando o Blockchain

O QUE É DINHEIRO?

- Física ou Tokens eletrônico ou Commodities que pode ser ter as seguintes propriedades:
- Unidade de conta à valor definido
- Meio de troca à aceitabilidade
- Reserva de valor à não perecível



O QUE É DINHEIRO ELETRÔNICO?



- Tokens transaccionado somente eletronicamente
- Exemplos: Facebook Gold, Digital Gold Currency, bitcoin, e outras moedas electrônicas
- Autorização de Pagamento Eletrônico à Cartões de crédito.

MOEDA

"pode ser definida como um bem que possui aceitação geral na sociedade e que seja utilizada como forma de pagamento nas transações de compra e venda."

FUNÇÕES DA MOEDA

- unidade de conta;
- intermediária de trocas;
- reserva de valor.

TIPOS DE MOEDA

- MOEDA FIDUCIÁRIA: é baseada apenas na confiança da sociedade, portanto, não tem lastro monetário e de metais.
- MOEDA LASTREADA: é baseada na fixação de um lastro em outras moedas ou metais.
- MOEDA BANCÁRIA: é criada através dos empréstimos da moeda depositada nos depósitos á vista nos bancos comerciais.

COMEÇO DO DINHEIRO

- Tokens intermediárias trocas
 - Mercadorias ou objetos de valor percebido
 - moedas cunhadas à unidades padronizadas de metais
- Código de Hammurabi: o pagamento da dívida legal
- Contas à certificado de crédito para a produção



PRIMÓRDIOS DO DINHEIRO MODERNO

- Notas de banco privado
- Empréstimos com base em depósitos na conta
- Início da Reserva fracionadas
- moedas nacionais
- de Bancos Centrais Reserva –apoiado por ouro ou prata

COMEÇO DO DINHEIRO MODERNO

- I Guerra Mundial & Fim do padrão do ouro
 - A escassez das reservas de ouro com a Ampliação da Circulação
 - Notas não são mais reembolsável para ouro
- Dinheiro por Decreto do Governo
 - Apoiado por emissores com capacidade para pagar dívidas
 - Suscetíveis a desconfiança pública
 - possível ter inflação descontrolada ou deflação

TIPOS DE MOEDA

- Moeda privada -> livre de bancos
- Moeda Comunitaria -> aceitabilidade local
- Moeda do mundo -> referência para comércio
- Moeda forte -> não-reversível
- Moeda macia -> permite disputas de pagamento

MOEDA PRIVADA

- Livre de bancos = sem Banco Central de Reserva
- Entrada gratuita para Indústria Bancária
- Liberdade de emissão de notas, aceitar depósitos e Coleta cheques para pagamento
- Liberdade de pedir dinheiro emprestado em Depósito a Prazo
- Liberdade para emprestar Ativos, Dinheiro e Investimentos.

MOEDA COMUNITÁRIA

- HORAS Ithaca

- Ithaca, NY



- Berkshares

- Berkshire, MS



- Dólar Toronto

- Toronto, Ontario



MOEDA DO MUNDO

- Referência de comercio global
 - Ouro, libra esterlina, dólar americano, Euro, Yen
- Fundo Monetário Internacional (FMI)
 - Direitos Especiais de Saque (SDR)
 - Ativos reserva suplementar



Open Source Peer-to-Peer Money

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA

The Economist

OCTOBER 31ST-NOVEMBER 6TH 2015

Economist.com

007 and the spectre of Britain's past

Turkey votes to the sound of bombs

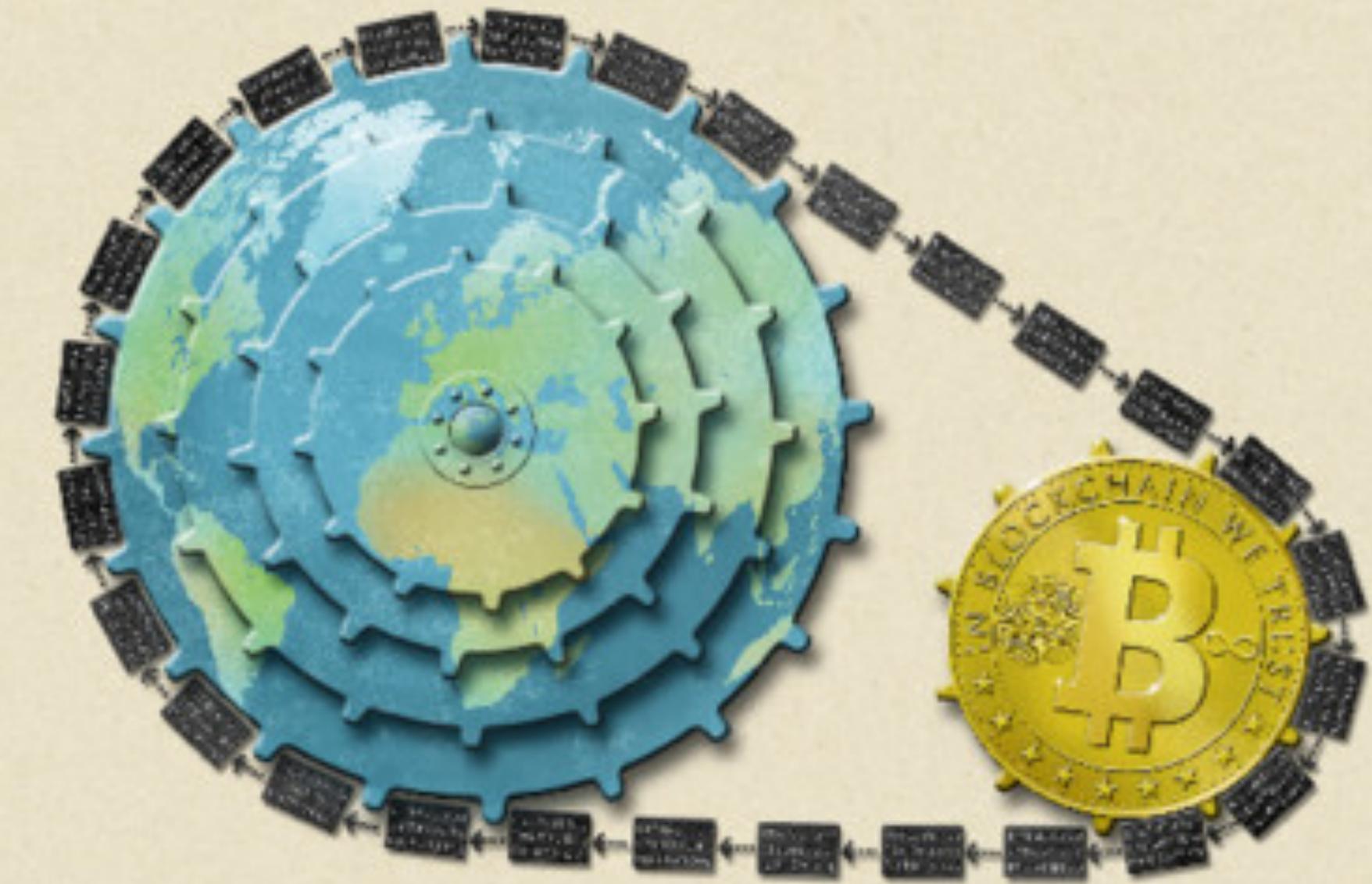
Those ever-creative accountants

America takes the fight to IS

Coywolves: the new superpredator

The trust machine

How the technology behind bitcoin
could change the world



CRISE DE 2008

- Começou em 2007 com uma crise no mercado de hipotecas subprime (segunda classe);
- O excesso de riscos assumidos pelos bancos ajudou a ampliar o impacto financeiro globalmente;
- Os bancos perderam o dinheiro do povo (depósitos).
- Socorros massivos de instituições financeiras pelo governo com dinheiro do povo (impostos).



BITCOIN - CRIAÇÃO

- 31/10/2008, publicação do paper de Satoshi Nakamoto entitulado Bitcoin: A Peer-to-Peer Electronic Cash System na cryptography mailing list.
- 03/01/2009, primeira blockchain foi criada por Satoshi Nakamoto com a mineração do bloco genesis com o texto:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

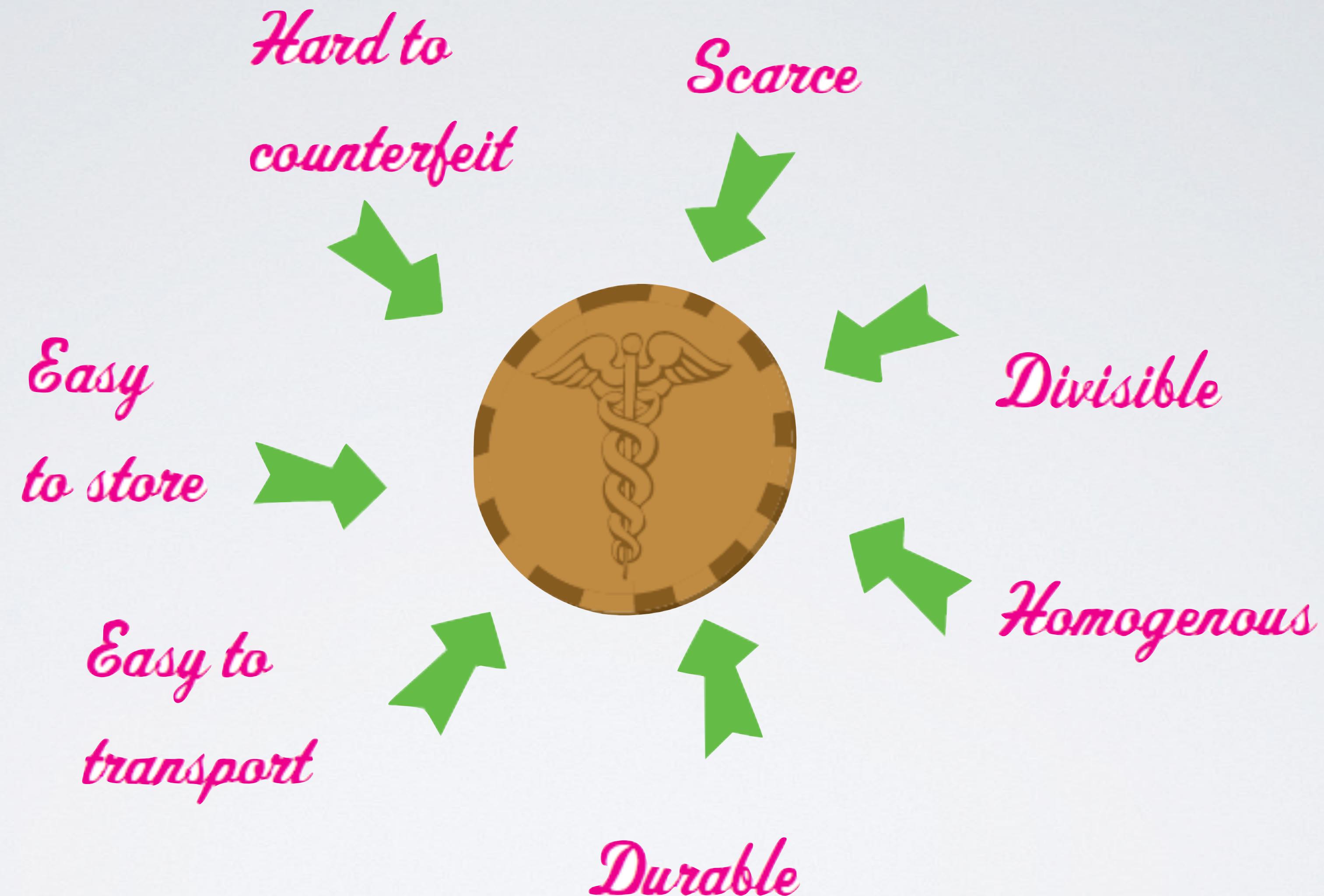
BITCOIN



- É simplesmente um meio de envio e recebimento de números para e de "endereços"
- Uma rede Open-Source Peer-to-Peer de pagamento
- Usando assinaturas digitais e Encriptação
 - descentralização é a base para a segurança e a liberdade de Bitcoin
- <https://www.youtube.com/watch?v=IWQYLvbGFC0>

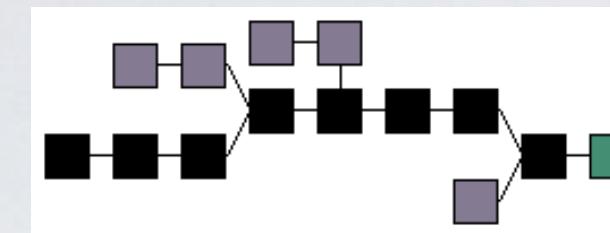
MOTIVAÇÃO BITCOIN

“Pela primeira vez na história do mundo, qualquer um pode agora enviar ou receber qualquer quantia de dinheiro com qualquer outra pessoa, em qualquer lugar, instantaneamente, basicamente, de graça, e é impossível para qualquer um, incluindo os governos, para impedi-los.”

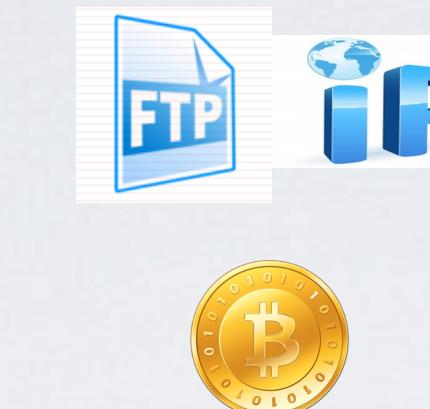


DINHEIRO BOM

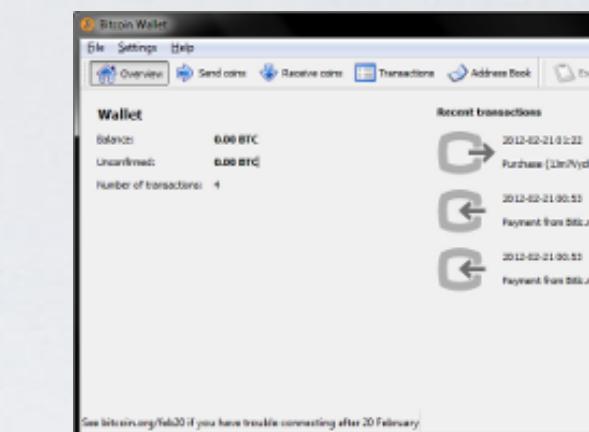
Blockchain



Protocol



Client



- rede aberta e descentralizada
- código aberto
- protocolo transparente
- registro público de todas as transações

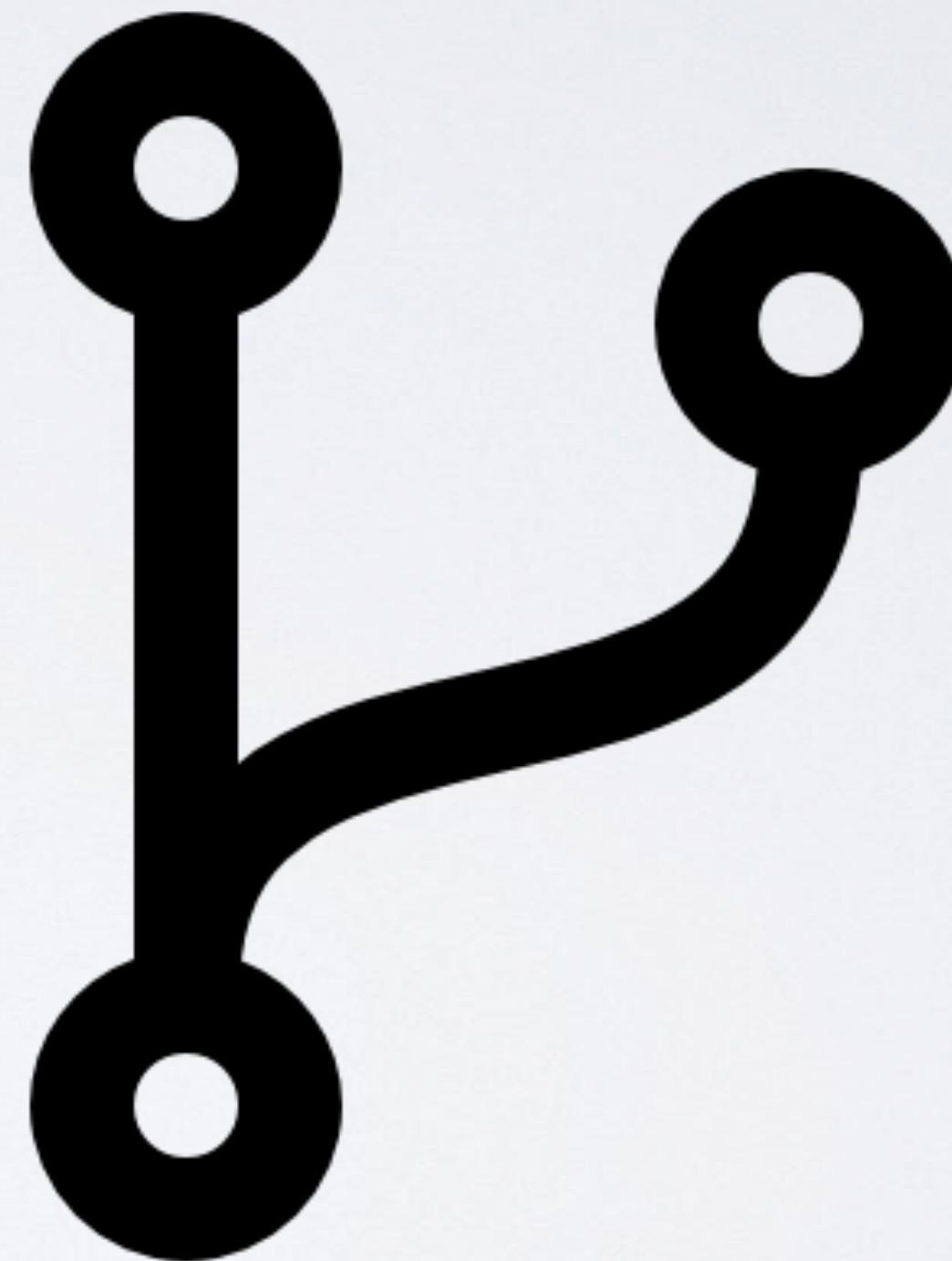
BITCOIN - GOVERNANÇA

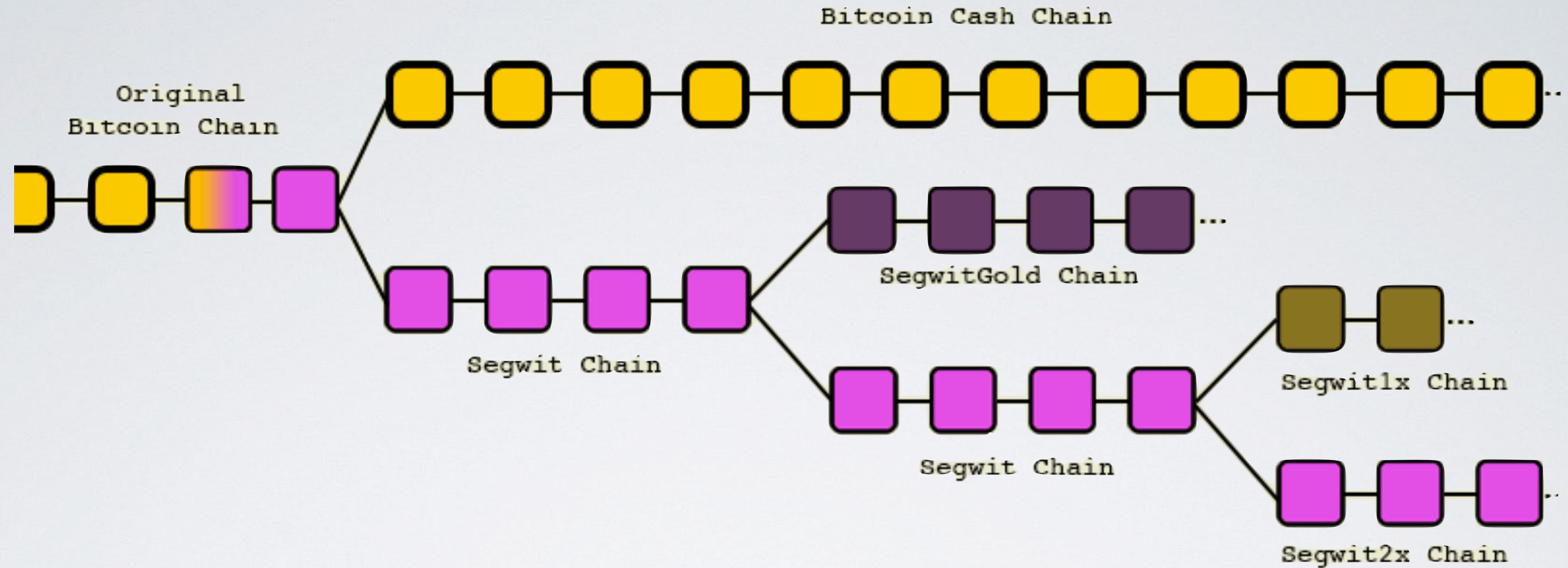
- uma comunidade de código aberto de empreendedores apoiados pela Fundação Bitcoin



BITCOIN - DEMOCRÁTICO

- Se alguém não gosta de uma das mudanças,
- Ele pode fazer um fork e implementar suas próprias regras.

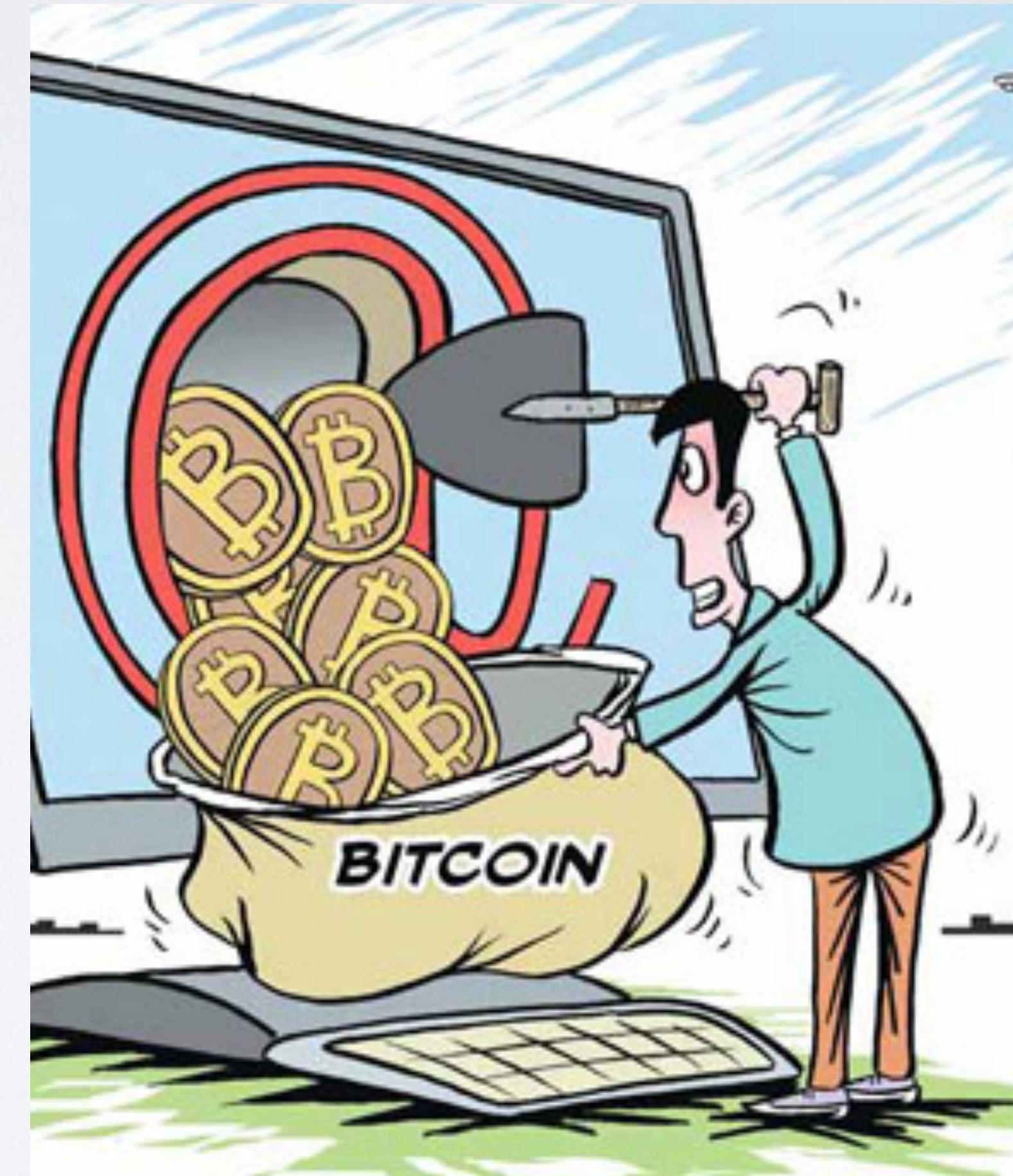




BITCOIN FORKS

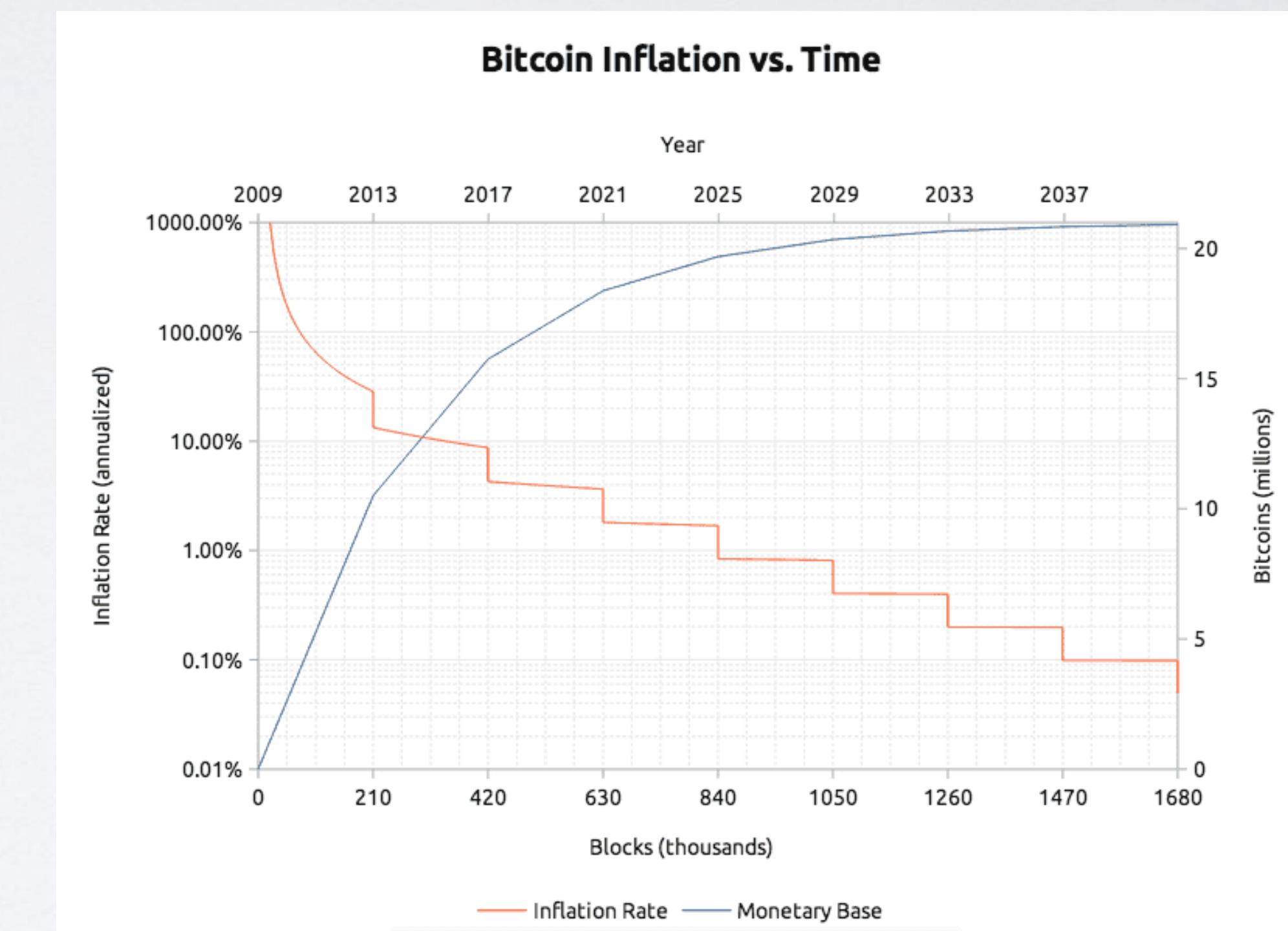
BITCOIN - CRIAÇÃO

- O bitcoin foi criado para ser dado para as pessoas, não para os bancos;
- Mas atualmente está concentrado na mão de mineradores.



BITCOIN - DEFLACIONÁRIO

- Deflacionário por design - oferta de dinheiro não pode ser manipulado
- fixada em 21 milhões de moedas, cada uma divisível até 8 decimal



BITCOIN - WIKIPEDIA

- Bitcoin é uma criptomoeda descentralizada, constituindo um sistema econômico alternativo (peer-to-peer electronic cash system).
- É considerada a primeira moeda digital mundial descentralizada, e responsável pelo ressurgimento do sistema bancário livre.
- O Bitcoin permite transações financeiras sem intermediários, mas verificadas por todos usuários (nós) da rede,
 - que são gravadas em um banco de dados distribuídos, chamado de blockchain.

BITCOIN - WIKIPEDIA 2

- A rede descentralizada ou sistema econômico alternativo Bitcoin possui a topologia ponto-a-ponto (peer-to-peer ou P2P)
 - isto é, uma estrutura sem uma entidade administradora central,
 - o que torna inviável qualquer autoridade financeira ou governamental manipular a emissão e o valor de bitcoins ou induzir a inflação com a produção de mais dinheiro.
 - o valor da criptomoeda não deriva de moedas fiduciárias ou outros bens, isto é, não é lastreado por nenhum ativo; Bitcoin é a mercadoria, é o ativo em si sem precedentes.

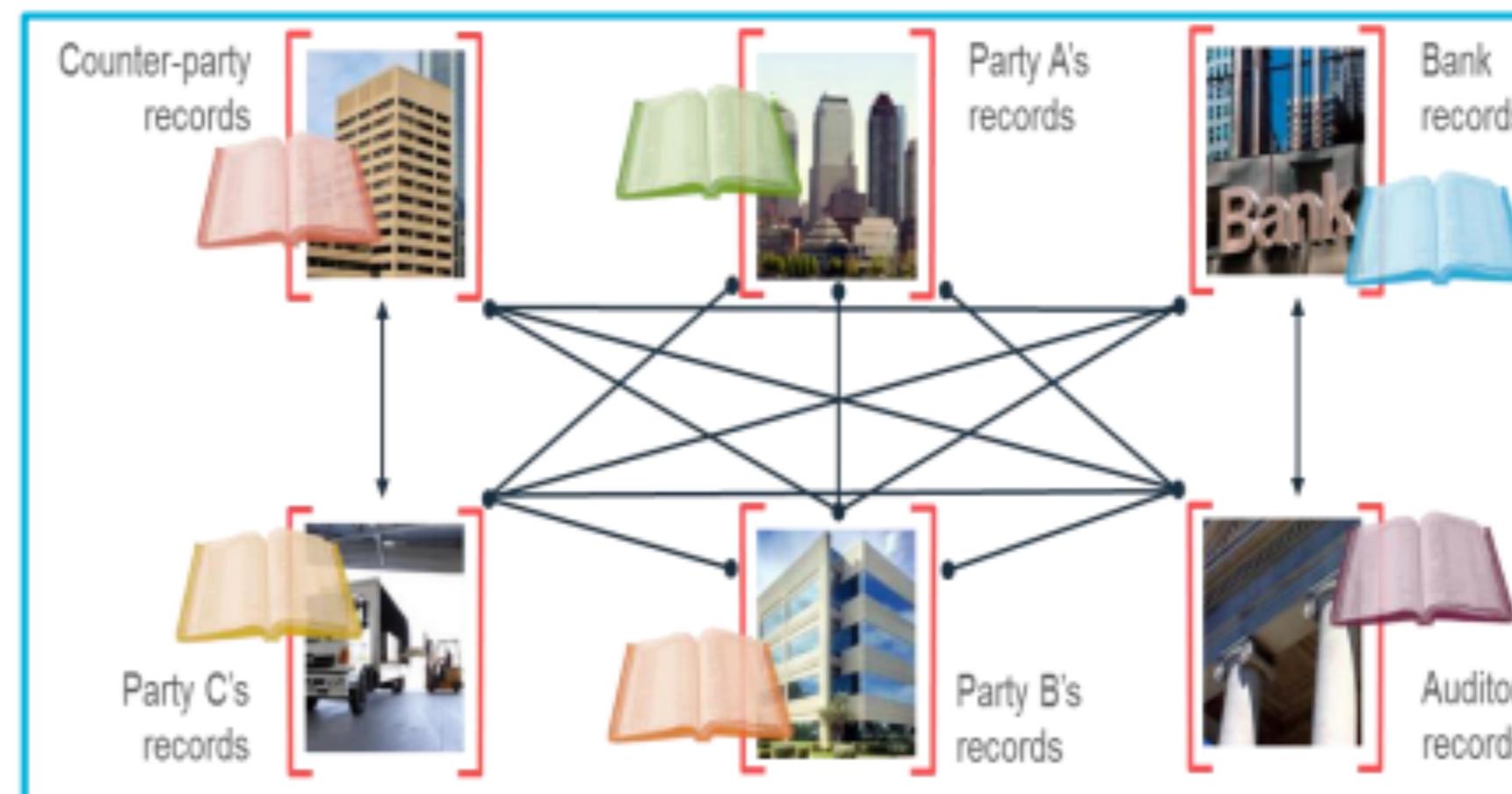
DINHEIRO X BITCOIN

- O dinheiro no passado gostaria de ser ouro;
- O dinheiro hoje em dia tem mais valor do que o ouro, já que é mais aceito.
- Qualquer tipo de dinheiro tem seu valor baseado no garantia que eles podem trocá-lo por último.

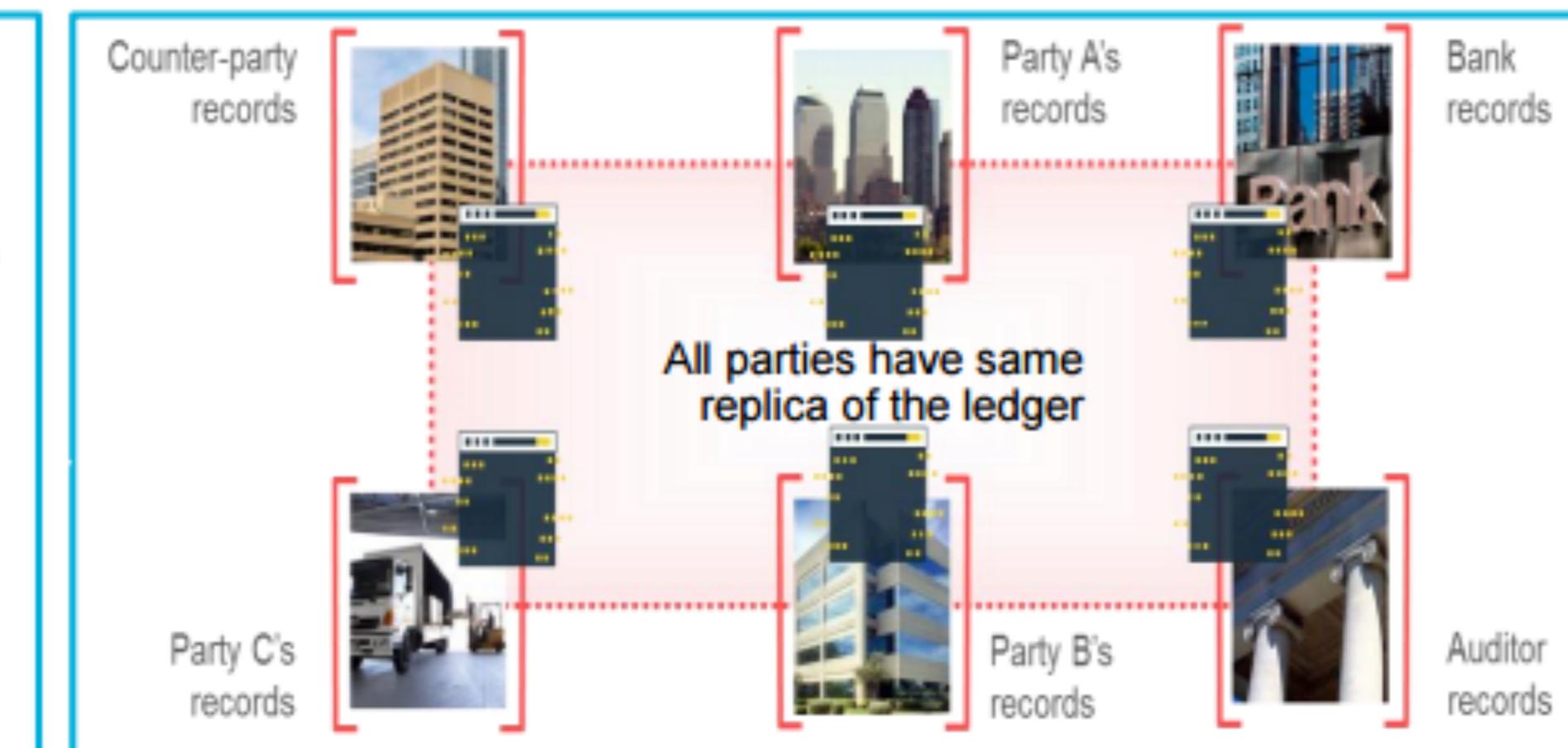
What's the difference with Blockchain?

What?

Without Blockchain



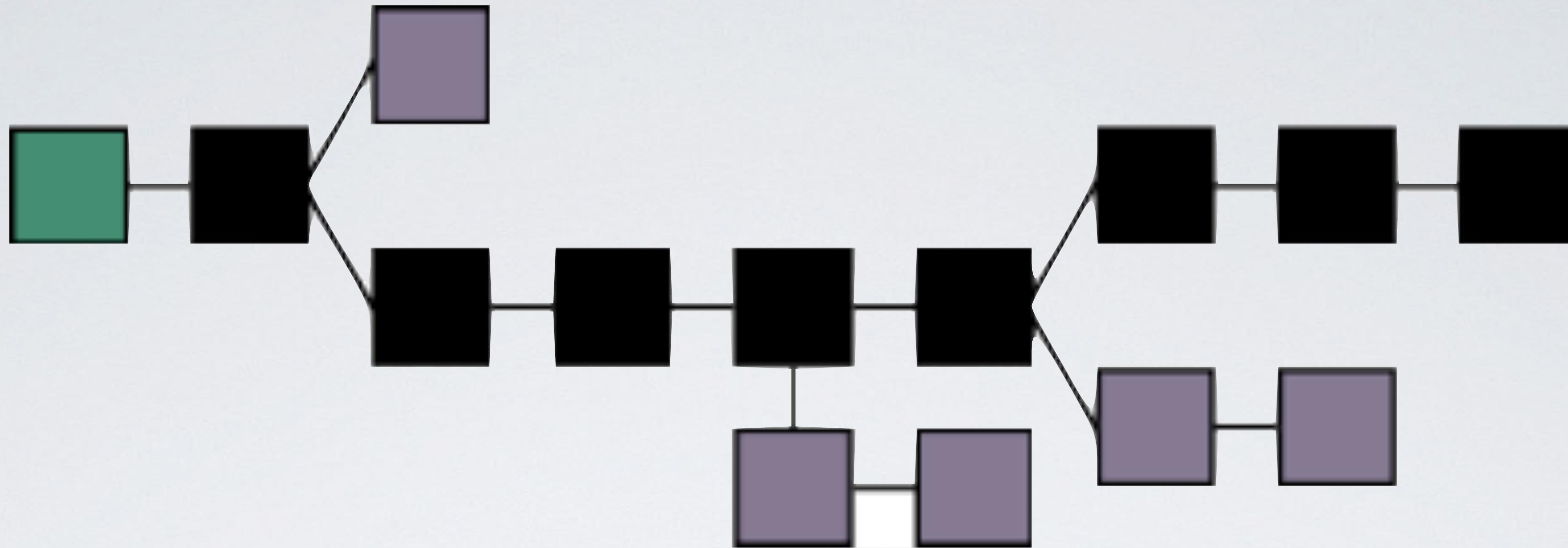
With Blockchain



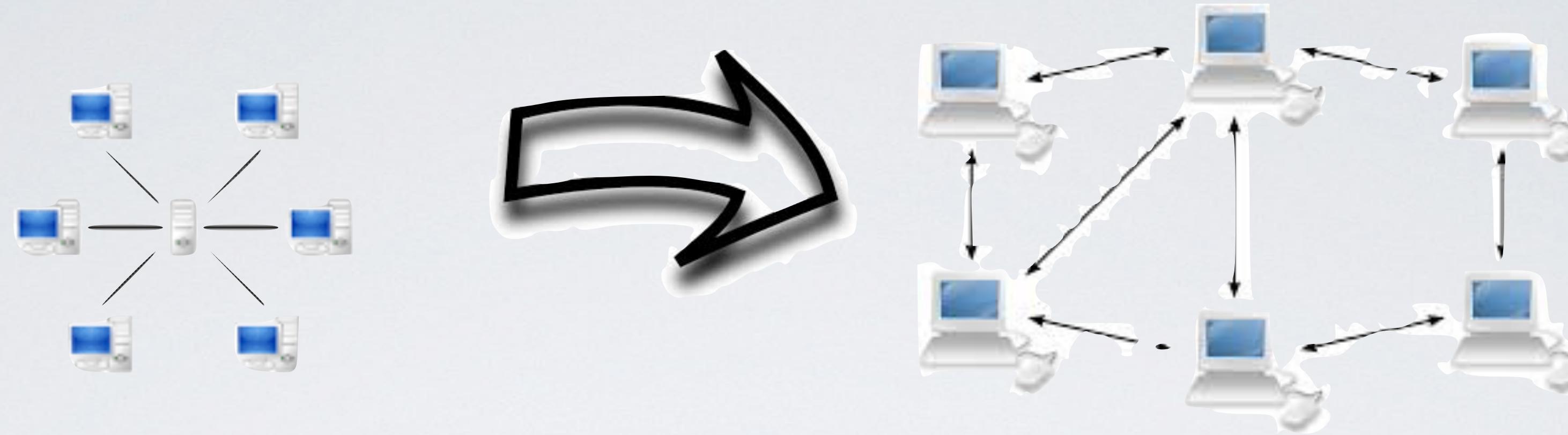
Inefficient, expensive, vulnerable

Consensus, provenance, immutability, finality

outthink your limits



- Um blockchain é um banco de dados não repudiável, com registro de data e hora, que contém todo o histórico registrado de transações no sistema.
- Cada processador de transação no sistema mantém sua própria cópia local desse banco de dados e os algoritmos de formação de consenso permitem que cada cópia permaneça em sincronia.



- As redes blockchain são redes peer-to-peer.
- As redes blockchain abertas são sem permissão
 - qualquer cliente pode sincronizar com a rede e começar a participar.

COMO FUNCIONA?

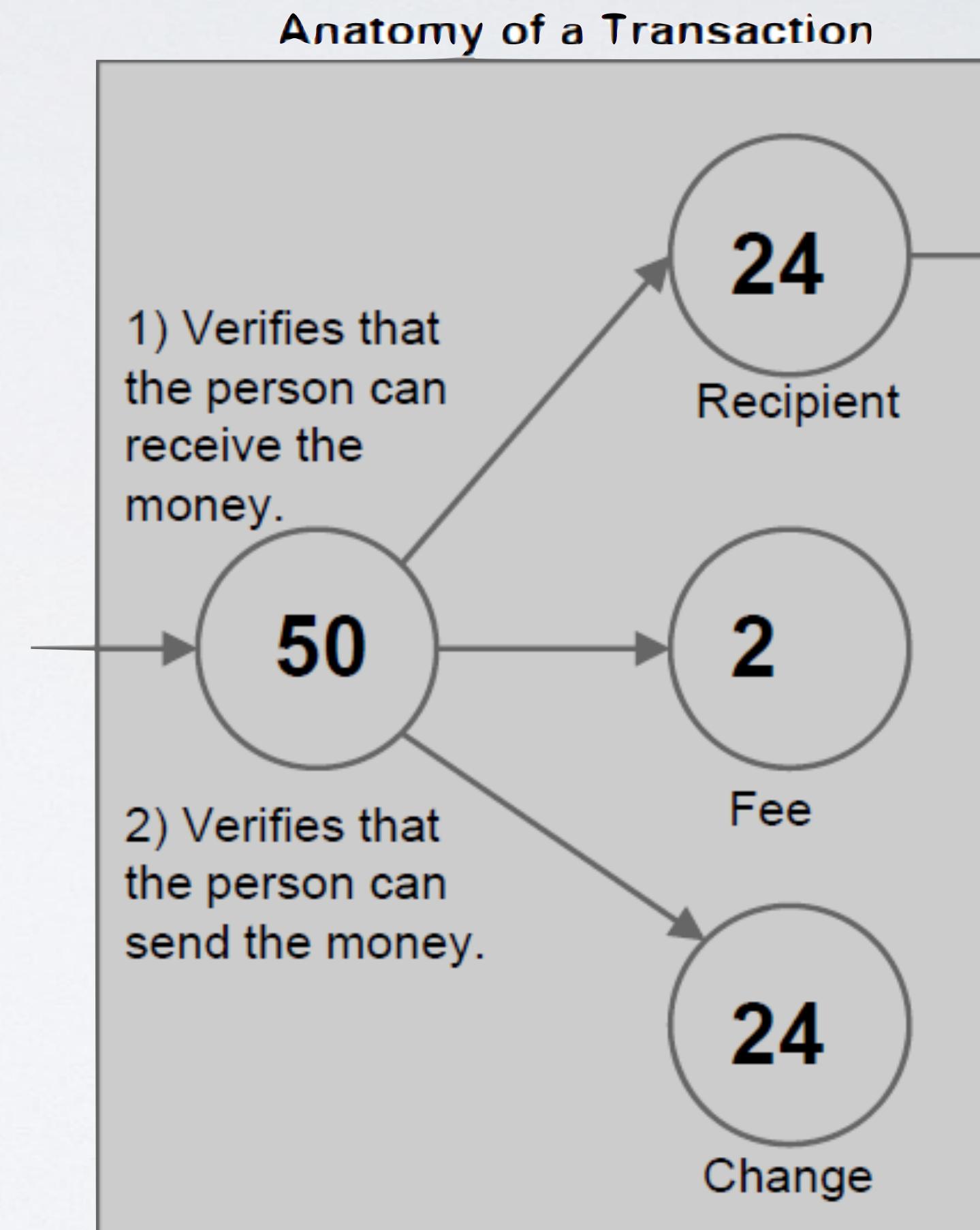
- A cadeia do bloco (block chain) é a estrutura de dados fundamental do protocolo Bitcoin.
- É uma única estrutura de dados onde participantes passam de um para o outro.
- Isso lhes permite saber quem possui o quê.
- Qualquer um pode alterá-lo para enviar dinheiro para alguém.
- Outros usuários matematicamente verificam a transação para garantir a sua validade.

- É essencialmente um livro de contabilidade:
 1. 3/3/13 Mark encontrado: \$ 15.00 (mineração)
 2. 3/3/13 Mark -> Esteban: \$ 10,00
 3. 3/4/13 Bruno -> Mark: \$ 4,00
- Quanto dinheiro é que Mark tem em sua carteira?
- Mark tinha \$15, em seguida, deu \$10 ao Esteban, em seguida, recebeu \$4 de Bruno, ficando com \$9,00 no final

TRANSAÇÕES

A entrada contém:

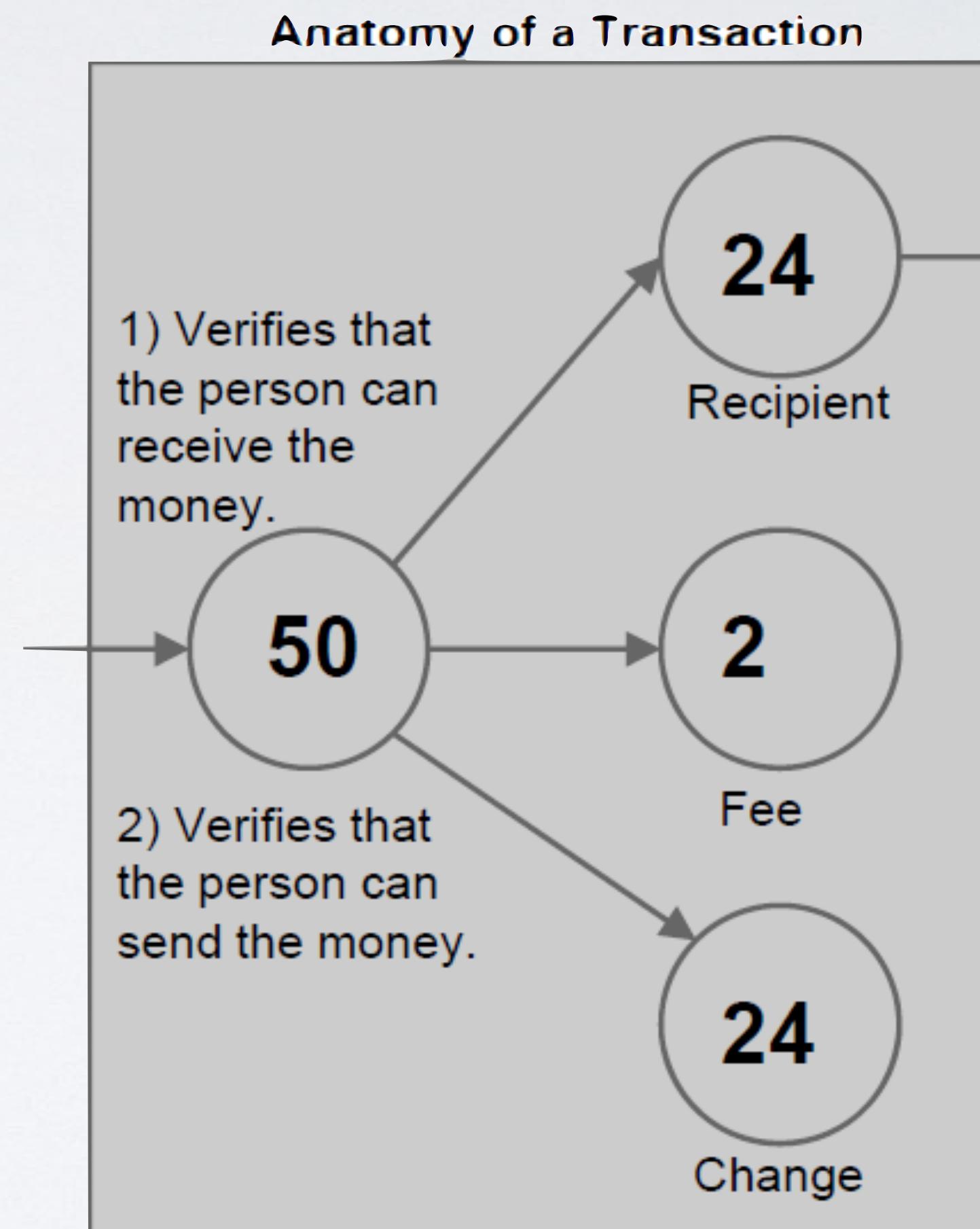
- 1) A chave pública que pertence à redentor da transação de saída.
- 2) Um ECDSA hash ao longo de um endereço calculado da transacção.



TRANSACTIONS

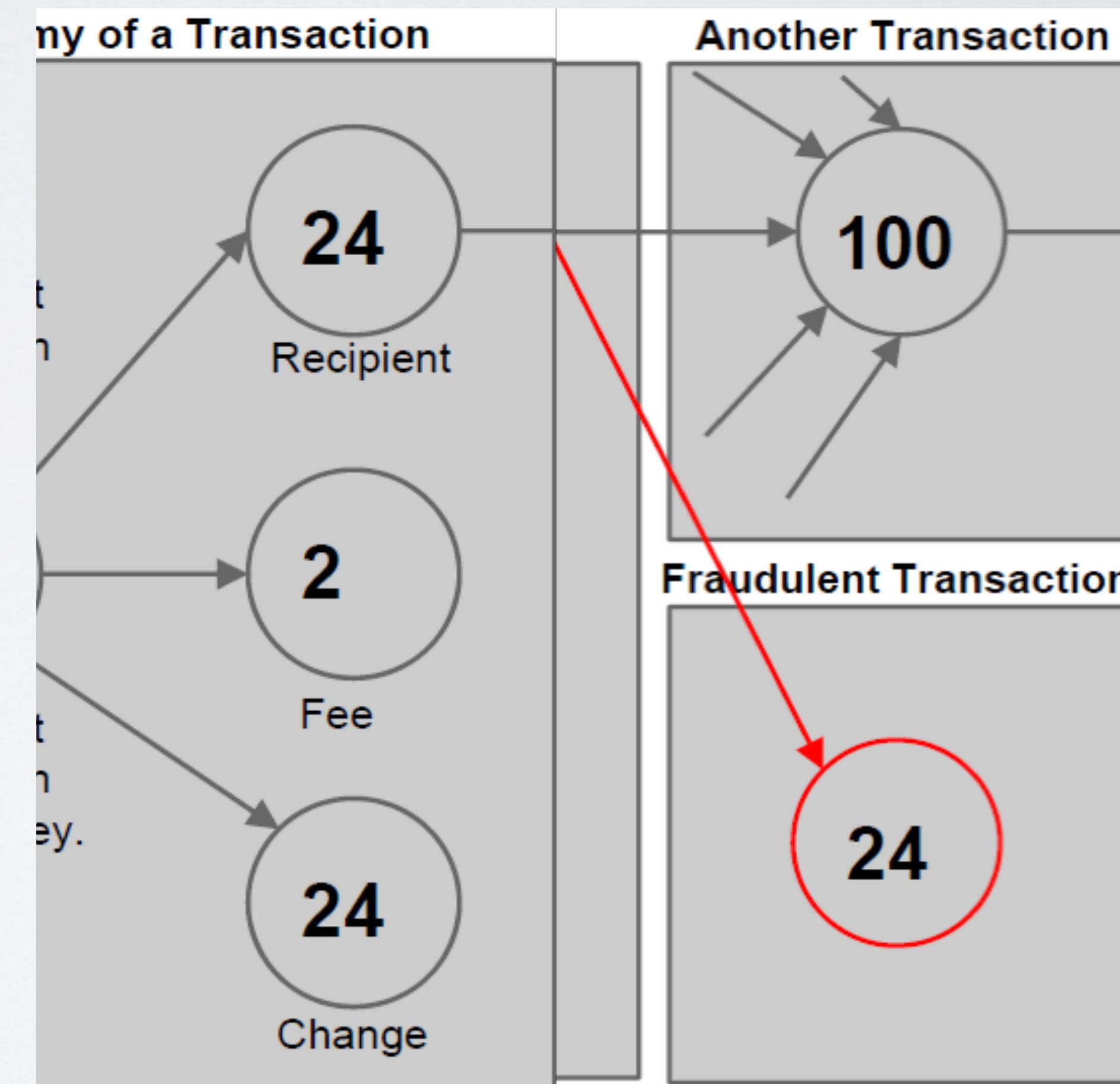
Saída contém:

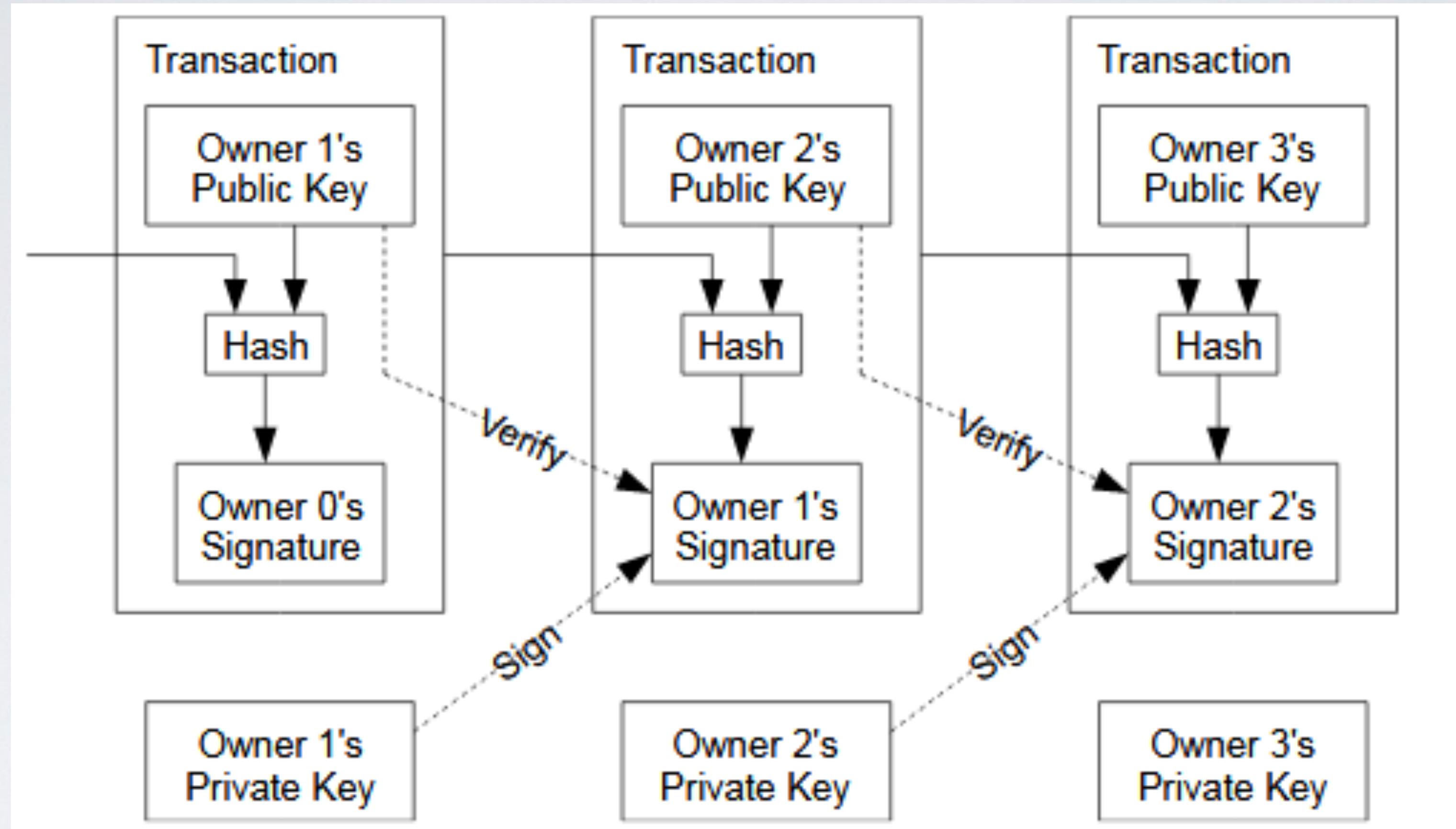
- 1) A quantidade a ser enviada para o destinatário.
- 2) A quantidade que está sendo enviado de volta para o remetente original (se houver)
- 3) A taxa de transação ligado à saída (se houver).



TRANSACTIONS

- O blockchain impede o ataque de gastar o dobro,
- dando outros nós o poder de verificar se as entradas de transação não foram já gastas em outro lugar.





TRANSACTIONS IN ACTION

GASTO DUPLO

- O Bitcoin resolve o chamado "problema do gasto duplo" presente com produtos digitais.
- Por exemplo, se eu tenho um arquivo mp3 ou um e-book no meu computador, posso copiar esse arquivo milhares de vezes livremente e enviá-lo para milhares de pessoas diferentes.
- Para uma moeda digital, a possibilidade de cópia ilimitada significaria uma rápida morte hiperinflacionária.
- O Bitcoin resolve isso mantendo uma rede peer to peer e registrando cada transação em único chamado de blockchain.
- Se eu enviar 1 bitcoin do meu endereço de bitcoin para meu amigo João. A rede de bitcoins registra essa transação na cadeia de blocos e eu não tenho mais a posse desse bitcoin.
- A moeda "mudou" da minha carteira de bitcoins para a carteira de João



MINING

MINERAÇÃO

- Mineiros recolher as transações na rede em grandes blocos chamados blocks
- Ex: "Alice paga Karim 10 bitcoins" e "Liam paga Sofia 8,3 bitcoins".
- Estes blocos são amarrados juntos em um registro contínuo, autoritário chamado blockchain,
- que não permite quaisquer transações conflitantes.
- E permite que você saiba com certeza absoluta quais transações são confiáveis (Sem gastos duplos!).

HASH

- Para entender a mineração, é preciso entender o que é uma função hash.
- Simplificando, uma função hash recebe uma entrada e cria uma saída aparentemente aleatória,
 - mas a saída é consistente toda vez que você executa a função em uma determinada entrada,
 - e é muito difícil determinar uma entrada, considerando apenas a saída.

EXEMPLO HASHING (NÚMEROS ENTRE O 50 LUGAR E O 100)

- raiz quadrada do numero primo $3 =$
1.73205080756887729352744634150
- Raiz quadrada do número primo, digamos $11 =$
3.3166247903553998491149327366707
- Facilmente calculado, mas dificilmente encontrado somente com a saída

BLOCKCHAIN

- Bitcoin garante que só há uma cadeia de bloco, fazendo blocos realmente difícil de serem produzidos.
- Mineiros têm para calcular um hash criptográfico do bloco que satisfaça certos critérios
 - A dificuldade é um dos critérios para o hash que é ajustado com base na frequência blocos estão sendo criados
 - Também validam cuidadosamente todas as transações que entram em seus blocos
 - mineiros bem sucedidos são recompensados com alguns tokens.

PREVENÇÃO DE FRAUDE

- Os usuários podem confiar na blockchain que foi mais difícil de produzir
 - As cadeias mais longas vencem
- Se houvesse uma blockchain "fake" competindo com os reais o fraudador teria que fazer tanto trabalho quanto o resto da rede para fazer a sua cadeia de bloco parecer tão confiável
- O intenso trabalho necessário para encontrar blocos através de hashing protege a rede contra fraude

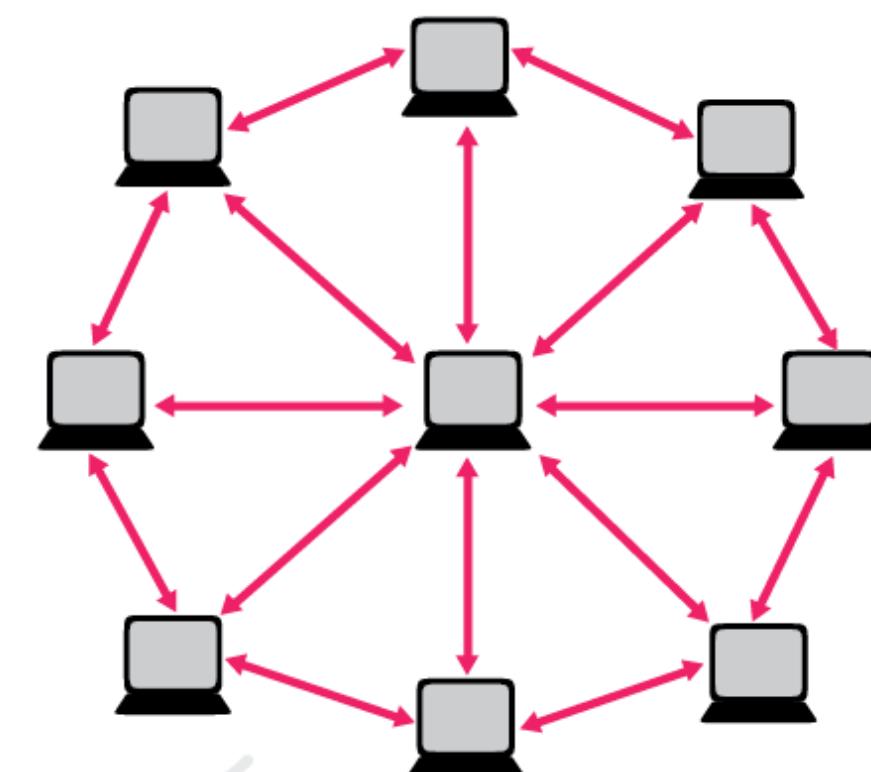


MINERAÇÃO DE BITCOIN

1. Recolhe transações da rede
2. Valida eles, e não permite transações conflitantes
3. Coloca eles em grandes blocos
4. Calcula hashes criptográficos até encontrar um hash "bom o suficiente para contar"
5. Em seguida, envia o bloco para a rede, adicionando-o à blockchain e ganhar uma recompensa em troca



Someone requests a transaction.



The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.

Validation

The network of nodes validates the transaction and the user's status using known algorithms.



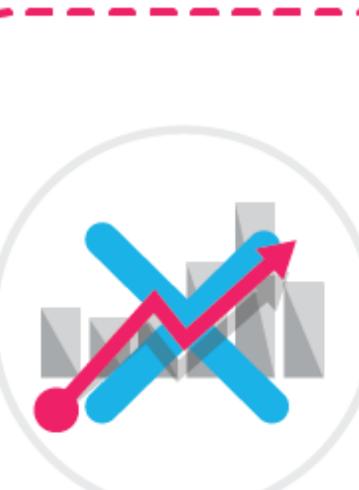
The transaction is complete.

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

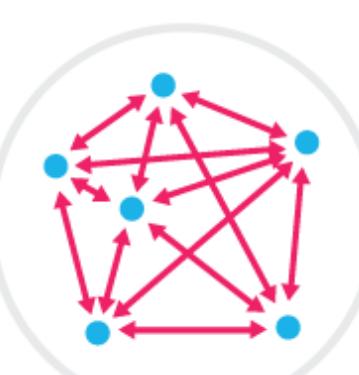
A verified transaction can involve **cryptocurrency**, contracts, records, or other information.

cryptocurrency

Has no intrinsic value in that is not redeemable for another commodity such as gold.



Has no physical form and exists only in the network.



Its supply is not determined by a central bank and the network is completely decentralized.

51% ATTACK

- Um invasor com > 50% de energia pode de hash
 - gastar o dobro: reverter transações que ele envia, enquanto ele está no controle
 - Impedir que algumas ou todas as transações de ganhar quaisquer confirmações
 - Impedir que alguns ou todos os outros geradores de obter quaisquer gerações
 - <https://www.crypto51.app/>

SUCESSOS DE 51% ATTACKS

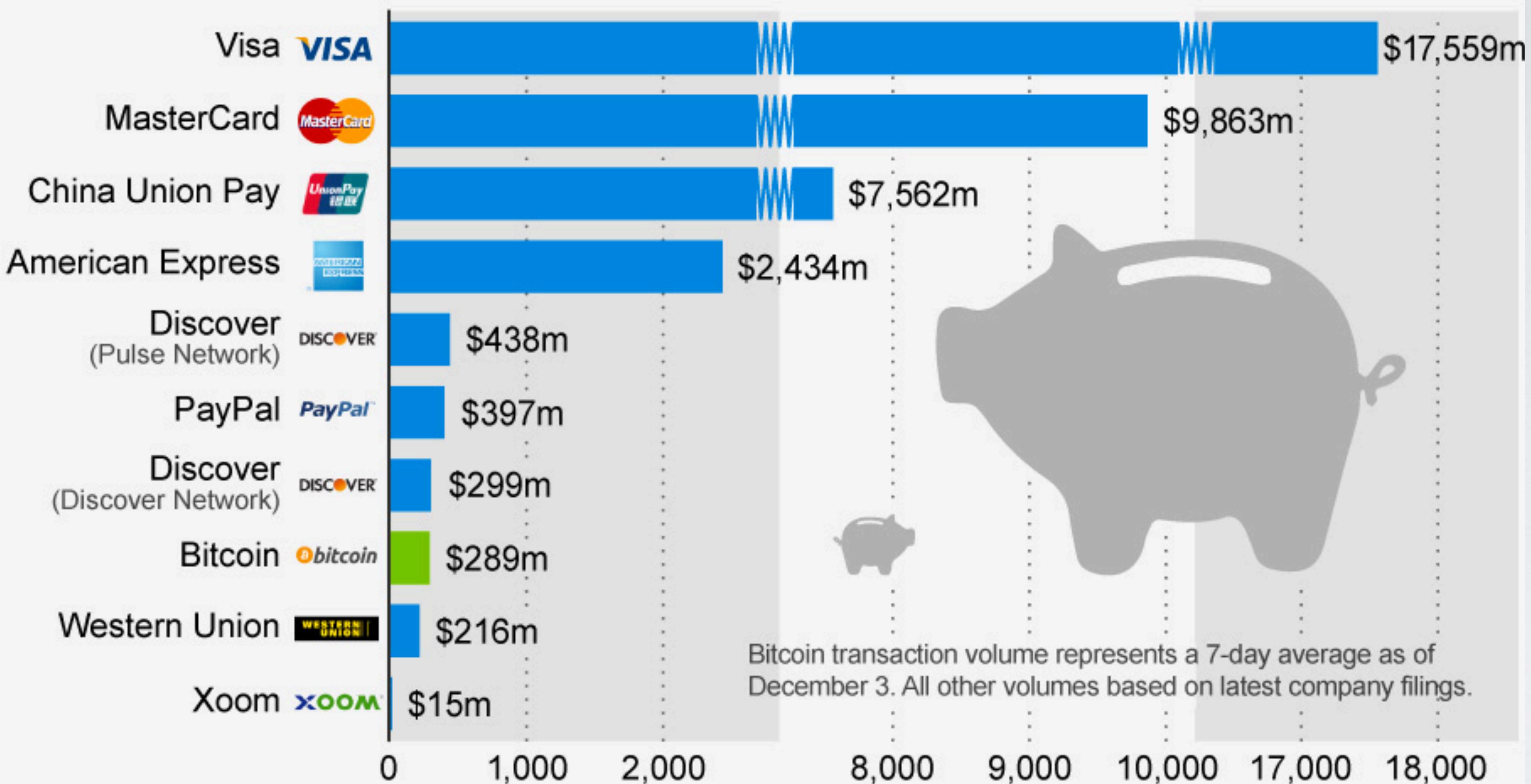
	Amount Stolen	Estimated Cost of 1Hr Attack
Bitcoin gold	1,860,000	3,936
Zencash	500,000	5,237
MonaCoin	90,000	3,729

PORQUE BITCOIN?

- Bitcoin pode ser usado para comprar mercadorias anonimamente (não mais)
- Bitcoin não está vinculado a nenhum país ou sujeito a regulamentação (mas tem manipulação do mercado)
- Vantagens para pequenas empresas porque no Bitcoin não há taxas de cartão de crédito ou estornos (mas tem fees)
- Algumas pessoas compram bitcoins como um investimento, esperando que elas aumentem seu valor. Esta é uma das razões para a instabilidade do preço

How Bitcoin Activity Stacks Up Against Other Payment Networks

Average daily transaction volume of selected payment networks (in million U.S. dollars)



PREOCUPAÇÕES COM O BITCOIN

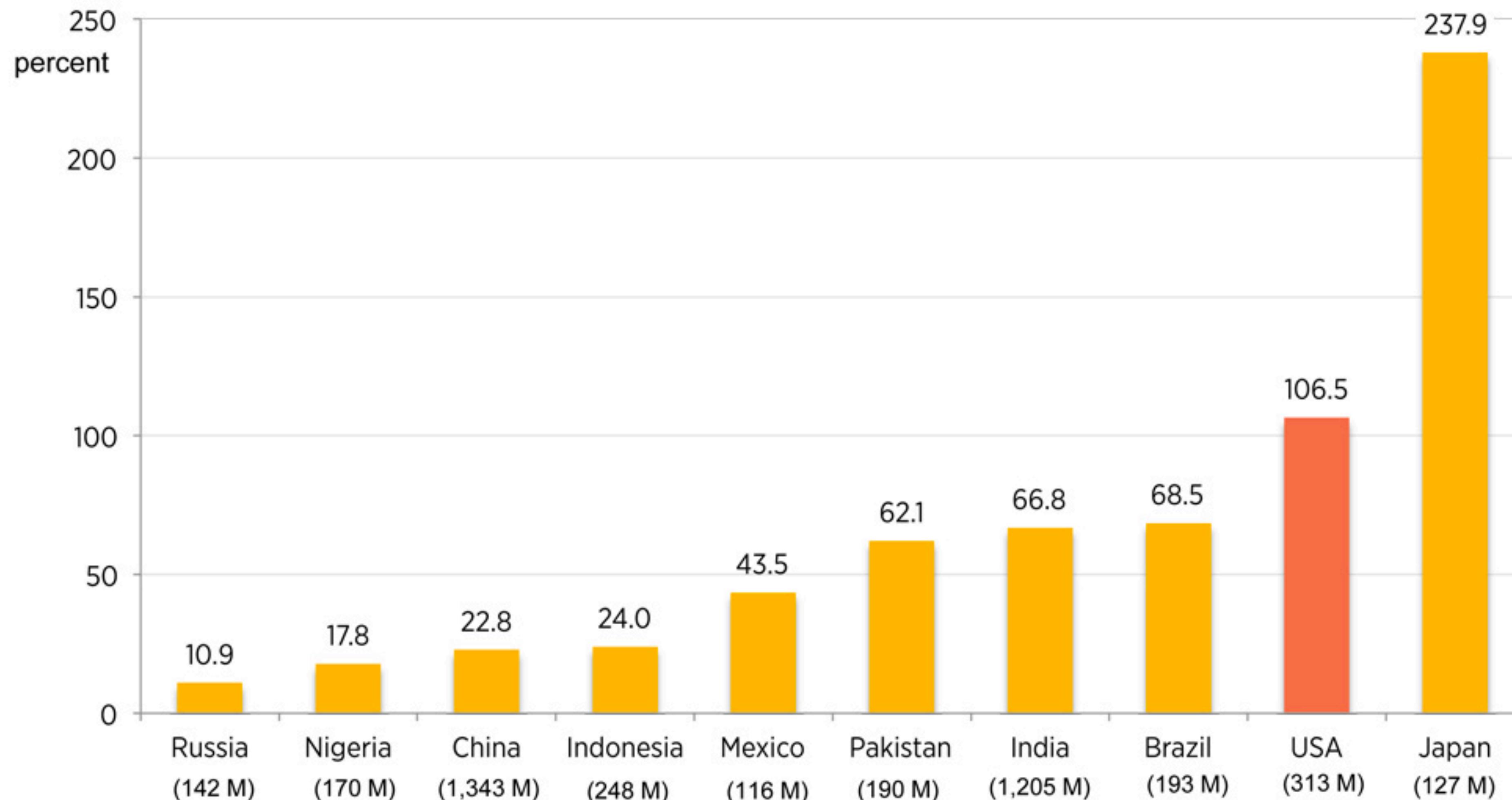
- Carteira vulneráveis a roubo e hacks
- Não é regulado (tentativa SEC)
- Bitcoins estão concentrados na mãos de poucos (manipulação do mercado);
- Consumo de energia
- Tulip Mania
- TPS (transactions-per-second) baixo

WHAT IS THE VALUE OF MONEY?





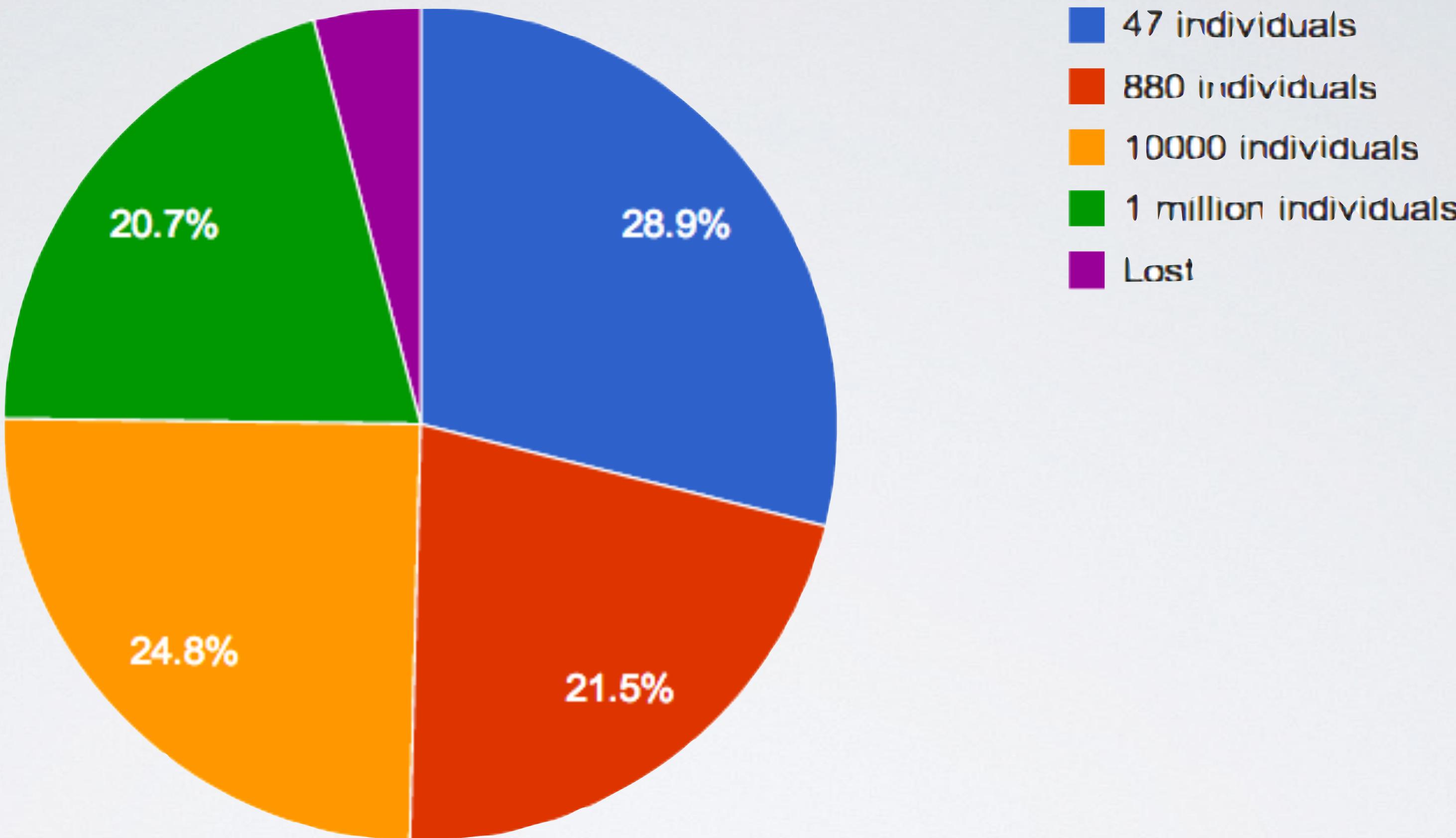
Debt-to-GDP of Most Populous Countries



Source: International Monetary Fund.

Data note: Data for Bangladesh (8th most populous country) unavailable.
Produced by Veronique de Rugy, Mercatus Center at George Mason University.

Slices Of The 12 Million Bitcoin Pie



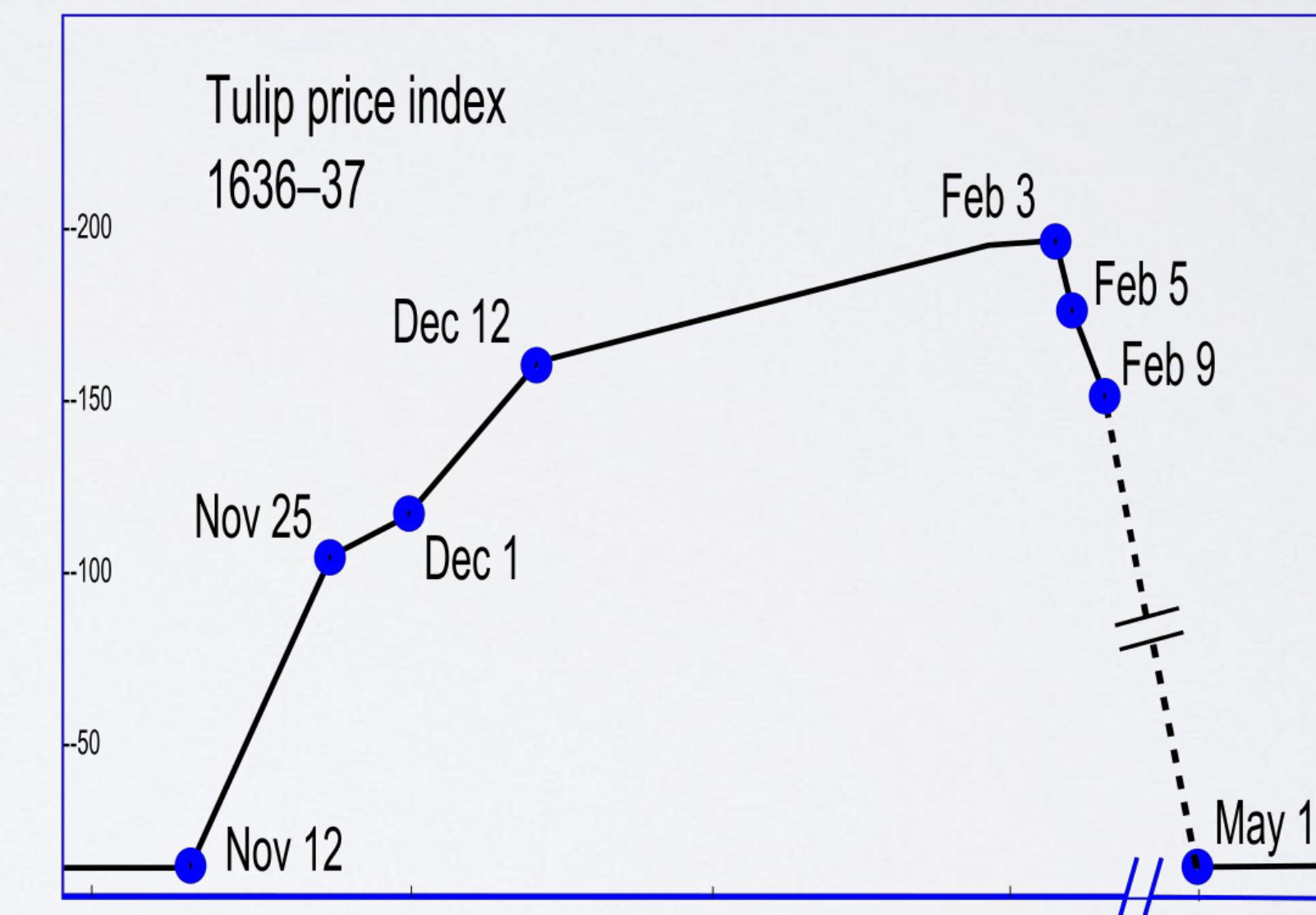
50% DE TODOS OS BITCOINS PERCEDEM A
1000 PESSOAS

ENERGY CONSUMPTION

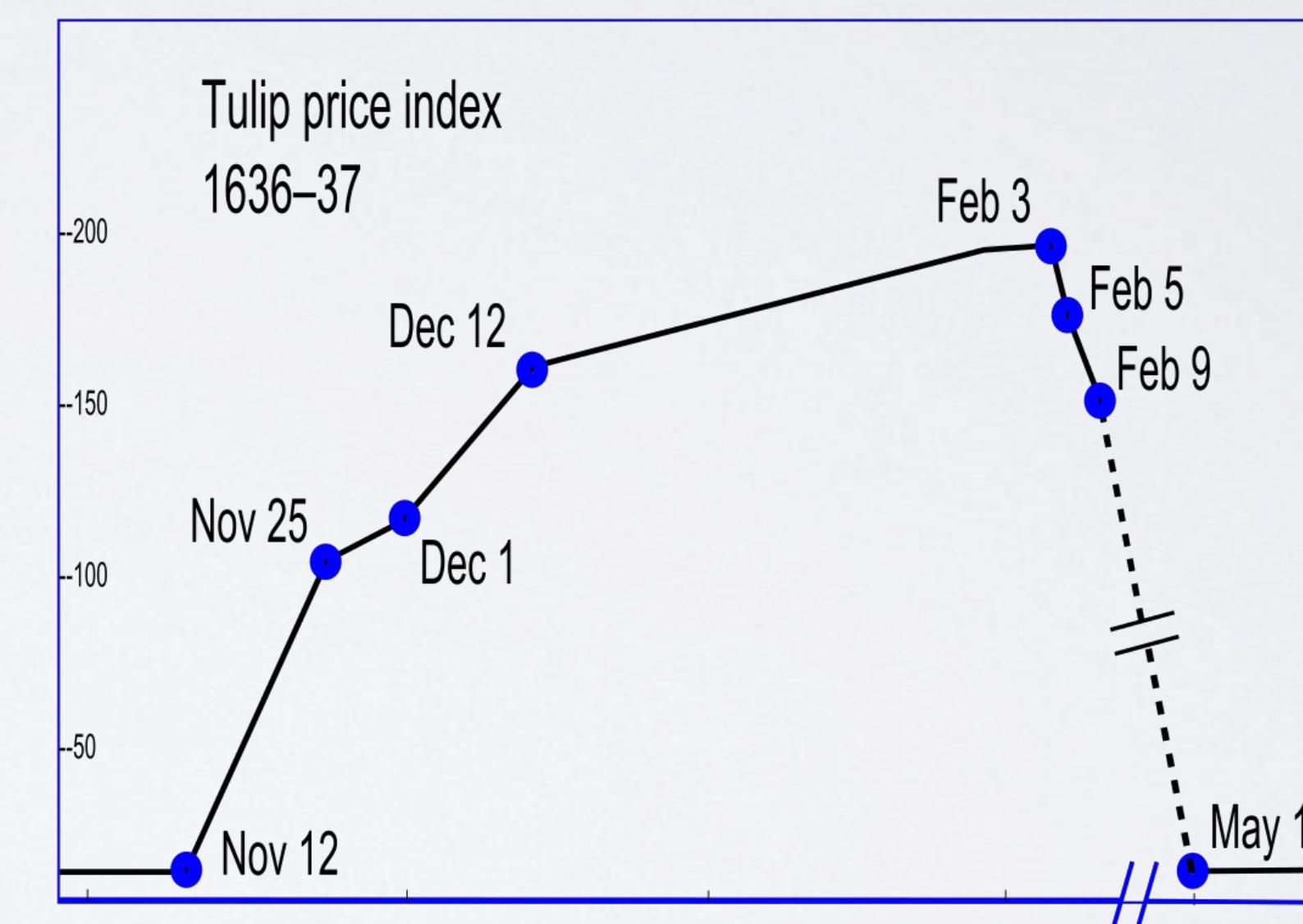
- Uma área de críticas pesadas tem a ver com a vasta quantidade de energia necessária para processar e armazenar transações, especialmente à medida que o uso da tecnologia blockchain aumenta
- As mineradoras da rede blockchain do Bitcoin estão tentando 450 mil trilhões de soluções por segundo nos esforços para validar as transações, usando quantidades substanciais de energia do computador
- Recursos desperdiçados: Mineração com Bitcoin desperdiça enormes quantidades de energia (US \$ 15 milhões / dia = Austria)

TULIP MANIA

- Tulip mania foi um período em que os preços de contrato para alguns bulbos de tulipas atingiram níveis extraordinariamente altos
- e então desmoronou dramaticamente em fevereiro de 1637.
- Geralmente é considerada a primeira bolha especulativa registrada.



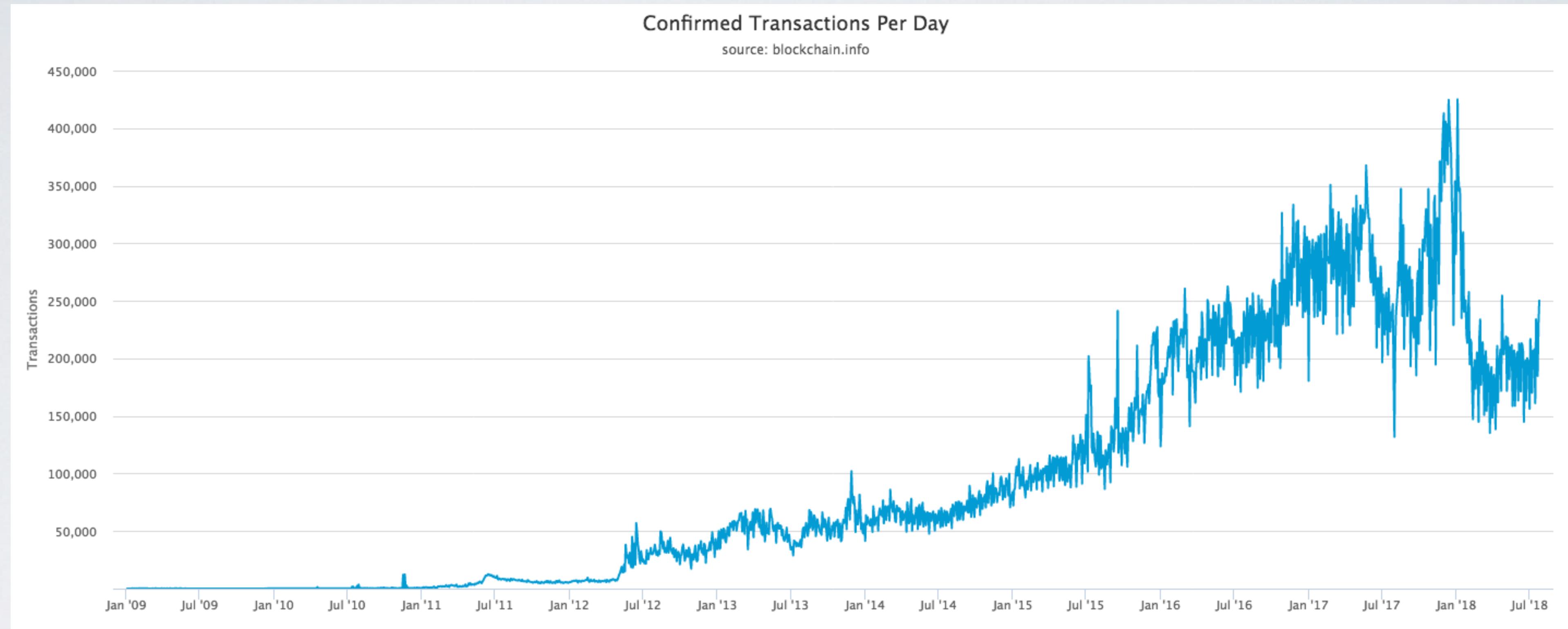
- Bitcoin > 300% em menos de 40 dias (\$5,500 para \$19,900)
- E o preço voltou ao inicial em 50 dias.

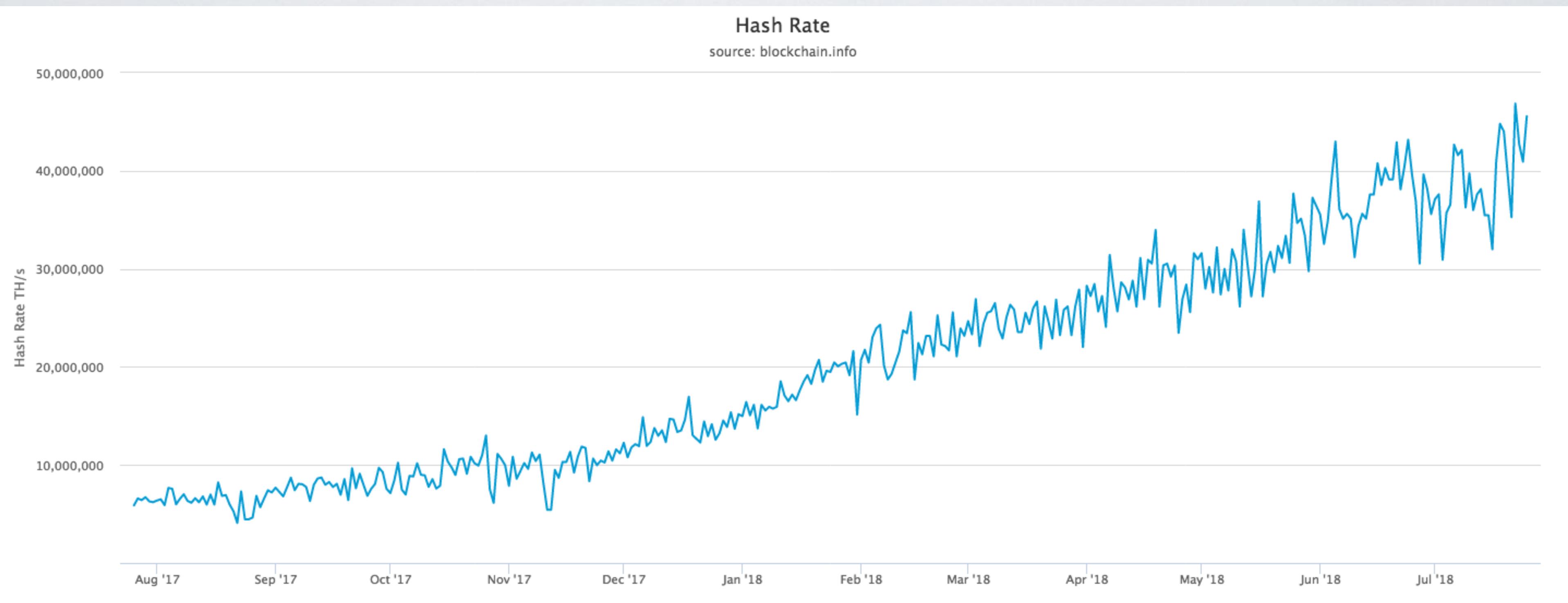


TPS

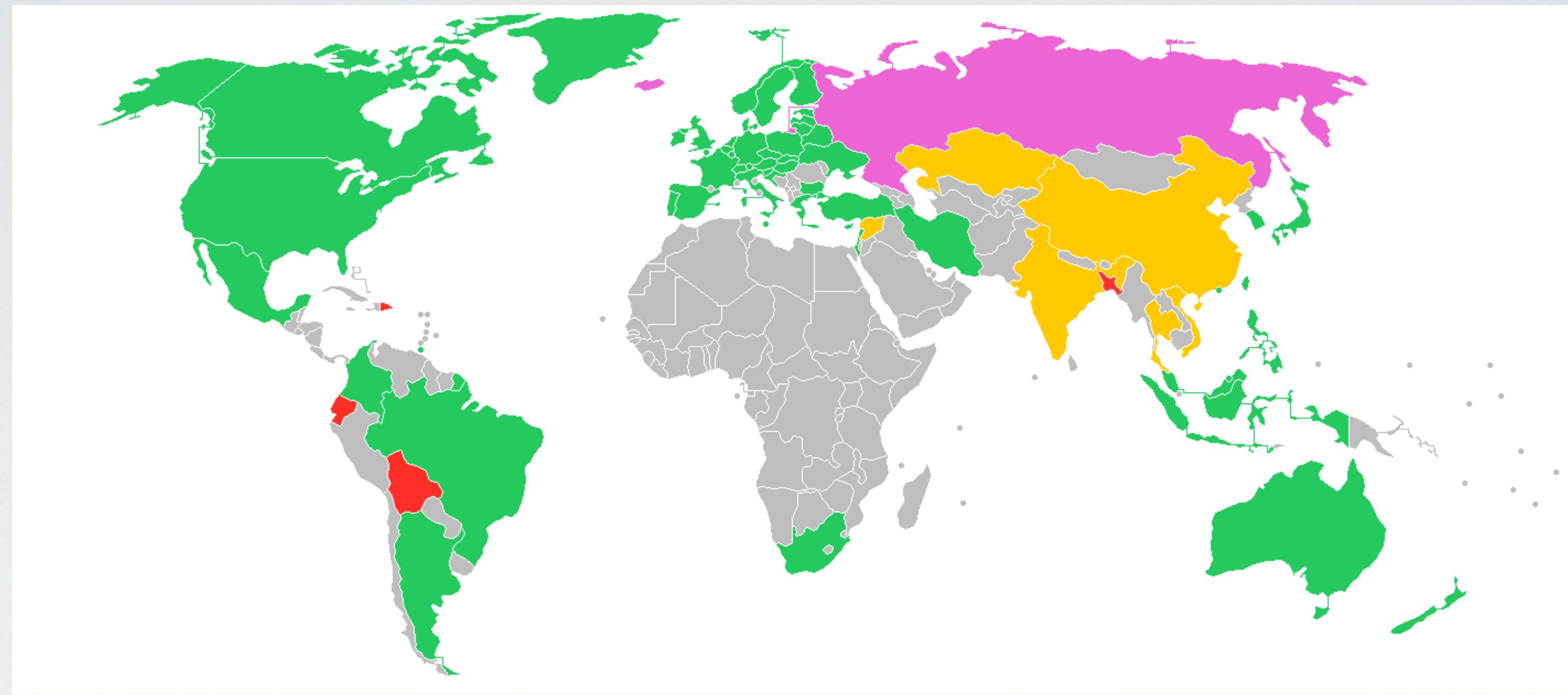
POSSIBILIDADES

- Fim das moedas nacionais
- Fim dos Bancos
- O fim do empréstimo predatório
- O fim do IRF
- O fim da cabine de votação
- O fim de ordens de pagamento
- Qualquer pessoa com um celular é um banco









LEGALITY

2	◆ Ethereum	\$48,153,443,418	\$477.06	\$1,588,420,000	100,937,495 ETH	0.50%	
3	✗ XRP	\$18,080,457,201	\$0.459879	\$188,618,000	39,315,683,476 XRP *	-0.60%	
4	฿ Bitcoin Cash	\$14,402,226,598	\$834.49	\$580,286,000	17,258,738 BCH	-0.15%	
5	⚡ EOS	\$7,702,915,690	\$8.60	\$621,283,000	896,149,492 EOS *	0.17%	
6	🚀 Stellar	\$6,097,836,041	\$0.324917	\$187,685,000	18,767,365,329 XLM *	0.21%	
7	฿ Litecoin	\$5,001,983,379	\$86.87	\$272,513,000	57,581,957 LTC	-0.46%	
8	✳️ Cardano	\$4,415,872,727	\$0.170319	\$77,473,100	25,927,070,538 ADA *	-1.09%	
9	⌚ IOTA	\$2,886,236,451	\$1.04	\$42,523,600	2,779,530,283 MIOTA *	5.10%	
10	₾ Tether	\$2,511,201,913	\$1.00	\$2,660,620,000	2,507,140,346 USDT *	0.42%	
11	🚩 TRON	\$2,490,663,391	\$0.037882	\$185,072,000	65,748,111,645 TRX *	1.35%	
12	㉔ Monero	\$2,297,669,536	\$141.30	\$29,724,000	16,261,161 XMR	0.21%	
13	⛓️ NEO	\$2,243,930,000	\$34.52	\$80,969,200	65,000,000 NEO *	0.57%	
14	⚡ Dash	\$2,033,845,016	\$247.53	\$137,089,000	8,216,593 DASH	0.45%	
15	diamond Ethereum Classic	\$1,767,381,725	\$17.11	\$181,955,000	103,320,612 ETC	3.04%	
16	똘 NEM	\$1,644,489,000	\$0.182721	\$10,169,900	8,999,999,999 XEM *	0.78%	
17	▼ VeChain	\$1,427,910,282	\$2.57	\$7,849,350	554,545,494 VEN *	30.49%	
18	₾ Tezos	\$1,322,588,690	\$2.18	\$2,532,330	607,489,041 XTZ *	4.44%	
19	diamond Binance Coin	\$1,273,659,496	\$13.34	\$53,571,400	95,512,523 BNB *	3.51%	
20	฿ OmiseGO	\$1,010,500,351	\$7.21	\$36,007,000	140,245,398 OMG *	0.86%	

3 NÍVEIS DE BLOCKCHAIN

1. Armazenamento para registros digitais
2. Trocar ativos digitais (chamados tokens)
3. Executando contratos inteligentes
 - Regras básicas - Termos e condições registrados no código
 - Rede distribuída executa contrato e monitora a conformidade
 - Os resultados são validados automaticamente sem terceiros

SMART CONTRACTS

- Os protocolos de consenso são fundamentais para determinar a sequência de ações resultantes do código do contrato.
- Isso permite que negociação de tudo usando peer-to-peer, desde energia renovável até reservas automatizadas de quartos de hotel.

O QUE SÃO SMART CONTRACTS?

- São protocolos de computador que facilitam, verificam ou reforçam a negociação ou a execução de um contrato ou que tornam desnecessária uma cláusula contratual
- Pode ajudar a trocar dinheiro, propriedade, ações ou qualquer coisa de valor de uma forma transparente e livre de conflitos, evitando os serviços de um intermediário
- Define as regras e penalidades em torno de um contrato da mesma maneira que um contrato tradicional, mas também automaticamente imponha essas obrigações (código é lei)

Average Settlement Time By Transaction Type



1



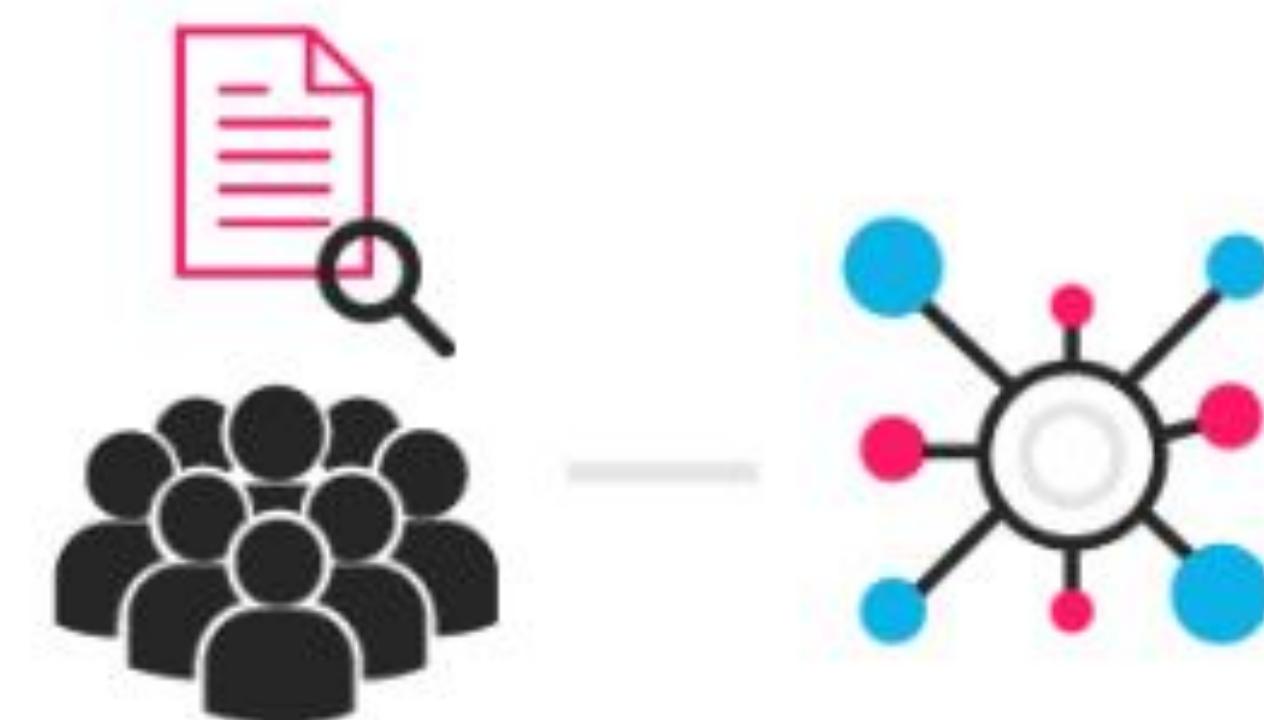
An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

2



A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

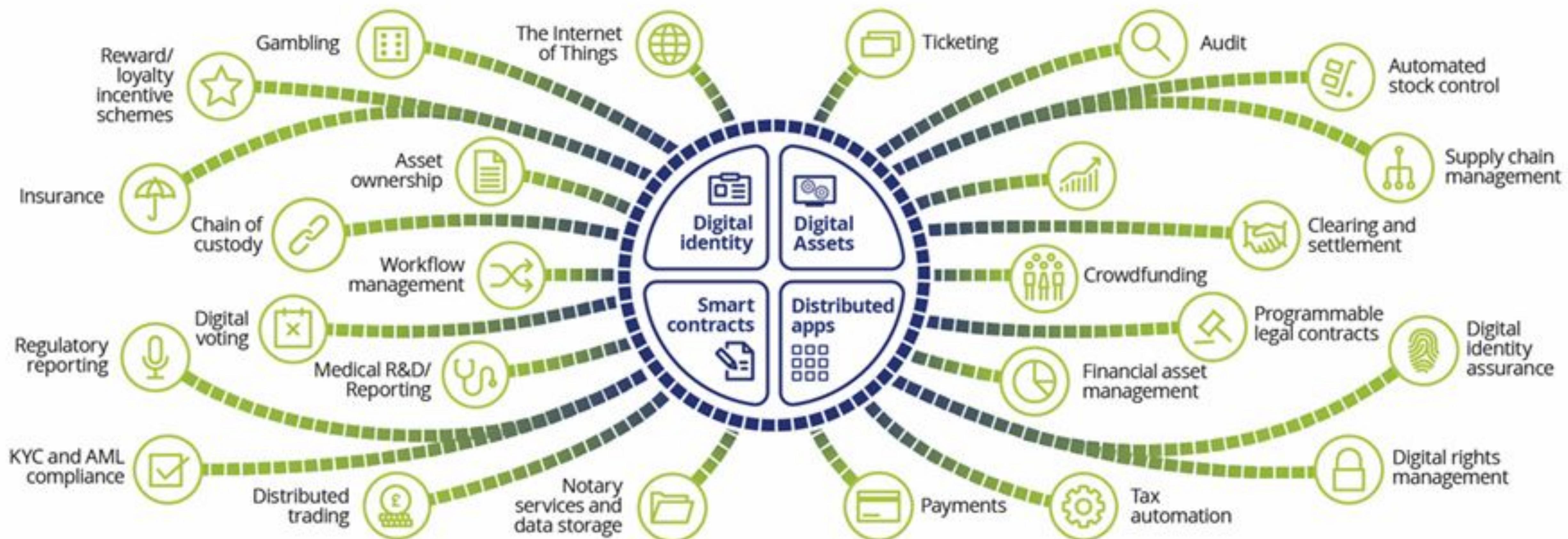
3



Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

What can you do with a blockchain?

KYC – Know Your Customer AML – Anti-Money Laundering



Deloitte.

www.deloitte.co.uk/blockchain



ethereum

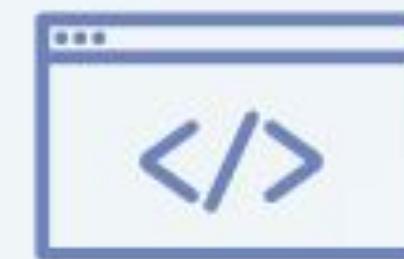
The World Computer - Open Source Peer-to-Peer Applications

ETHEREUM

- Ethereum é uma plataforma descentralizada que executa contratos inteligentes: aplicativos que são executados exatamente como programados, sem qualquer possibilidade de tempo de inatividade, censura, fraude ou interferência de terceiros.
- Esses aplicativos são executados em um blockchain personalizado, uma infra-estrutura global compartilhada extremamente poderosa que pode movimentar valor e representar a propriedade da propriedade.
- Isso permite que os desenvolvedores criem mercados, armazenem registros de dívidas ou promessas, movimentem fundos de acordo com instruções dadas no passado (como um testamento ou um contrato futuro) e muitas coisas que ainda não foram inventadas, tudo sem um intermediário ou risco da contrapartida.



OUR VISION



Be an open source standard, not a product



Address enterprise deployment requirements



Evolve in tandem with advances in public Ethereum



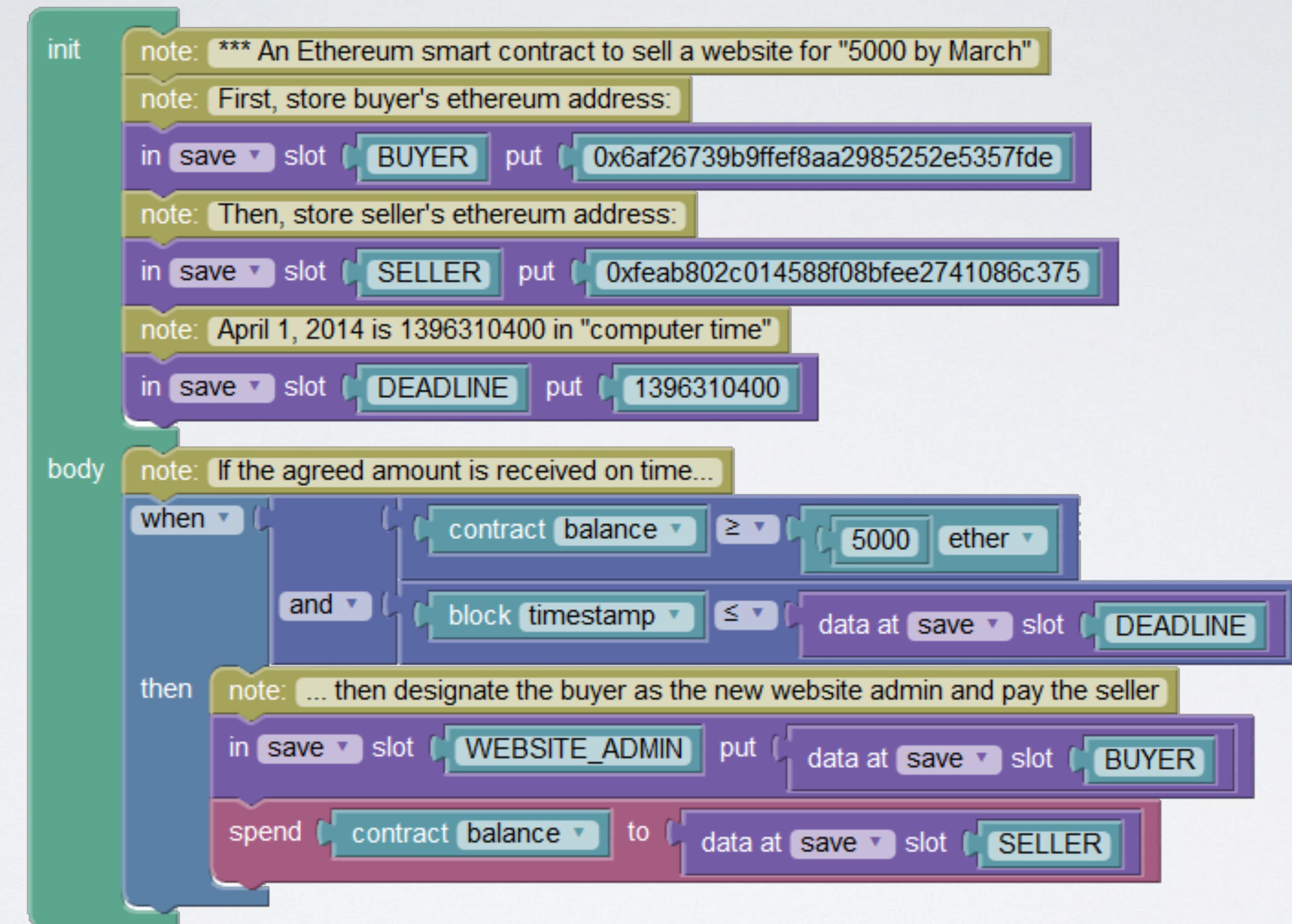
Leverage existing standards

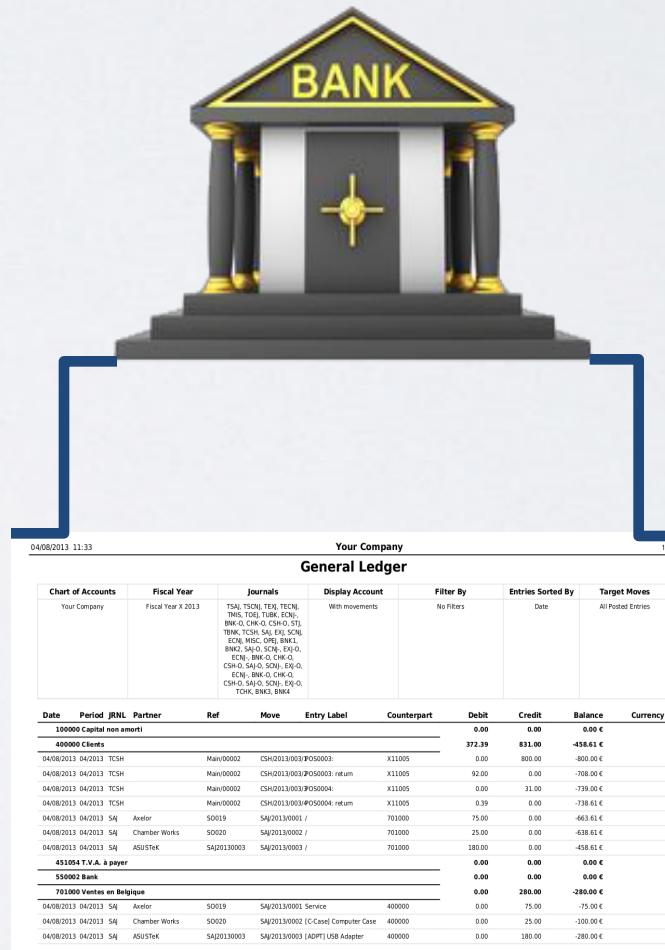
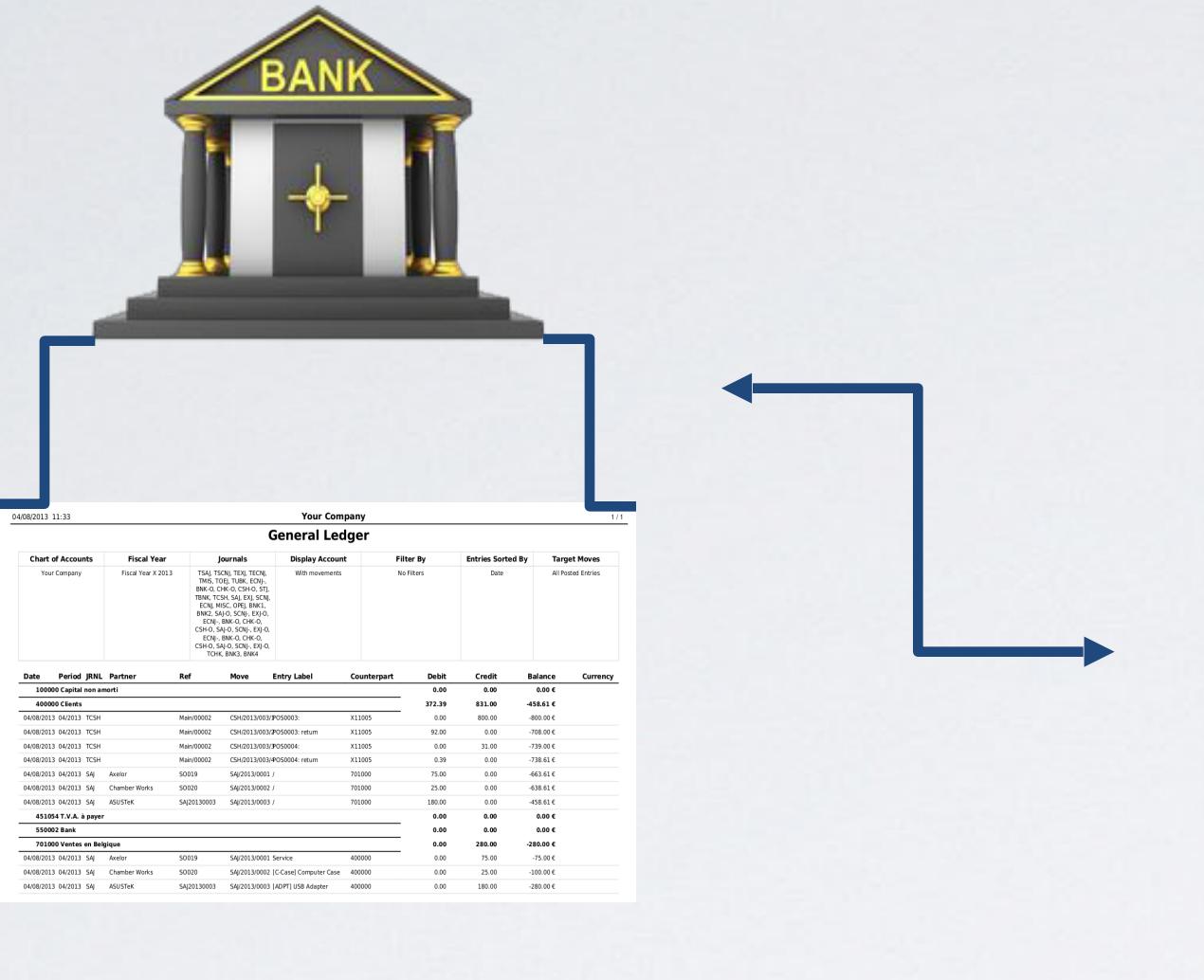
OUR MISSION

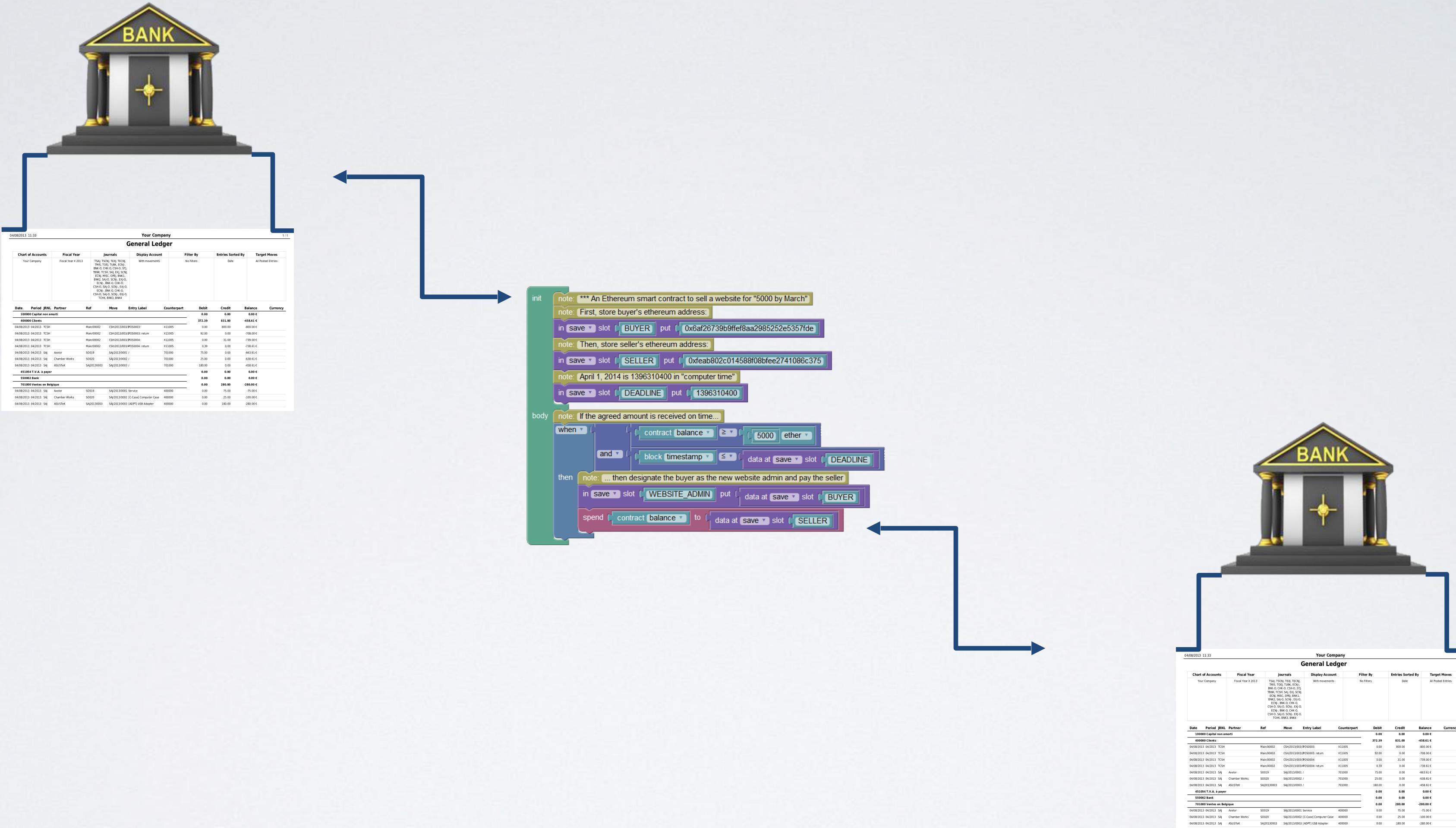
A clear roadmap for enterprise features and requirements

Robust governance model and accountability, clarity around IP and licensing models for open source technology

Resources for businesses to learn about Ethereum and leverage this groundbreaking technology to address specific industry use cases











```
init
  note: *** An Ethereum smart contract to sell a website for "5000 by March"
  note: First, store buyer's ethereum address
  in (save slot BUYER put 0x6af26739b9ffef0aa2985252e5357de)
  note: Then, store seller's ethereum address
  in (save slot SELLER put 0xfeab802c014588f08bfee2741086c375)
  note: April 1, 2014 is 1396310400 in "computer time"
  in (save slot DEADLINE put 1396310400)

body
  note: If the agreed amount is received on time ...
  when
    contract balance >= 5000 ether
    and
      block timestamp <= data at save slot DEADLINE
  then
    note: ... then designate the buyer as the new website admin and pay the seller
    in (save slot WEBSITE_ADMIN put data at save slot BUYER)
    spend contract balance to data at save slot SELLER
```



ETHEREUM ALLIANCE

- O projeto Ethereum foi inicializado por meio de uma pré-venda de éter durante agosto de 2014 (ICO).
- É desenvolvido pela Ethereum Foundation, uma organização sem fins lucrativos na suíça, com contribuições de indivíduos e organizações em todo o mundo.

ETHER

- O éter é um elemento necessário - um combustível - para operar a plataforma de aplicação distribuída Ethereum.
- É uma forma de pagamento feita pelos clientes da plataforma para as máquinas que executam as operações solicitadas, funcionando como o incentivo que garante que os desenvolvedores escrevam aplicativos de qualidade e que a rede permaneça saudável.
- Os desenvolvedores que pretendem criar aplicativos que usarão o blockchain Ethereum precisam de éter.
- Os usuários que desejam acessar e interagir com contratos inteligentes no blockchain Ethereum também precisam de éter.

TOKENS

- Um uso mais amplo é suportado pela infraestrutura digital introduzida pelo Bitcoin, são representada por “tokens”.
- Um “token” pode ser definido como um “ativo digital escasso baseado na tecnologia subjacente inspirada pelo Bitcoin”.
- Os tokens podem usar bases de código similares, mas diferentes bancos de dados blockchain.
- O Ethereum foi inspirado pelo Bitcoin, mas tem seu próprio blockchain e foi projetado para ser mais programável. Tokens podem ser emitidos no topo do blockchain Ethereum.
- Os compradores de tokens estão comprando chaves privadas, que são semelhantes às chaves da API, mas podem ser transferidas para outras partes sem o consentimento.

TOKENS

- Os tokens têm um valor e, portanto, um preço.
- Os tokens são um novo modelo de tecnologia e podem ser uma alternativa ao financiamento baseado em capital.
- Os tokens não diluem o capital. Eles introduzem um enorme aumento na base de compradores e no tempo para liquidez.
- Lançamentos de tokens diferem das vendas de ações (ICOs); no entanto, eles podem ser emitidos como uma maneira de compartilhar lucros.
- Os tokens podem ser vendidos internacionalmente pela internet e estão sempre abertos para negócios.
- Tokens descentralizam o processo de financiamento da tecnologia.



ERC-20

ERC-20

- ERC (Ethereum Request for Comments) é um protocolo oficial para fazer sugestões para melhorar a rede Ethereum;
- 20 – é o número de identificação único da proposta.
- Os tokens que atendem a essas especificações são conhecidos como tokens ERC-20 e, na verdade, são contratos inteligentes para o sistema
- O padrão ERC-20 define um conjunto de regras que devem ser atendidas para que um token seja aceito e capaz de interagir com outros tokens na rede.
- Os próprios tokens são ativos de bloco, que podem ter valor, e podem ser enviados e recebidos como qualquer outra criptomoeda de blocos Ethereum.
- O padrão ERC-20 fornece seis parâmetros obrigatórios e três opcionais (mas recomendados) para qualquer contrato inteligente.

Transaction Information

TxHash:	0x2e81009efe3c00f4869ac4a39fa9b106d5b9fb14d73e98a70d7c5f6f96f4d807
Block Height:	4243645 (1287952 block confirmations)
TimeStamp:	236 days 3 hrs ago (Sep-06-2017 06:28:17 AM +UTC)
From:	0x5e44c3e467a49c9ca0296a9f130fc433041aaa28
To:	Contract 0xd26114cd6ee289accf82350c8d8487fdb8a0c07 (OmiseGoToken) 
Token Transfer:	▶ 2.77347842 (\$47.86)  OmiseGO Token from 0x5e44c3e467a49c... to → 0x7d50f34e781142e...
Value:	0 Ether (\$0.00)
Gas Limit:	300000
Gas Used By Txn:	52158
Gas Price:	0.000000025 Ether (25 Gwei)
Actual Tx Cost/Fee:	0.00130395 Ether (\$0.89)
Nonce:	21525

PROTOCOLO ERC-20

- As principais características do protocolo ERC-20:
 - Opcionais
 - Nome do Token, Símbolo, Casas Decimais (até 18)
 - Obrigatórias: totalSupply, balanceOf, transfer, transferFrom, approve, allowance

EXEMPLOS DE ERC-20

- Binance Coin (BNB)
- Walton (WTC)
- OmiseGO (OMG)
- VeChain (VEN)
- SUBstratum (SUB)

ERC721

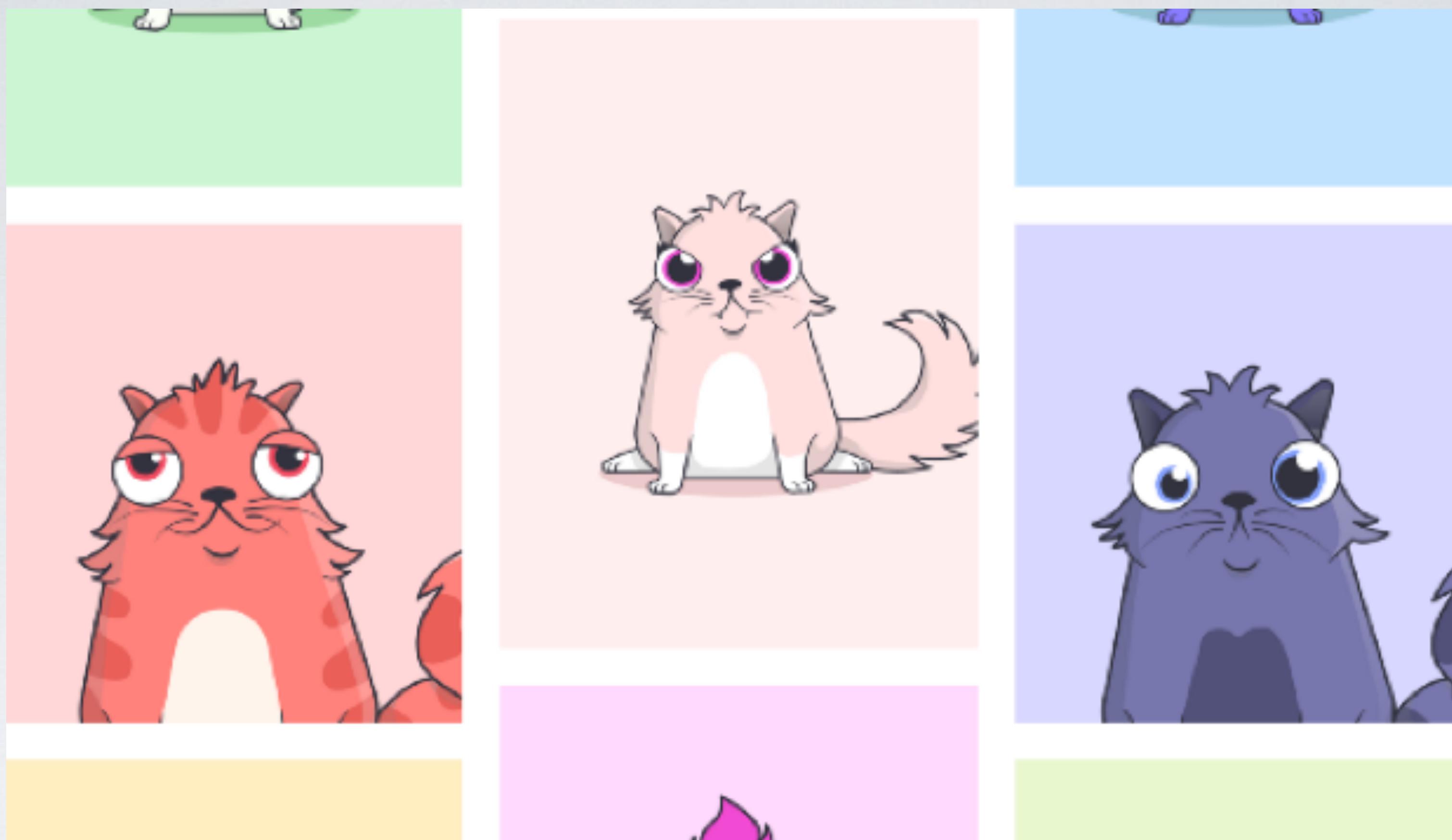


C

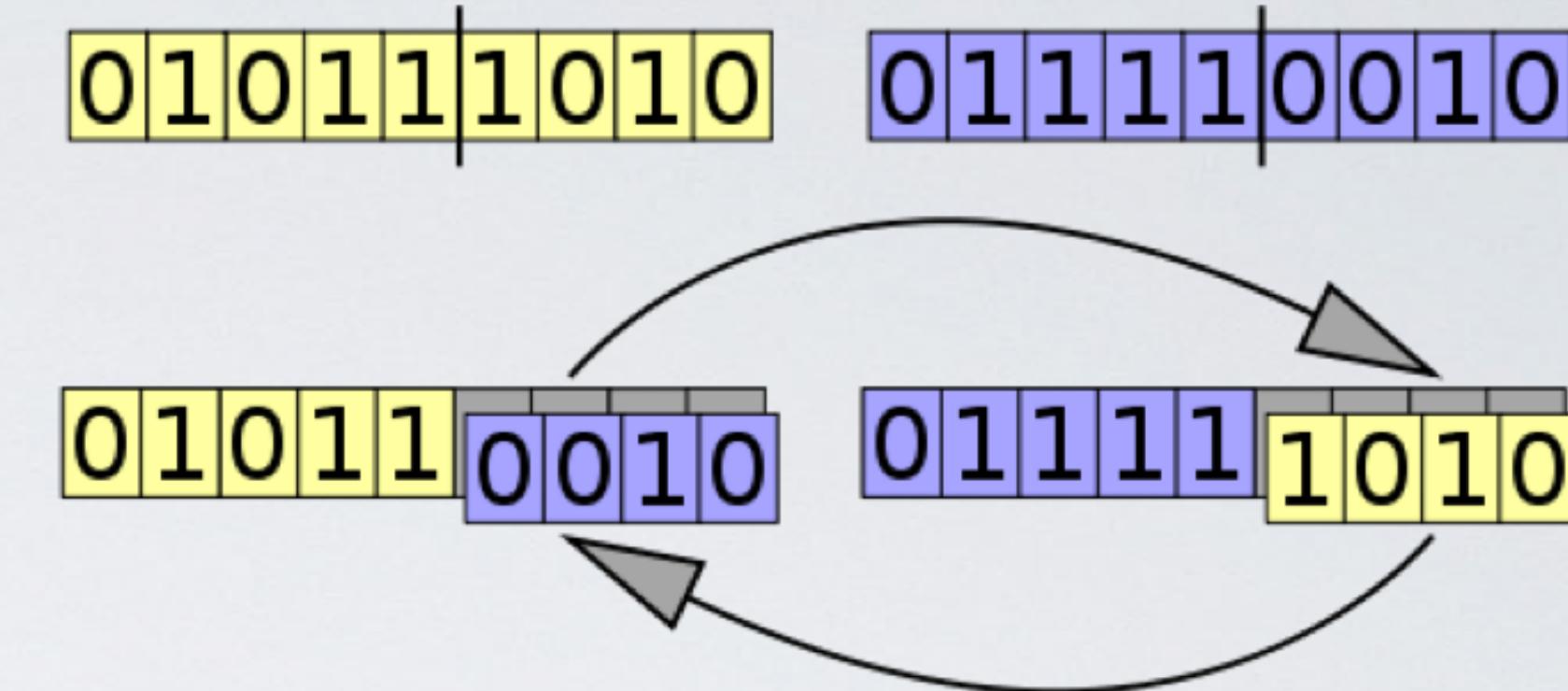
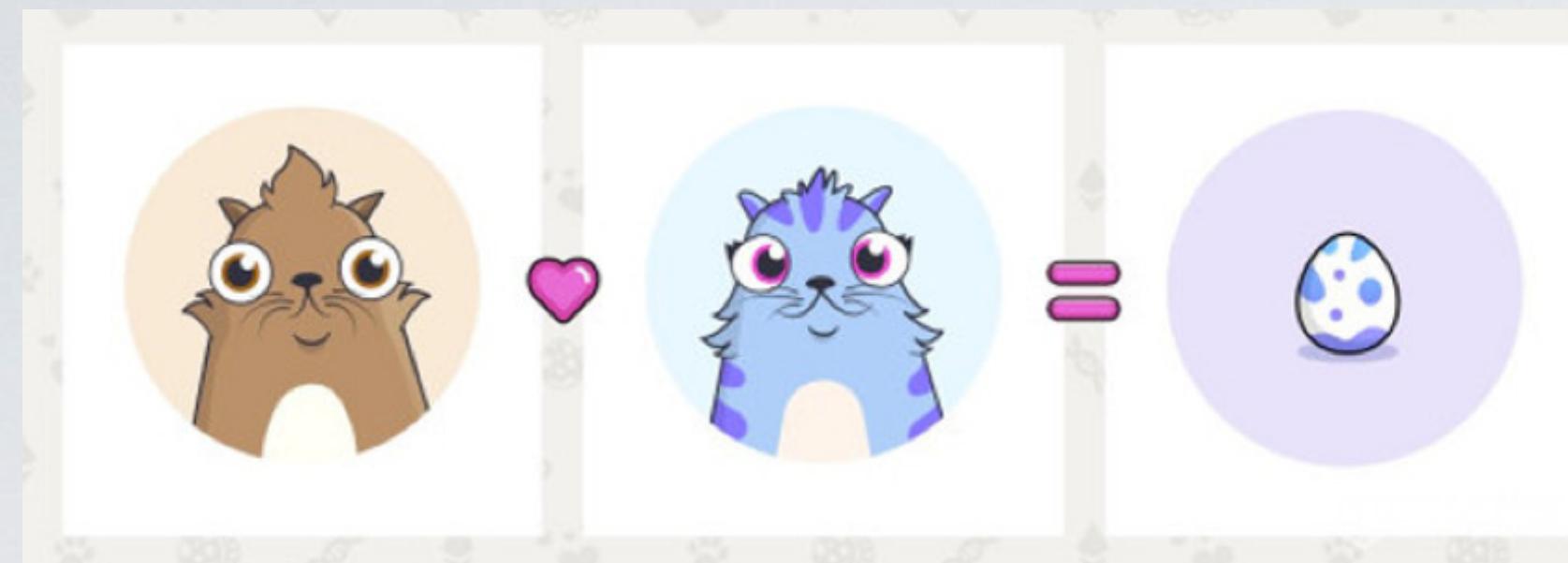
ERC-721

ERC-721

- O ERC-721 é um padrão aberto e gratuito que descreve como criar fichas não fungíveis ou exclusivas na blockchain Ethereum.
- Embora a maioria dos tokens seja fungível (cada token é o mesmo que qualquer outro token), os tokens ERC-721 são todos únicos.
- Pense neles como itens colecionáveis raros e únicos.



CRYPTOKITTIES



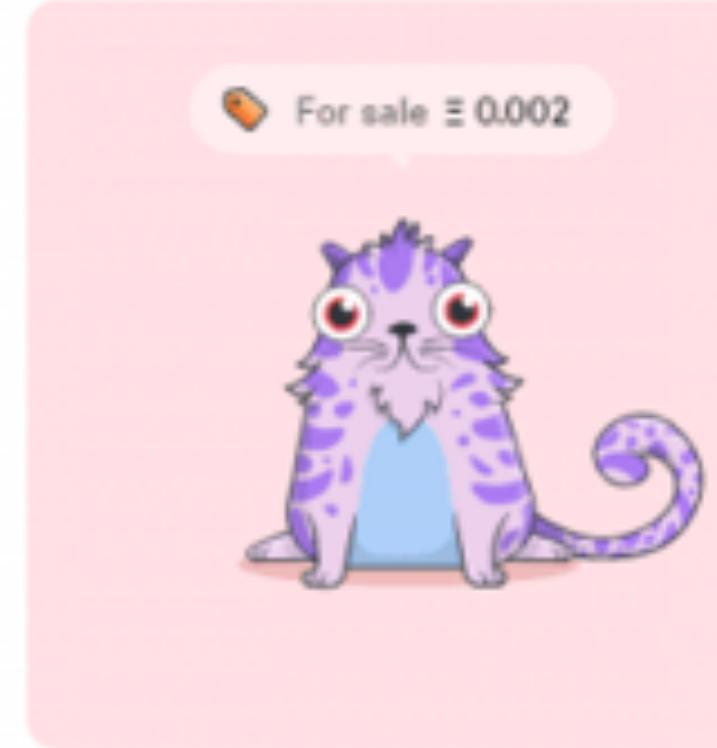
All Kitties Gen 0

Search filters

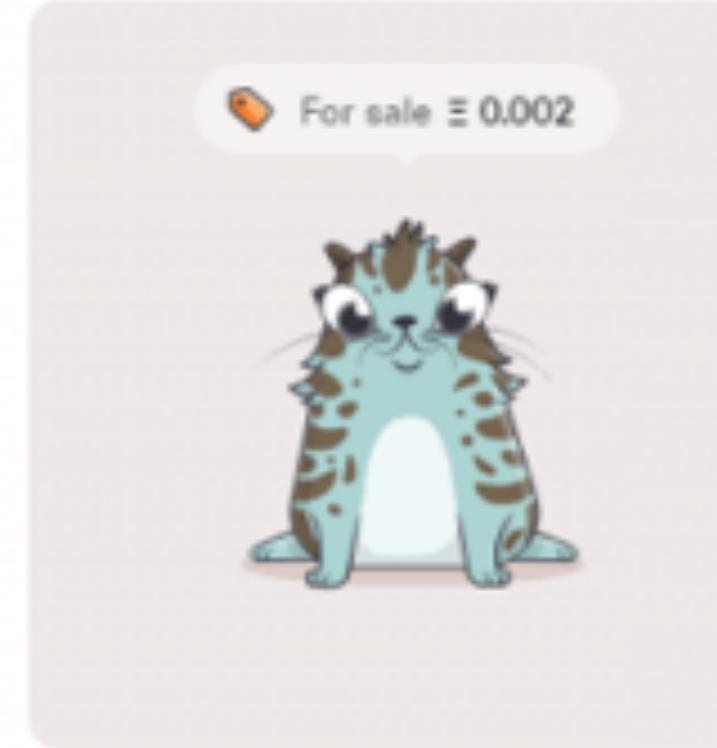
include for sale siring other

143537 Kitties

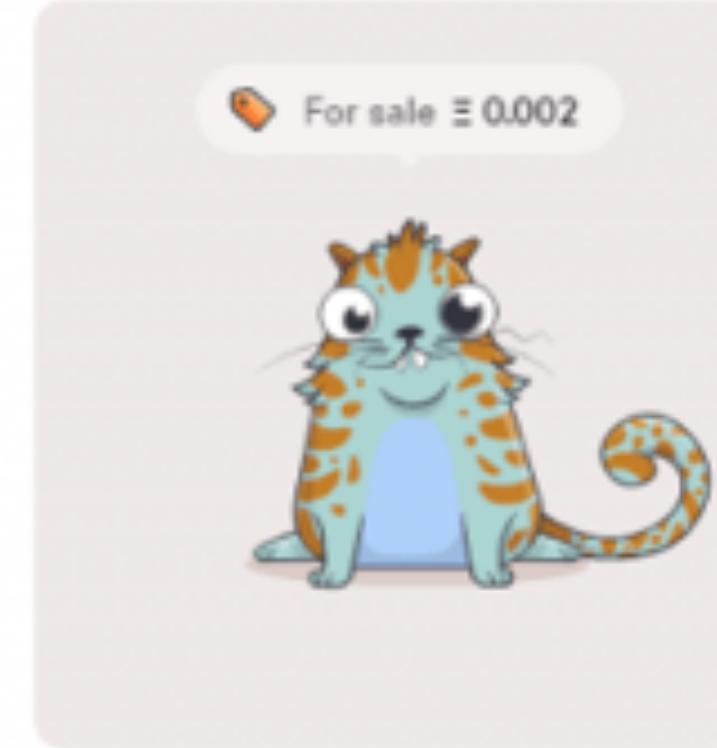
sort by Price ▾ Low to high ▾



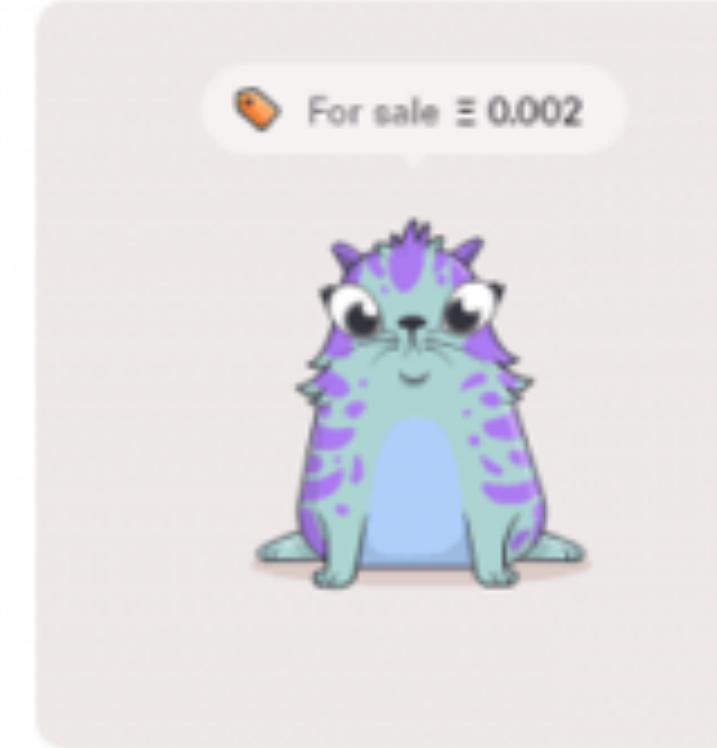
Kitty 705454 · Gen 7 · Snappy



Kitty 700134 · Gen 9 · Snappy



Kitty 705664 · Gen 13 · Brisk



Kitty 700525 · Gen 10 · Brisk

CRYPTOKITTIES

- <https://www.cryptokitties.co/>
- CryptoKitties é um jogo virtual baseado em blockchain desenvolvido pela Axiom Zen que permite aos jogadores comprar, coletar, reproduzir e vender vários tipos de gatos virtuais.
- Representa uma das primeiras tentativas de implantar a tecnologia blockchain para fins recreativos e de lazer.
- A popularidade do jogo em dezembro de 2017 congestionou a rede Ethereum, fazendo com que ela alcançasse um recorde de transações e desacelerasse significativamente.
- Em 20 de março de 2018, foi anunciado que a CryptoKitties seria desmembrada em sua própria empresa e arrecadou US \$ 12 milhões de várias empresas de capital de risco e investidores-anjo.
- Em dezembro de 2017, um CryptoKitty foi vendido por US \$ 100.000



CONTRATO DO CRYPTOKITTIES

- KittyBreeding: Este arquivo contém os métodos necessários para criar gatos juntos, incluindo manter as ofertas e depende de um contrato externo de combinação genética.
- KittyAuctions: Aqui temos os métodos públicos para leiloar ou licitar em gatos ou serviços.
 - A funcionalidade real do leilão é tratada em dois contratos (um para vendas e outro para contratação), enquanto a criação de leilões e os lances são mediados principalmente por essa faceta do contrato principal.

CONTRATO DO CRYPTOKITTIES

- KittyMinting: Esta última faceta contém a funcionalidade que usamos para criar novos gatos gen0.
- Podemos criar até 5000 gatos “promo” que podem ser doados (especialmente quando a comunidade é nova), e todos os outros só podem ser criados e colocados imediatamente em leilão através de um preço inicial determinado por algoritmos.
- [https://etherscan.io/address/
0x06012c8cf97bead5deae237070f9587f8e7a266d#code](https://etherscan.io/address/0x06012c8cf97bead5deae237070f9587f8e7a266d#code)

CRYPTOCOUNTRIES

- Compra e venda de países
- com um sistema inflacionário, onde o custo do item sempre aumenta a cada transação (25%)
- mecânica de batata quente (todo mundo que vende ganha o lucro com a taxa, menos o ultimo comprador, que acaba sem vender para ninguém).
- China nesse sistema atualmente tem valor de U\$124.000



Australia



OWNER: CRYPTOGIRL

Capital
Canberra
Population
24117360

Language
English
Currency
Australian dollar

12.1135... ETH

Buy



Taiwan, Province ...



OWNER: MUDDLEDBOX

Capital
Taipei
Population
23503349

Language
Chinese
Currency
New Taiwan d...

10.1084... ETH

Buy



Korea (Republic of)



OWNER: CRYPT0JON

Capital
Seoul
Population
50801405

Language
Korean
Currency
South Korean ...

9.62870... ETH

Buy



Japan



OWNER: TOM BRADY

Capital
Tokyo
Population
126960000

Language
Japanese
Currency
Japanese yen

9.44681... ETH

Buy

Total Research Pot: 2Ξ (10% distributed daily)

Global Goo Production: 4 (per second)



You currently have 83798 Goo

Your lab produces 3 Goo/s, roughly 75% of the Global Production
In 01:59:02, you will earn 75% of today's 0.2Ξ research pot

Rare Item Raffle

 Worth 0.5Ξ
 01:59:39 left
 Ticket Cost: 1K
 (You have 0 Tickets)
 1x 10x MAX BUY

Game Tutorial:

Buy scientists and upgrades to increase your Goo production.
 Some items cost Eth as well as Goo, but offer more production.
 All scientists can be sold for 75% of their Eth/Goo buy price.
 You can spend your Goo in the Barracks to attack other players!
 Finally the raffle allows you to win Eth by spending Goo on tickets.

Balance: 0Ξ Withdraw Goo Leaderboards

 Intern Kitties Makes: 1Ξ (each) Cost: 30Ξ 1x 10x MAX BUY 1x 10x ALL SELL	 Graduate Gerbils Makes: 2Ξ (each) Cost: 50Ξ 1x 10x MAX BUY 1x 10x ALL SELL
 Lab Rats Makes: 10Ξ (each) Cost: FREE 1x 10x MAX BUY 1x 10x ALL SELL	 +100% Production Cost: 100Ξ BUY +100% Production Cost: 100Ξ BUY

Switch to Barracks **Join Discord**

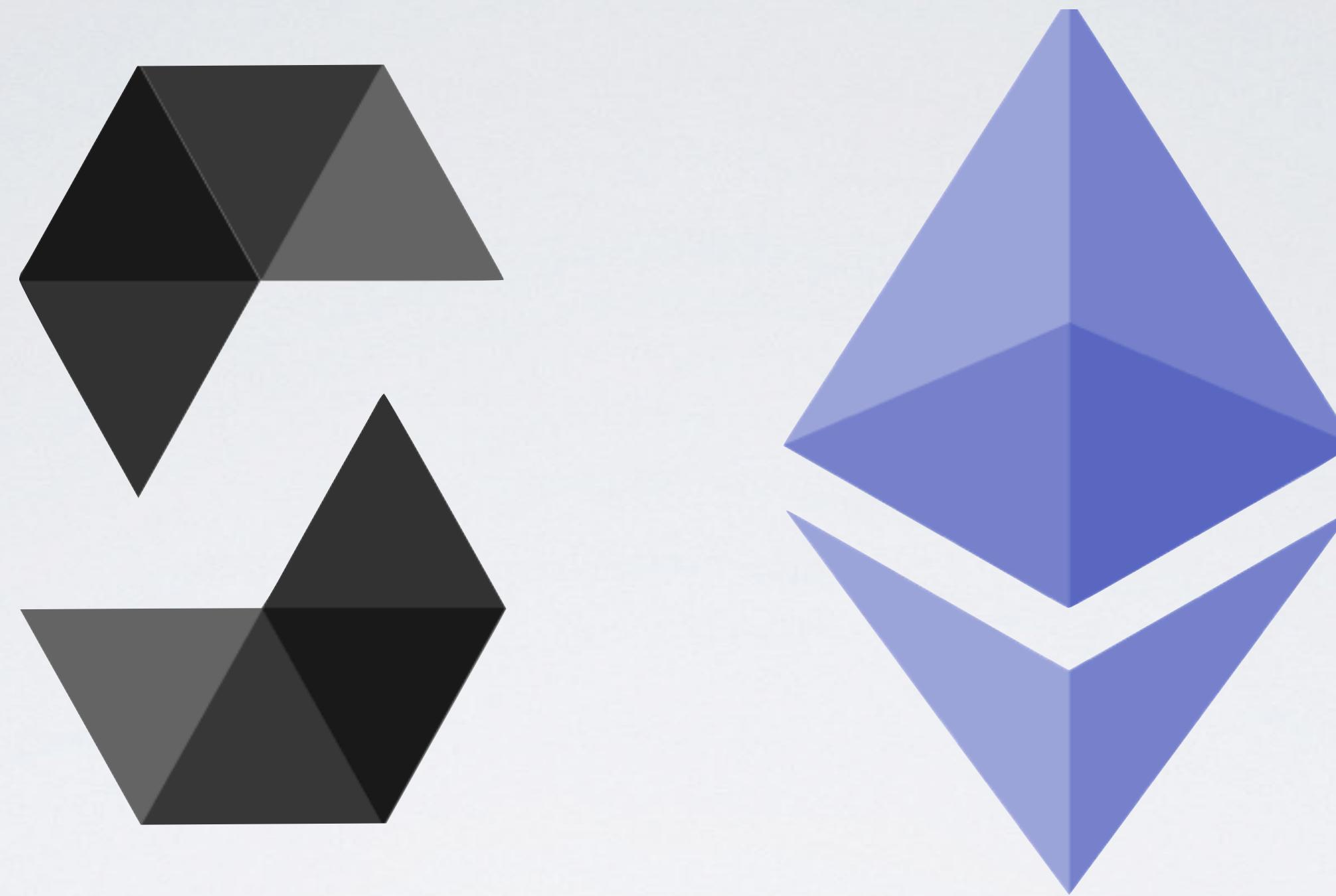
ETHER GOO

<https://ethergoo.io/>

EII

- eII criou um token ERC-20
- Esta desenvolvendo o game Cryptowars, totalmente utilizando smart contracts
- CryptoWars tenta colocar no gameplay as limitações da rede de forma a trazer uma experiência game
- Jogadores criam vilas e fazem batalhas entre eles e ataques a vilas adversárias de forma a ganharem token do outro jogador



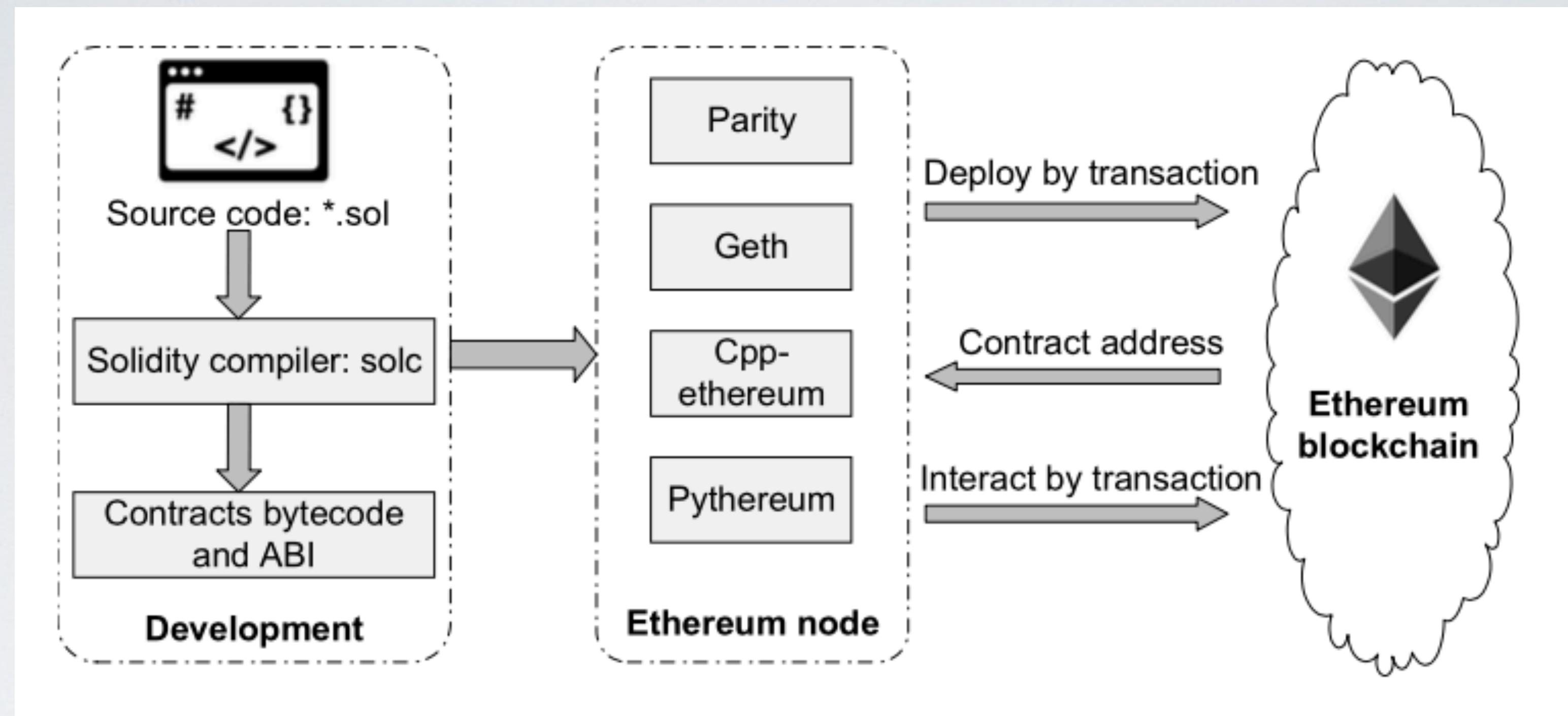


SOLIDITY

Linguagem para criação de Smart Contracts

SOLIDITY

- Linguagem Orientada a Objetos de Alto Nível para Smart Contracts, inicialmente proposta em agosto de 2014 por Gavin Wood
- Solidity permite programar no Ethereum, uma máquina virtual baseada em blockchain
- Solidity é uma linguagem de programação com tipagem estática
- Uma linguagem de programação Contract que tenha semelhanças com Javascript e C
- Solidity é compilado para bytecode que é executável no EVM



SMART CONTRACT DEPLOYMENT

VANTAGENS PARA GAMES

- Evitam ataques DOS (Denial-of-Service)
- Uso em economia (sem depender de um terceiro)
- Compartilhamento de itens e economia

FERRAMENTAS

- <https://remix.ethereum.org> - Plataforma para o desenvolvimento e publicação de um contrato
- Metamask - ETH Wallet
- Rede Kovak para testes
 - Verificar transações: <https://kovan.etherscan.io/>
 - Pegar eth para testes: <https://gitter.im/kovan-testnet/faucet>

FERRAMENTAS

- Nethereum: [https://github.com/Nethereum/
Nethereum](https://github.com/Nethereum/Nethereum)
- Web3: <https://github.com/ethereum/web3.js/>

LOOM SDK

The screenshot shows the Loom Network Platform Alpha - 0.1.3 Build interface. The left sidebar includes links for DAppChain Generator, Block Explorer, Delegates, Accounts, and Oracles. The main content area is titled "DAppChain Generator" and displays "1000 ZombieTokens Staked". It features a search bar at the top right. Below the search bar, there's a section for "Existing Templates" with a card for "DelegateCall Ask a Question" about blockchain. To the right of the template cards is a large, stylized graphic of a 3D cube with geometric shapes floating around it, labeled "Event-driven Game Engine", "Turn-based Battles", and "Crypto-Collectibles". Below the templates, there's a section for "Generate Your Own:" with a "Choose Consensus Mechanism" section. It lists three options: "Loom Consensus Algorithm" (Experimental), "Tendermint PoS" (Unstable API), and "Casper PoS" (Coming Soon). At the bottom, there's a "DAppChain Ruleset" section with four items: "Rails ActiveRecord Adapter" (Experimental), "Serverless JS Lambda Functions" (Experimental), "REST gateway (with WebSockets)" (Experimental), and "Ethereum Virtual Machine" (Functional - Not Recommended).

ESPECIALIZAÇÃO EM BLOCKCHAIN

- Curso na PUCPR (<https://www.pucpr.br/cursos-especializacao/desenvolvimento-em-blockchain/>)
- Focado em aprender as técnicas para desenvolvimento em Blockchain
 - Criar Blockchain próprias, criar smart contracts, criar aplicações que usam a blockchain...
- Aulas quinzenais aos sábados com duração de 2 anos

PERGUNTAS

- Contato:

mark.joselli@pucpr.br

- Códigos:

<https://github.com/mjoselli/sbgames2018blockchain>