

Disciplina:

SMART CONTRACTS

Professor: Pablo V. Rego



SMAC_2022Sem02–Mod.02

Agenda Módulo #2 : Blockchain Overview

1. Bitcoin

- História do **Bitcoin**
- Problema dos Generais Bizantinos
- Ecosistema do Bitcoin
- Confiabilidade
- Distributed Ledger

3. Ethereum, Hyperledger

4. Casos de Uso

- **Smart Contracts**

2. Blockchain

- Conceitos
- Evolução
- Uso de Criptografia
- Funcionamento
- Processo de Transação
- Componentes
- Tipos
- Características , Benefícios, Tradeoffs, Capacidades, Desfavorecimentos
- Consenso

5. DeFi [mais adiante]

- Conceitos
- CEx/Dex
- Protocolos
- Uniswap
- AMMs
 - Liquidity Pools
 - Liquidity Providers
 - Constant Product Formula
 - AMM Variations

Módulo 02

Blockchain Overview

Tópico :

BITCOIN

História do Bitcoin

2008

- Idéia publicada pelo pseudônimo de Satoshi Nakamoto

2009

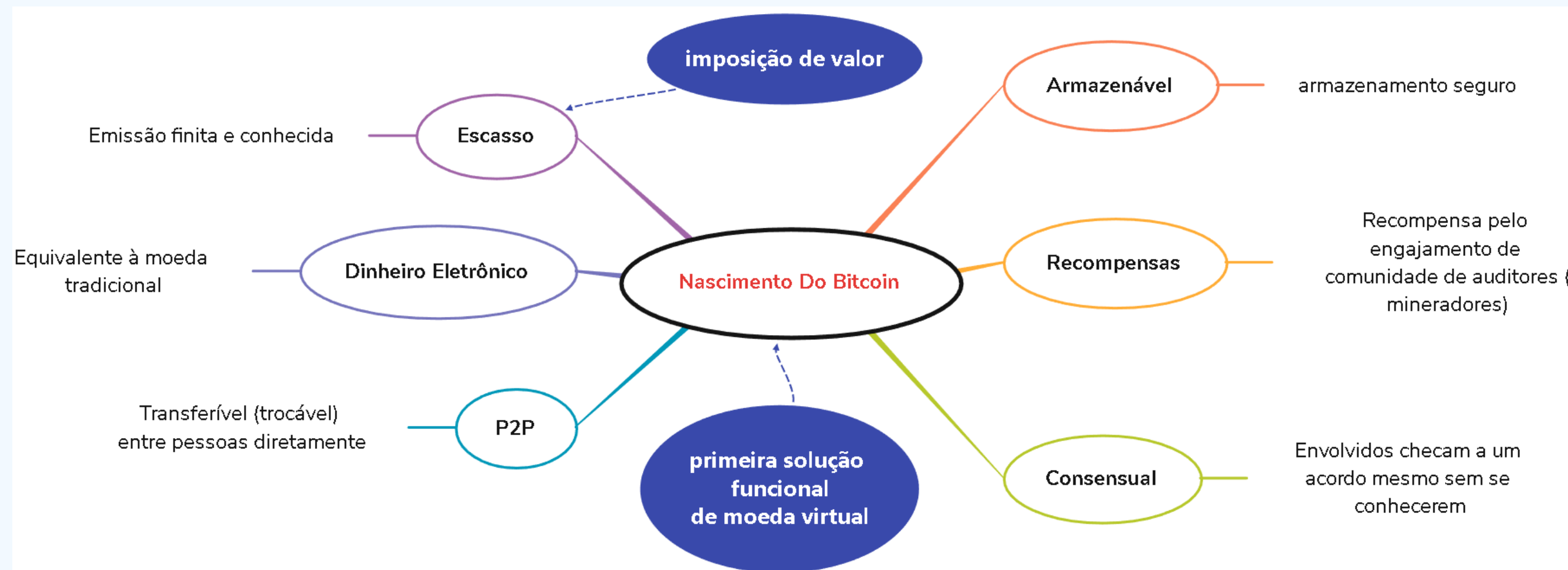
- Início das operações na Rede Bitcoin

2010

- Primeira exchange de criptomoedas lançada

2011

- 1 BTC = 1 USD



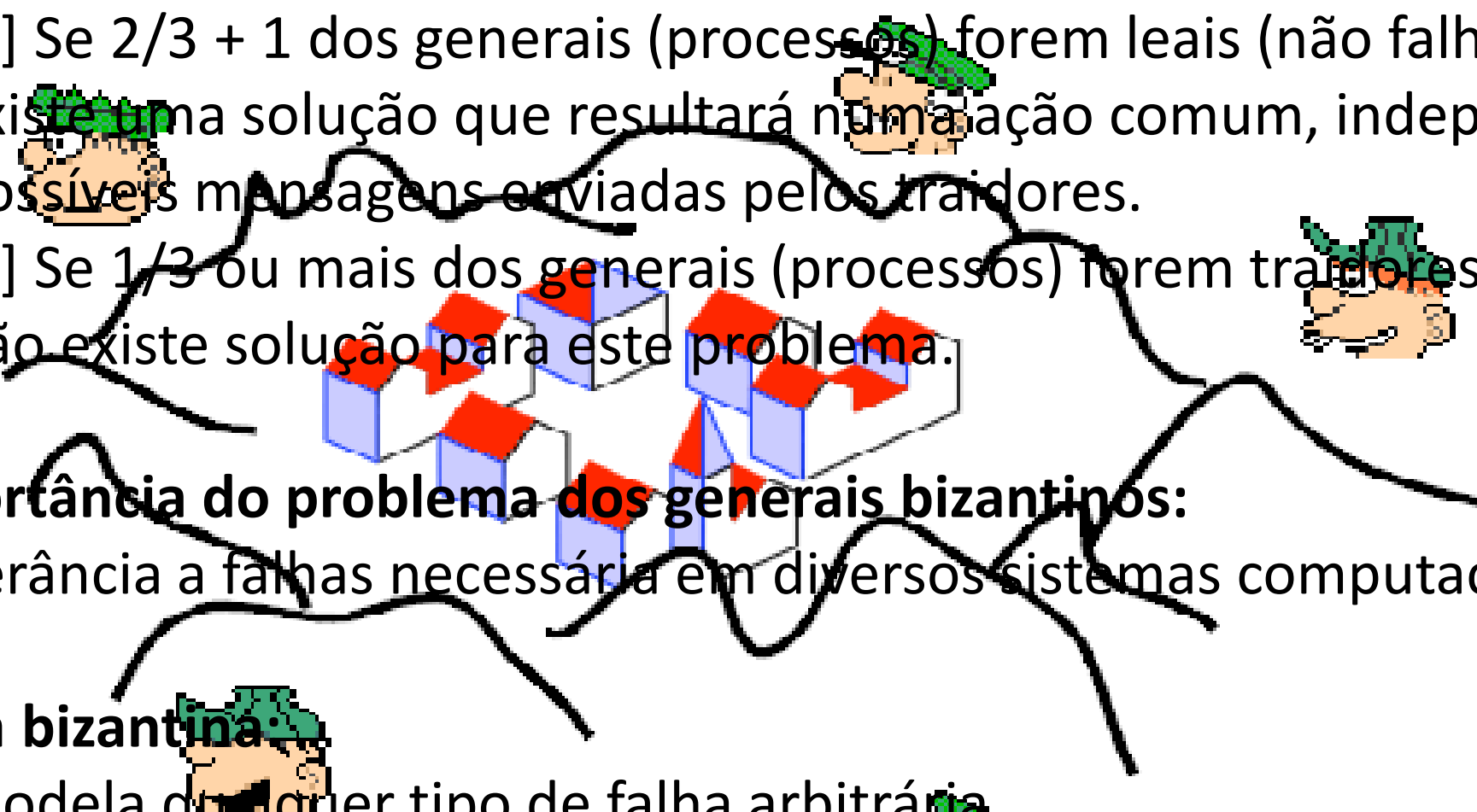
- 2013: 1 BTC = 100 USD
- 2014: Microsoft começa a aceitar pagamentos em BTC
- 2017: 1 BTC = 10k USD

Problema dos Generais Bizantinos

- Experimento para ilustrar as armadilhas e desafios de planejamento na tentativa de coordenar uma ação através da comunicação sobre uma enlace não confiável.
- Resolvido pelo modelo transacional do Bitcoin

- 1 Os generais cercam uma cidade com suas tropas
- 2 Generais são separados pelo relevo e só podem se comunicar através de mensageiros
- 3 Todos os generais devem chegar a um consenso sobre atacar ou recuar
- 4 Existem generais que são traidores
- 5 Os generais só vencem se todos os generais atacarem ao mesmo tempo

Teoremas:

- [1] Se $2/3 + 1$ dos generais (processos) forem leais (não falharem),  existe uma solução que resultará numa ação comum, independente de possíveis mensagens enviadas pelos traidores.
- [2] Se $1/3$ ou mais dos generais (processos) forem traidores (falharem), não existe solução para este problema.

Importância do problema dos generais bizantinos:

- Tolerância a falhas necessária em diversos sistemas computacionais.

Falha bizantina

- Modela qualquer tipo de falha arbitrária.
- Exemplo: enviar informações conflitantes a diferentes partes de um sistema.

Ecosistema do Bitcoin

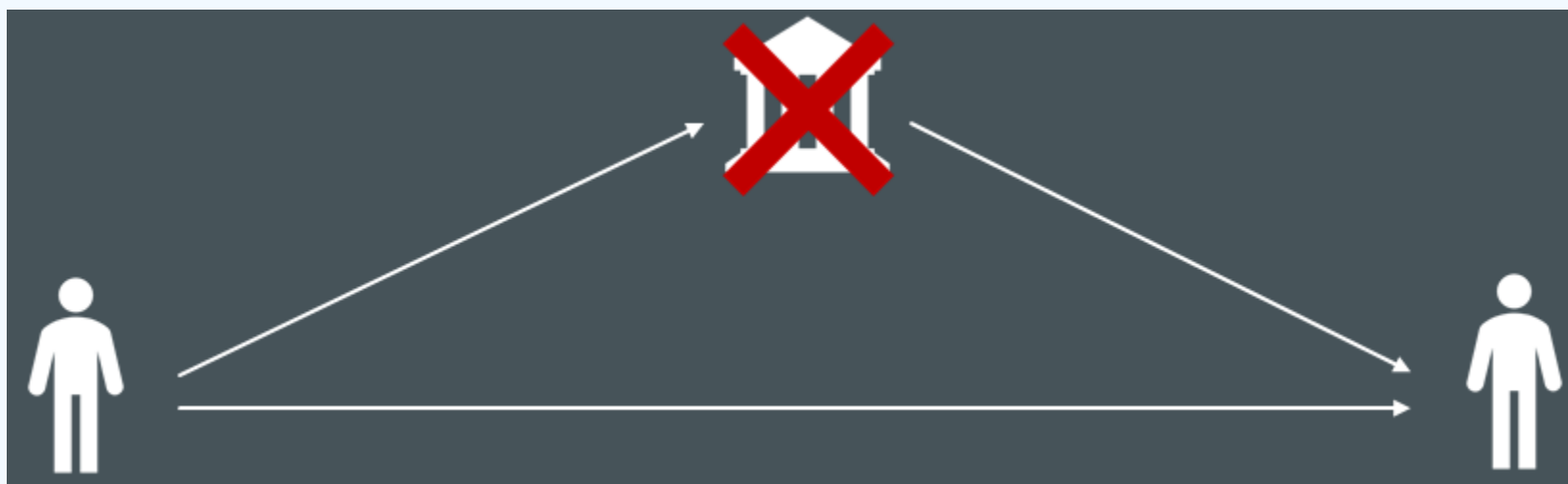
Bitcoin ≠ A “Blockchain”

- Diferenças
 - Bitcoin = is an application of blockchain technology
 - Blockchain = Is the underlying datastructure, which can be used for many things, including cryptocurrencies
- Bitcoin
 - A public network in which anyone can participate without restriction (including a malicious participants)
 - Not organized by a central authority



Ecosistema do Bitcoin

Ausência de Intermediação



Construção do consenso



Testemunhas



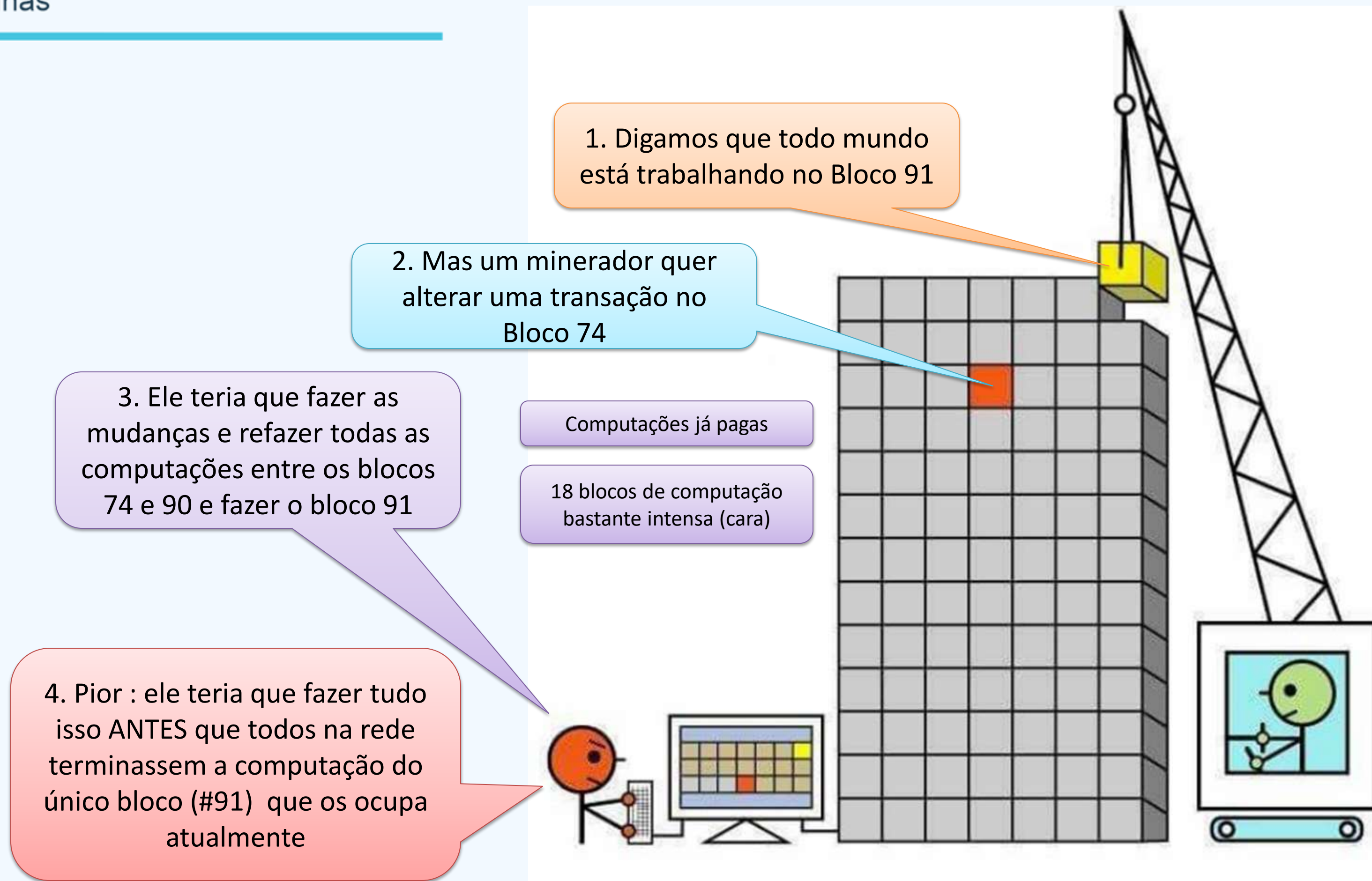
Características Chave

- Escrita, imutável, armazenamento de dados transparente
- Descentralizada, sem intermediários
- Consistência entre todos os participantes
- Resistente contra participantes maliciosos
- Aberta

Desafios

- Consumo de energia
- Escalabilidade
- Prevenção à lavagem de dinheiro
- Responsabilidade pessoal

Por que é tão difícil “quebrar” (cheat) o Bitcoin?



Tópico :

BLOCKCHAIN

Blockchain : muitos significados

“To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general.” (The Trust Machine, THE ECONOMIST, Oct. 31, 2015)

O que é Blockchain?

- Tecnologia que :

- Permite transações armazenadas, organizadas e disponibilizadas
- Encadeia blocos em ordem cronológica por criptografia
- Permite o ledger resultante ser acessado por diferentes servidores

Um método de armazenamento de dados em seções discretas (blocos) que são vinculadas.

Blockchains especificam critérios para quais dados podem ser armazenados em um bloco e rejeitam dados inválidos.

A submissão de blocos a uma blockchain descentralizada é regida por seu mecanismo de consenso.

Uma série de blocos que são unidos usando assinaturas criptográficas.

Devido ao uso de métodos de criptografia seguros e uma estrutura de banco de dados distribuída, as blockchains são úteis para proteger dados importantes, como criptomoedas.

Um livro digital composto por dados imutáveis e gravados digitalmente em pacotes chamados blocos.

Cada bloco é “encadeado” ao próximo bloco usando uma assinatura criptográfica.

Evolução



BLOCKCHAIN

1.0

Moedas



BLOCKCHAIN

2.0

Contratos

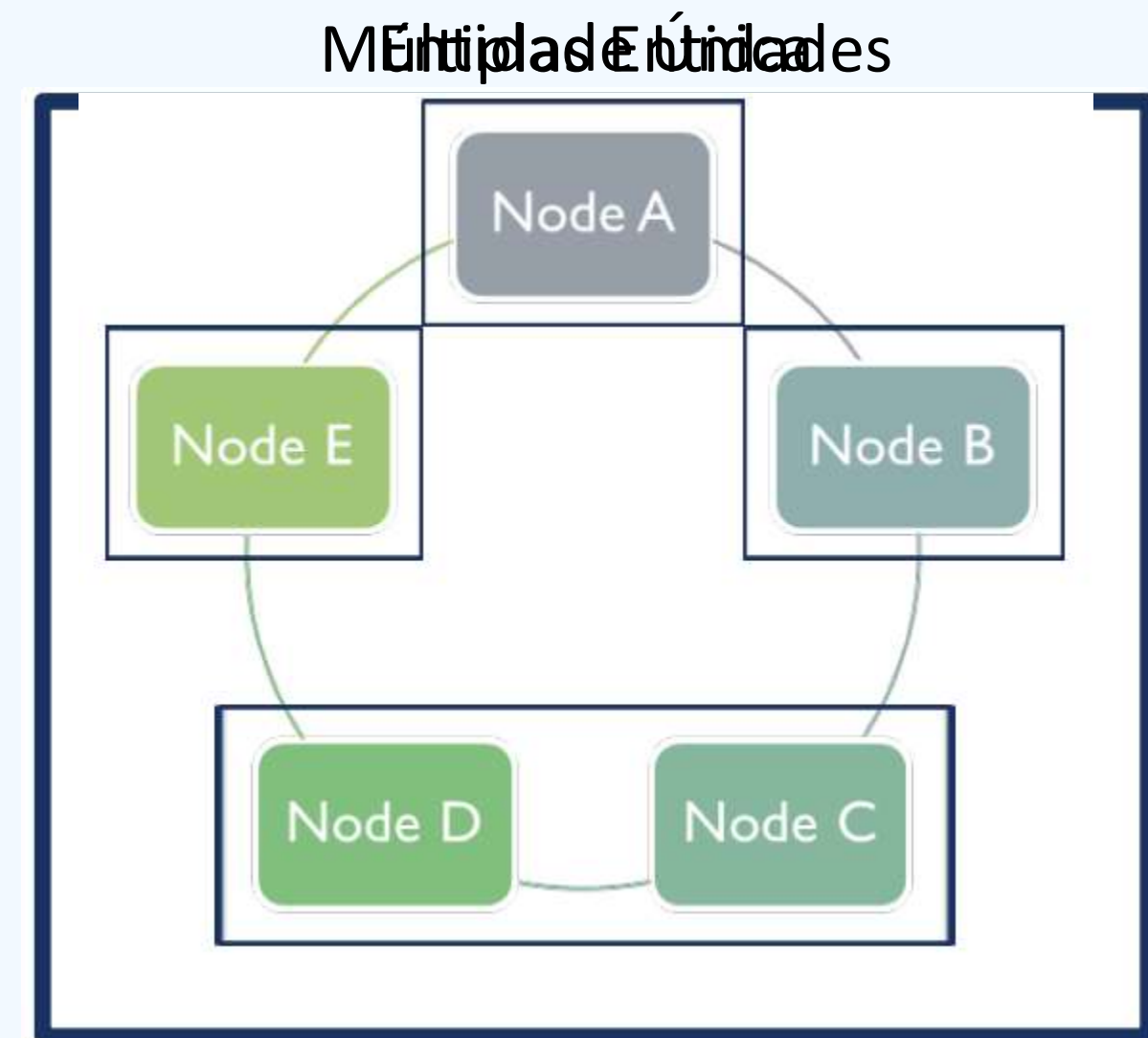
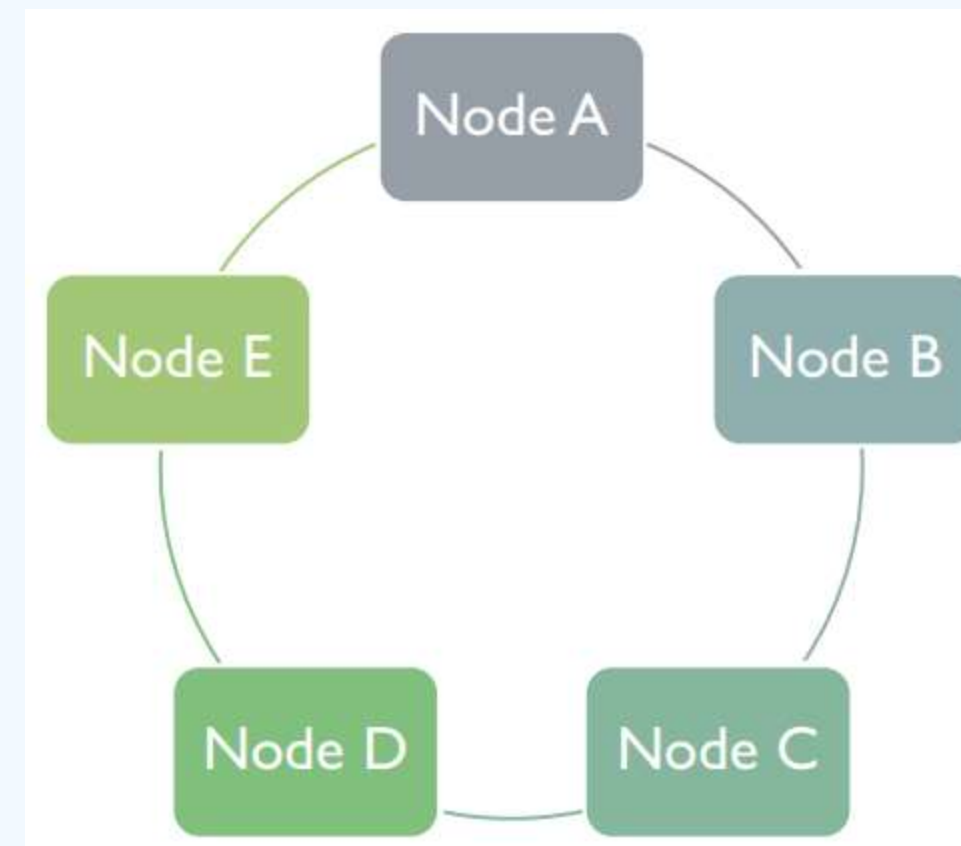
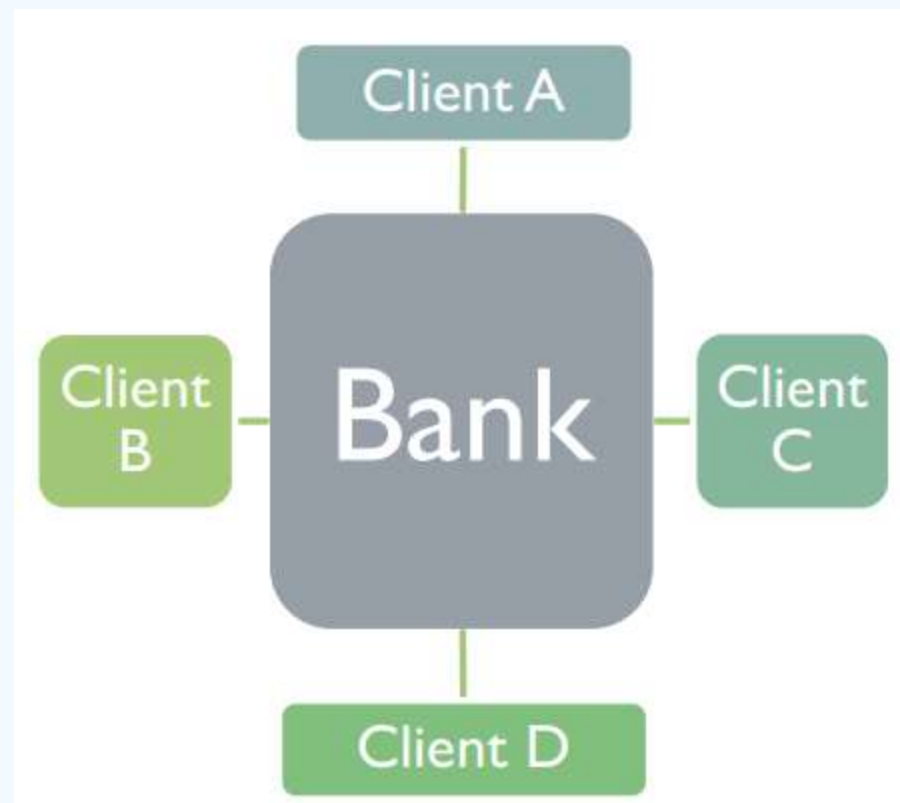


BLOCKCHAIN

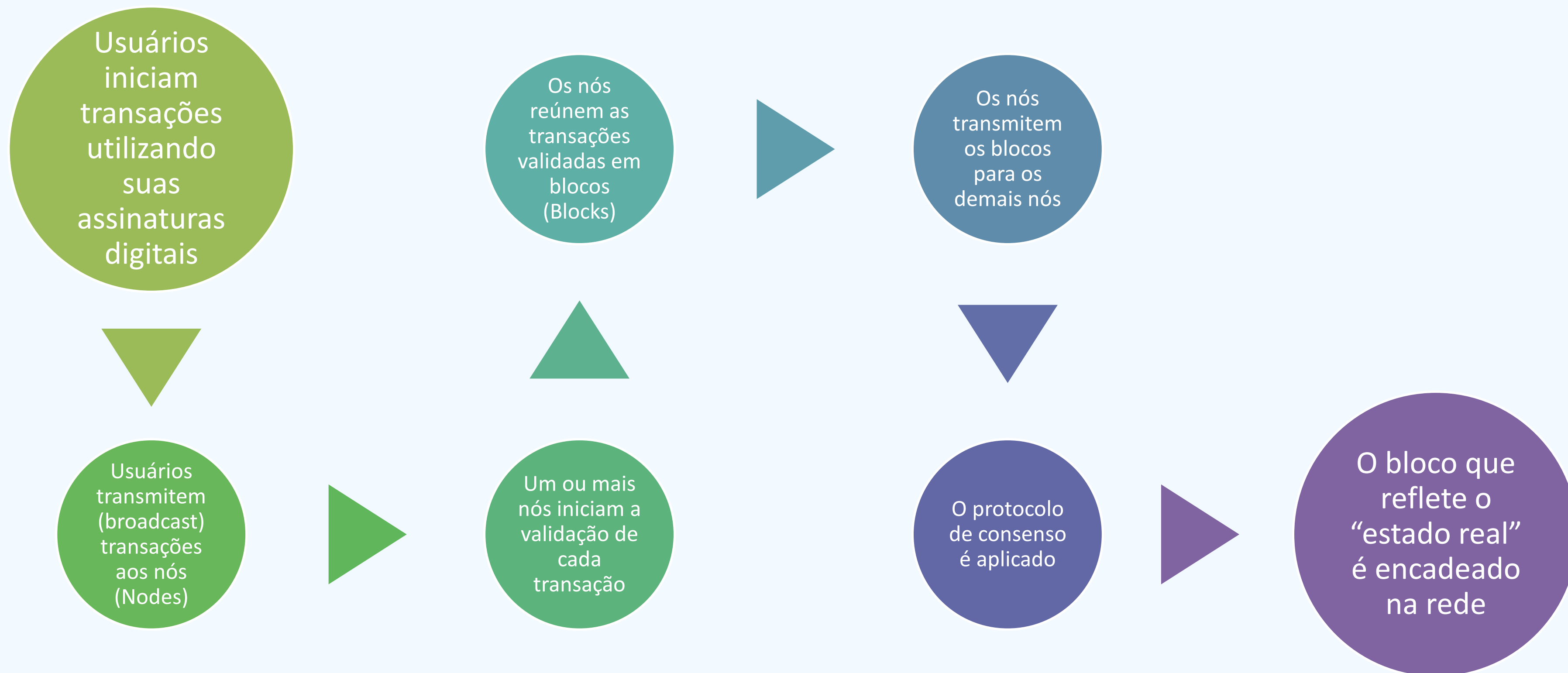
3.0

Sidechains

Distributed Ledger



Distributed Ledger : Funcionamento



Onde criptografia é aplicada?

Inicialização e Transmissão das Transações

- Assinaturas Digitais
- Chaves pública/privada

Validação das Transações

- Consenso

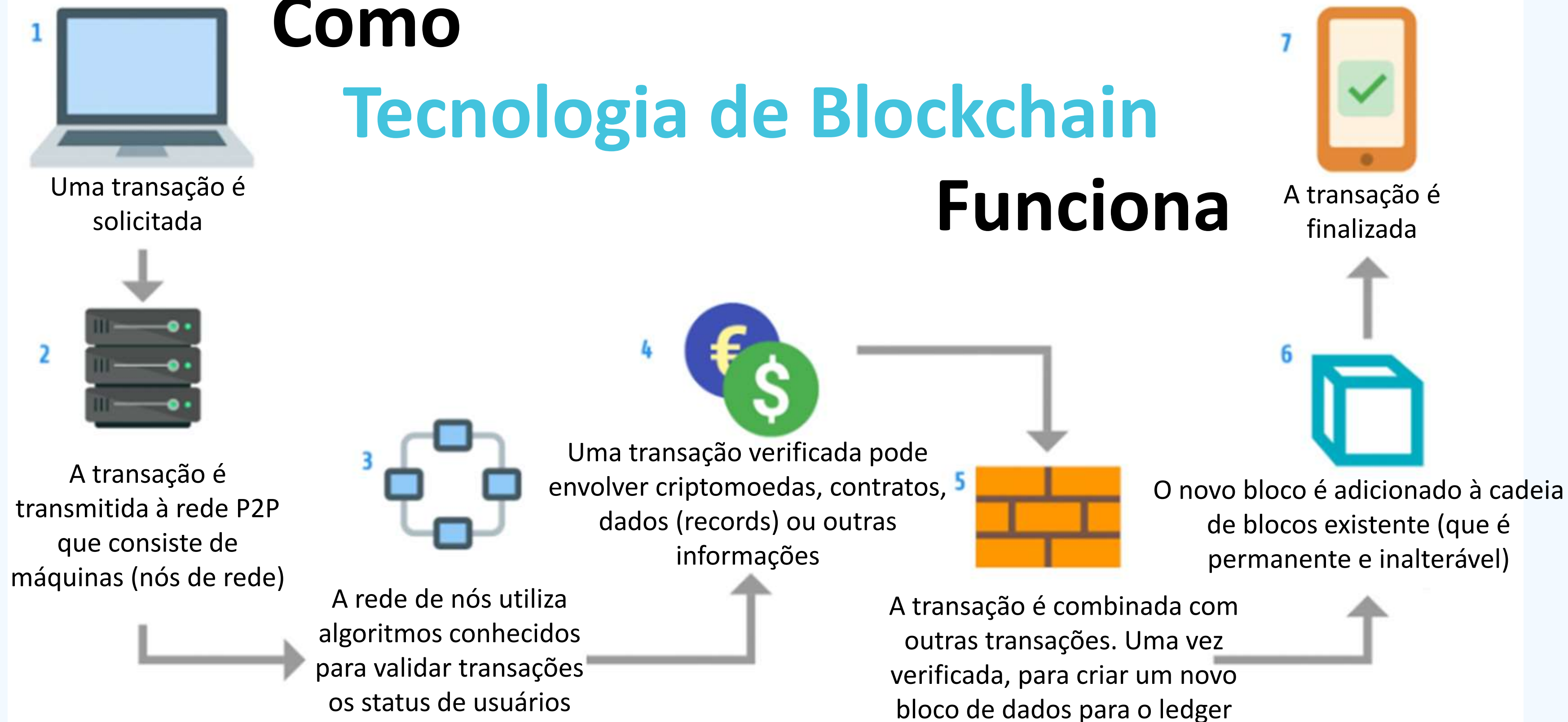
Encadeamento dos Blocos

- Funções de Hashing

*Delegação

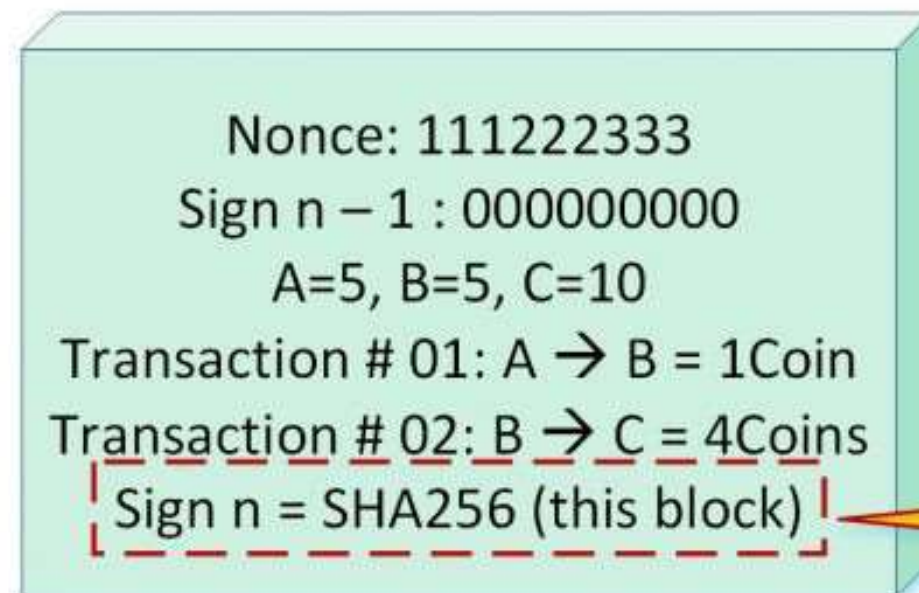
- Atribuição de poder

Como Tecnologia de Blockchain Funciona

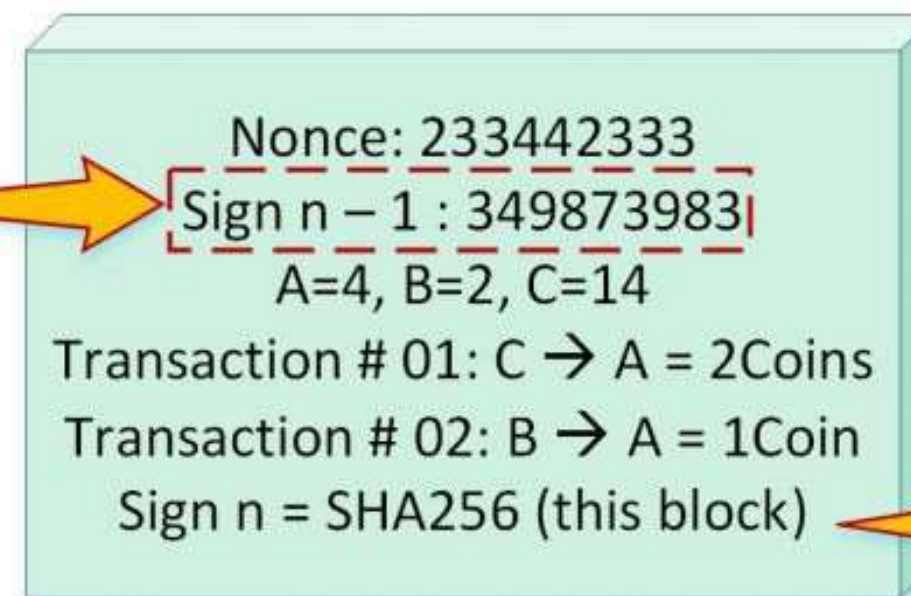


Como transações ocorrem

Genesis Block 0

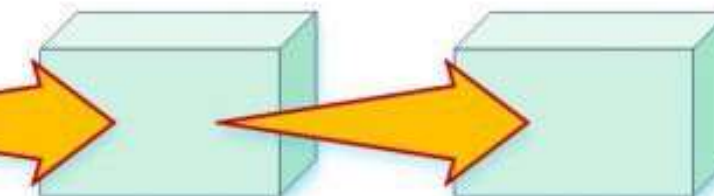


Block 1



Block 2

Block 3



[3]

- O nonce é um número arbitrário aleatório ou pseudoaleatório de 32 bits atribuído pelo minerador a cada bloco para garantir que a comunicação antiga não seja repetida.
- Pode ser usado como um vetor de inicialização de funções de hash criptográfico.

[4]

- O valor do sinal n -1 para o bloco de gênese é 0, porque o sinal n denota o valor de hash do bloco anterior, que não é nenhum para o bloco de gênese.
- Quando passarmos para o bloco 1, o sinal n será considerado para o bloco 1 e terá o valor de hash do bloco anterior (bloco 0), o mesmo será para o próximo bloco e assim por diante.

[5] Agora, o usuário A tem quatro moedas, o usuário B tem duas moedas e o usuário C tem quatorze moedas.

- O valor de hash para o bloco genesis será calculado usando o algoritmo SHA-256 para garantir a integridade do bloco.
- Agora, movendo-se para o bloco 1, o valor "Nonce" e o valor "Sign n -1" devem ser calculados para este bloco.
- O valor do sinal n -1 exigirá o valor SHA-256 do bloco anterior (Bloco 0). As transações são salvas neste bloco da mesma forma que no bloco anterior.
- Por fim, o valor SHA-256 é calculado para este bloco e da mesma forma, a cadeia continua

Componentes de uma Blockchain

Nós (Nodes)

- Usuário/máquina dentro de uma arquitetura de blockchain
- Cada um possui uma cópia independente do ledger

Transações

- Menor unidade de um bloco de uma blockchain
- Serve como propósito da Blockchain

Blocos

- Estrutura de dados utilizada para manter um conjunto de transações
- Distribuídos para todos os nós da rede

Cadeia (Chain)

- Sequência de blocos em uma ordem específica

Mineradores

- Nós específicos que realizam processos de verificação antes de adicionar dados à estrutura viva da rede

Consenso

- Conjunto de regras e arranjos para realizar operações na blockchain

Tipos de Blockchain

Pública

Dados e acesso ao sistema disponíveis abertos

Bitcoin, Ethereum, Litecoin

Privada

Controlada por usuários de uma organização específica

Acesso por convite

Híbrida

Combinação de rede pública/privada

Dragonchain

Consortício (Federada)

Gerenciada por um conjunto de organizações ou nós, em vez de uma rede centralizada ou descentralizada.







Energy Web Foundation, Ripple

Características dos Tipos de Blockchain

(tipicamente)

Propriedade	Pública	Privada	Consortio
Determinação do consenso	Todos os mineradores	Nós de uma organização	Nós selecionados
Permissão de leitura	Público	Público ou restrito	Público ou restrito
Nível de imutabilidade	Quase impossível de adulterar	Potencialmente baixo	Potencialmente baixo
Eficiência (uso de recursos)	Baixo	Alto	Alto
Centralização	Não	Sim	Parcial
Consenso	Permissionless	Precisa de permissão	Precisa de permissão

Características/ Benefícios do uso da Blockchain

-  Consenso de informação entre múltiplas partes
-  Time Stamping : eventos com informações temporais validadas pela rede
-  Segurança : encriptação e verificação permitem participantes não confiáveis compartilharem informação segura com terceiros
-  Autenticidade : assinaturas digitais provêm autenticidade e não-repudio
-  B2B Ownership : Ciclos de vida end2end incluindo ownership, custódia e proveniência podem ser rastreados
-  Proteção contra Perda de Dados : perda de dados universal se torna um problema de menor importância

Consenso

- Na indústria de blockchain, o **processo pelo qual seções distintas de uma rede determinam uma única verdade**.
- As redes Blockchain usam algoritmos de consenso para estabelecer um acordo sobre quais blocos devem ser adicionados à cadeia e quais nós são válidos.
- O processo usado por um grupo de pares, ou nós, em uma rede blockchain para concordar com a validade das transações submetidas à rede.
- Mecanismos de consenso dominantes :
 - Proof of Work (PoW) e Proof of Stake (PoS).
- Mecanismo: O processo usado para validar uma transação em uma rede blockchain distribuída projetada para atingir a tolerância a falhas bizantinas.
- **Byzantine Fault Tolerance (BFT)**
 - Uma propriedade de um sistema distribuído e descentralizado para resistir a falhas completas, mesmo quando alguns dos nós falham ou agem maliciosamente.

Mecanismos de Consenso

Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Authority (PoA)

Proof of Burn (PoB)

Proof of Capacity (PoC)

- No PoW, dados de transação (bloco) + sequências aleatórias de dígitos (nonce de bloco) são aplicados repetidamente a uma fórmula matemática (hashing) pelos mineradores, até que um resultado desejável seja encontrado (a prova de trabalho).
- Outros mineradores então verificam a prova de trabalho pegando a suposta string de entrada e aplicando-a às mesmas fórmulas para ver se o resultado é de fato o que foi apresentado.
- Se os resultados forem os mesmos, a transação é verificada e adicionada ao blockchain.
- Como muitos mineradores estão correndo para resolver a fórmula que exige muito poder de computação, o PoW consome muitos recursos.

Mecanismos de Consenso

Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Authority (PoA)

Proof of Burn (PoB)

Proof of Capacity (PoC)

- No PoS, os mineradores colocam (ou seja, "aposta") algumas das criptomoedas do blockchain (por exemplo, ether para o blockchain Ethereum) para aumentar suas chances de serem selecionados para validar um bloco.
- A participação é bloqueada como um depósito para garantir que o minerador valide o bloco de acordo com as regras.
- Se o minerador violar as regras, o depósito será "queimado" ou destruído.
- O PoS consome menos recursos do que o PoW, pois menos mineradores estão concorrendo para resolver a fórmula matemática.

Mecanismos de Consenso

Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Authority (PoA)

Proof of Burn (PoB)

Proof of Capacity (PoC)

- PoA é uma forma alternativa ao algoritmo PoS.
- Em vez de apostar em criptomoeda (riqueza), no PoA você aposta sua identidade.
- Isso significa divulgar voluntariamente quem você é em troca do direito de validar bloqueios.
- Quaisquer ações maliciosas que você realizar como validador refletirão na sua identidade.
- As blockchains PoA exigem uma forma completa de KYC (Know Your Customer - um processo de verificação que determina que você realmente é quem afirma ser).

Mecanismos de Consenso

Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Authority (PoA)

Proof of Burn (PoB)

Proof of Capacity (PoC)

- O PoB permite que os mineradores “queimem” ou destruam criptomoedas, o que lhes concede o direito de adicionar blocos na proporção das moedas destruídas.
- Os mineradores queimam moedas/tokens para comprar plataformas de mineração virtuais que lhes dão o poder de minerar blocos.
- Quanto mais moeda for queimada pelo minerador, maior será a plataforma de mineração virtual resultante.
- Para queimar, os mineradores enviam moeda para um endereço comprovadamente impossível de ser gasto.
- Esse processo não consome muitos recursos, portanto, o PoB é frequentemente chamado de PoW sem desperdício de energia.
- Dependendo da implementação, os mineradores podem queimar a moeda nativa ou a moeda de uma cadeia alternativa e, em troca, recebem uma recompensa na moeda nativa do blockchain.

Mecanismos de Consenso

Proof of Work (PoW)

Proof of Stake (PoS)

Proof of Authority (PoA)

Proof of Burn (PoB)

Proof of Capacity (PoC)

- O PoC permite que os dispositivos de mineração na rede usem seu espaço disponível no disco rígido para decidir os direitos de mineração, em vez de usar o poder de computação do dispositivo de mineração (como no PoW) ou a participação do minerador na criptomoeda (como no PoS).

Proof of Work

vs.

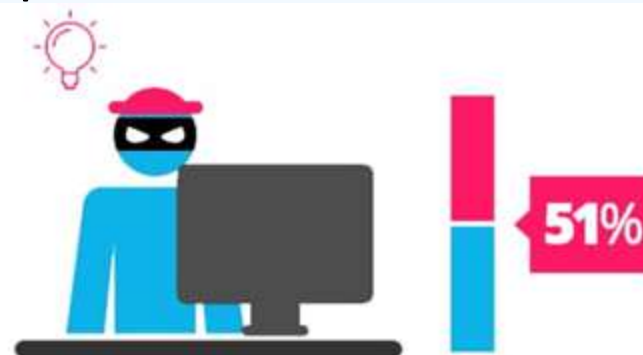
Proof of Stake



Para adicionar cada bloco à cadeia, mineradores competem para resolver um quebra-cabeças complexo utilizando seu poder computacional



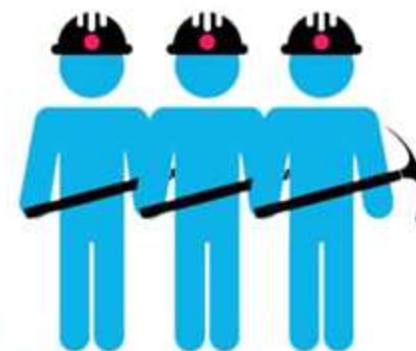
Não há competição, visto que o criador do bloco é escolhido baseado na quantidade de moedas em stake



Para submeter um bloco malicioso, o usuário teria que ter poder computacional maior que 51% de toda a rede



Para submeter um bloco malicioso, usuário teria que possuir (para entregar em stake) 51% de todo supply de moedas da rede



O primeiro minerador a resolver o quebra-cabeças recebe uma recompensa pelo trabalho



Não há recompensa por construir o bloco, mas o criador do bloco recebe uma taxa por transação

<https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

Mecanismos de Consenso

Consensus	POP	POW	POS	POA	POSA	DPOS	BFT	POH
Name	Proof of Performance	Proof of Work	Proof of Stake	Proof of Authority	Proof of Staked Authority	Distributed Proof of Stake	Byzantine Fault Tolerance	Proof of History
Transaction speed	fast	slow	medium	fast	fast	fast	medium	fast
consensus finality	fast	slow	fast	fast	fast	fast	Near Instant	fast
Hardware acceleration	yes	no	no	no	no	no	no	no
Security	high	high	medium	low	medium	medium	low	medium
Scalability	large	large	medium	medium	low	small	small	large
Server CPU resources	Low	High	medium	medium	medium	medium	medium	medium
Example Chains	HPB	Bitcoin, Ethereum	Cardano	Vechain	BSC	EOS, Tron	Avalanche	Solana

Blockchain : Benefícios Técnicos

Transparência

Coordenação sobre bancos de dados compartilhados

Censorship e resistência à fraude

Resiliência de dados

- Dados (records), detalhes de transações e processos são abertos e visíveis publicamente

Blockchain : Benefícios Técnicos

Transparência

Coordenação sobre bancos de dados compartilhados

Censorship e resistência à fraude

Resiliência de dados

- As partes podem compartilhar banco de dados como única fonte de verdade
- A criptografia fornece confiança na integridade do registro de dados
- Coordenação entre concorrentes, fornecedores da indústria, reguladores, etc. no mesmo sistema

Blockchain : Benefícios Técnicos

Transparência

Coordenação sobre bancos de dados compartilhados

Censura e resistência à fraude

Resiliência de dados

- Ausência do administrador central reduz a censura e a oportunidade de fraude

Blockchain : Benefícios Técnicos

Transparência

Coordenação sobre bancos de dados compartilhados

Censorship e resistência à fraude

Resiliência de dados

- Redundância de dados em milhares de nós
- Fornece armazenamento de dados e continuidade do processo em caso de falha de hardware ou ataques externos

Blockchain : Deficiências Técnicas

Tempos de transação lentos

Confidencialidade/Privacidade dos Dados

Gestão de Acesso

Prontidão

- Mecanismo de consenso subjacente a bancos de dados descentralizados inerentemente mais lentos
- Redundância de dados: todos/muitos “nós” processam, sincronizam, baixam todas/muitas transações independentemente

Blockchain : Deficiências Técnicas

Tempos de transação lentos

Confidencialidade/Privacidade dos Dados

Gestão de Acesso

Prontidão

- Privacidade de dados reduzida e maior transparência em relação a bancos de dados centralizados (potencial/risco de mais acesso por outros)

Blockchain : Deficiências Técnicas

Tempos de transação lentos

Confidencialidade/Privacidade dos Dados

Gestão de Acesso

Prontidão

- Chaves privadas podem ser necessárias como “senhas” para usar contas e enviar transações
- Gerenciamento de chaves difícil
- Revogação de chave não facilitada
- Disseminação difícil

Blockchain : Deficiências Técnicas

Tempos de transação lentos

Confidencialidade/Privacidade dos Dados

Gestão de Acesso

Prontidão

- DLTs (Distributed Ledger Technologies) muito em desenvolvimento para atender às necessidades de segurança, escalabilidade e velocidade de transação

Tópico

ETHEREUM, HYPERLEDGER

Ethereum

- Funciona como uma plataforma através da qual as pessoas podem usar tokens para criar e executar aplicativos e criar contratos inteligentes
- Ethereum permite que as pessoas se conectem diretamente através de um poderoso supercomputador descentralizado
- Linguagem – Solidity / Vyper
- Moeda – Ether
- Consenso : 1.0 \leftarrow PoW (2.0 \leftarrow PoS)

Hyperledger


























































O Hyperledger é um esforço colaborativo de código aberto criado para avançar as tecnologias blockchain entre indústrias. É uma colaboração global, hospedada pela The Linux Foundation, incluindo líderes em finanças, bancos, Internet das Coisas, cadeias de suprimentos, manufatura e tecnologia.



Tópico

BLOCKCHAIN : CASOS DE USO

Alguns Casos de Uso da Blockchain

 CURRENCY	 EXCHANGE	 FINANCE	 TRADING	 E-COMMERCE	 SUPPLY CHAIN	 PAYMENT	 DIAMONDS	 CRM DATA	 CROWD FUNDING
 HOTEL BOOKING	 CHARITY	 CAR LEASING	 LAW & LEGAL	 FORECASTING	 CYBER SECURITY	 HEALTHCARE	 SMART CONTRACTS	 IOT PROTECTION	 CAR SECURITY
 GOVERNMENT	 MEDIA	 BANKING	 DAIRY	 PHARMA	 WATER	 DIGITAL KYC	 OIL & GAS	 TOURISM	 INSURANCE
 SCHOOLS	 MANUFACTURING	 ADVERTISING	 FARM TO TABLE	 LENDING	 TRACKING	 REAL ESTATE	 CLOUD STORAGE	 AGRICULTURE	 TELCOM
 ENERGY	 GAMING	 FLIGHT TRACKING	 CERTIFICATES	 E-VOTING	 CAR SHARING	 DRONE FARMING	 PRIVACY	 FINANCING	 TRACING
 GREEN FARMING	 TIME TO MARKET	 SMART HOMES	 AVIATION	 SMART CITY	 COURIER	 SMART FARMS	 LOGISTICS	 SME INDUSTRY	 SECURE MESSAGING

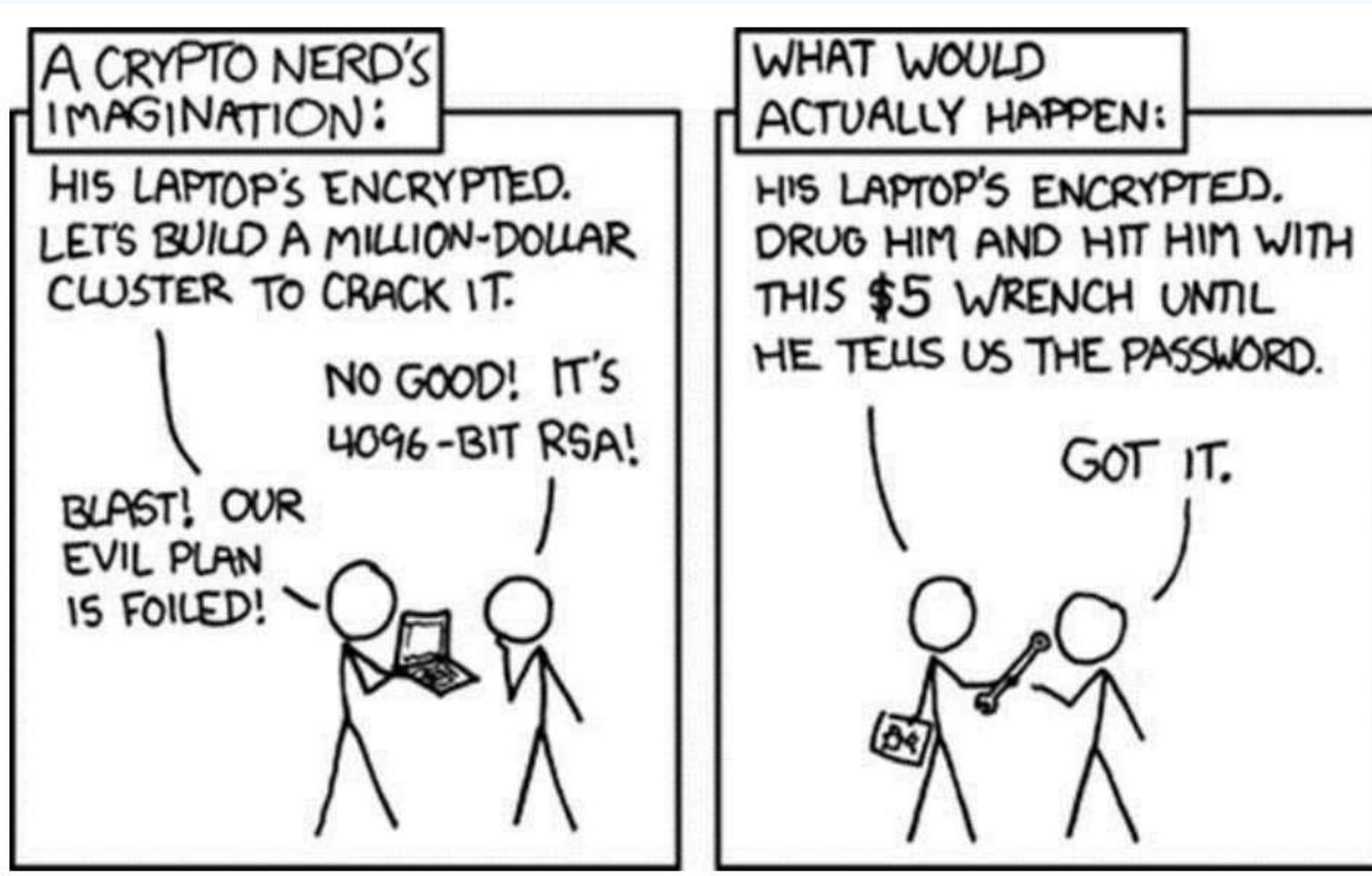
50+ BLOCKCHAIN REAL WORLD USES CASES



https://miro.medium.com/max/1400/1*cVeTQYLF5Z35yGoZ23Sfmw.png

Smart Contracts

- Nem contratos inteligentes nem legais
- Programas de computador auto-executáveis que facilitam a automação de transações e eliminam a necessidade de intermediários
- Permite que os pares em uma rede de contabilidade distribuída troquem valores sem risco de contraparte
- Os contratos inteligentes baseados em blockchain são visíveis para todos os usuários de um blockchain, o que significa que o código está aberto a vulnerabilidades
- Um contrato inteligente é um acordo ou conjunto de regras que regem uma transação comercial
- Ele é armazenado no blockchain e é executado automaticamente como parte de uma transação
- Seu objetivo é fornecer segurança superior ao direito contratual tradicional, reduzindo os custos e atrasos associados aos contratos tradicionais



source: xkcd.com/538