ESCOLA SUPERIOR DE REDES

Módulo 1
Trilha Blockchains Corporativos

GoLedger

O Valor das Coisas

Micronésia - 1700

Pedra Rai das ilhas Yapi (Micronésia)

Pedras Rai

- Variavam de 3 cm a 3 m de diâmetro
- Pesavam até 2 toneladas
- Pedras trazidas de outra ilha
- Pedra possuía uma história, transmitida oralmente de geração a geração
- Artefato com funções sociais e financeiras
- Oferecia ao proprietário status e riqueza.

Mundo - 2022

Bored Ape #2087 vendido em set/2021
por **U$ 2.307.638,00**

NFT

- Disponíveis em redes Blockchain públicas.
- Possui padrões digitais de propriedade e transferência.
- Conceitos digitais de exclusividade e escassez.
- Possuem uma história de proprietários.
- Artefato com funções sociais e financeiras.

Qual o valor das coisas?

Valor de troca

Valor de guarda

Valor de confiança

Valor de escassez

Valor utilitário

Valor cultural

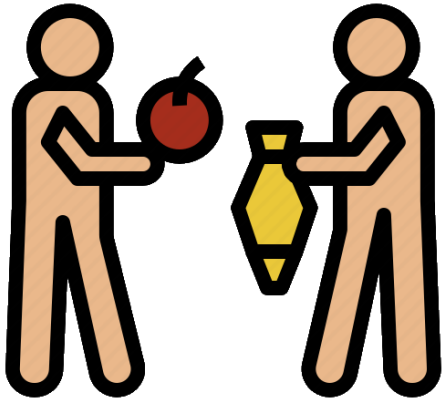
Valor social

Valor digital

Do livro-razão ao Blockchain

Ledger

- O **livro-razão** (**ledger** em inglês) representa uma registros de transações ordenadas cronologicamente.
- Os **ledgers** apareceram aproximadamente em 5.000 AC.
- Antes disso o ser humano **raramente possuía mais do que podia carregar** com eles, limitando o comércio ou troca entre os povos nômades a pequenas tribos ou aldeias.



* A partir de agora iremos chamar o livro-razão de **ledger**

Evolução do Ledger

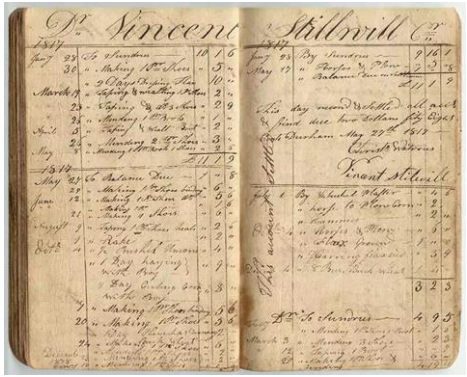
Primeiro

- Entrada única somente

Ledgers encontrados na babilônia

Segundo

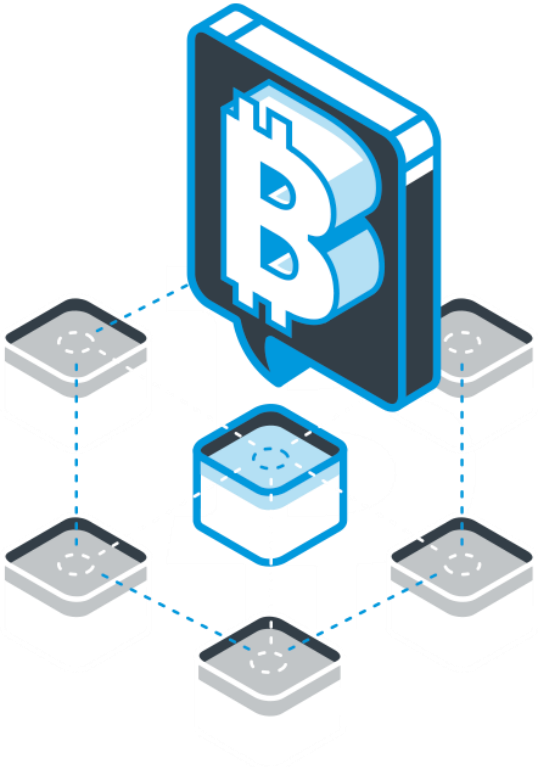
- Acompanhe débitos e créditos
- Conte a história de uma transação de ambos/todos os lados



Débitos à esquerda, Créditos à direita – a marca registrada da contabilidade de dupla entrada.

O **ledger** sempre foi utilizado pela humanidade para registro de **valores** e **propriedades**.

Bitcon e o Protocolo da Confiança



Em novembro de 2008, Satoshi Nakamoto lançou o paper

A peer-to-peer electronic cash system

Esse documento lançou os fundamentos de transações eletrônicas gravados em um **ledger distribuído** (rede peer-2-peer insegura) e criou a moeda/ativo/coisa que hoje conhecemos como **Bitcoin**

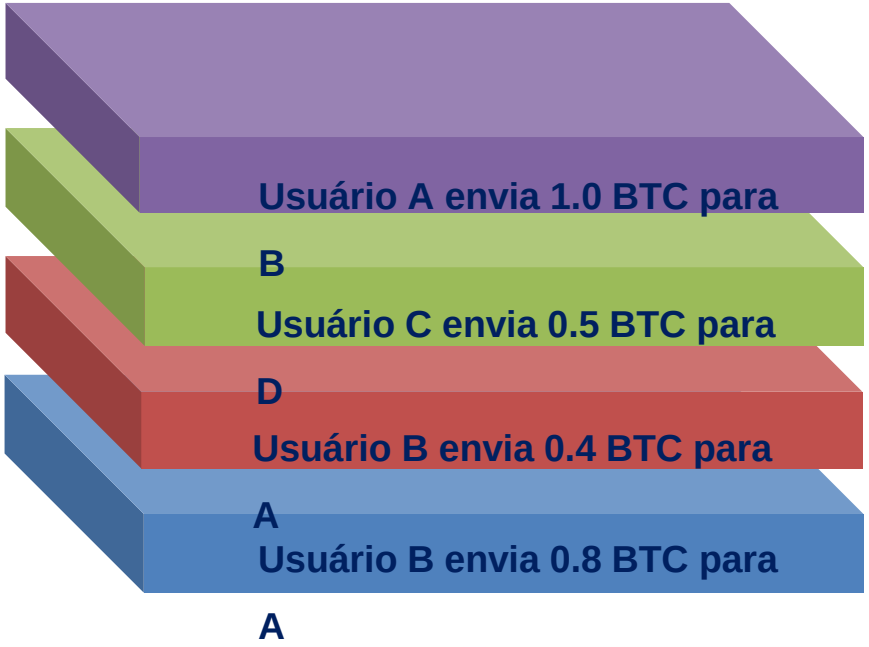
Bitcon e o Protocolo da Confiança

Usuário identificado pela sua chave pública

Senha é a sua chave privada

Transações são geradas no mundo e enviadas para a na tentativa de se tornarem operações válidas

Transações realizadas em uma rede peer-to-peer pública



A rede agrupa as transações em blocos possíveis de serem validad

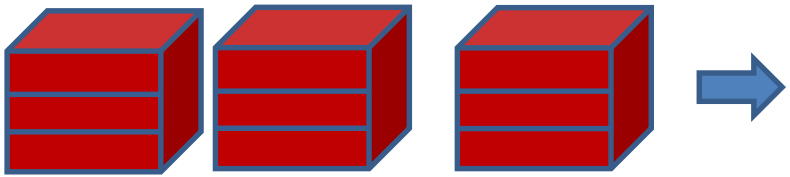
A idéia de Satoshi

Computadores chamados de “mineradores” competem na rede para agruparem as transações no próximo bloco válido.

Um algoritmo matemático similar a um processo de loteria é executado na rede. O minerador que resolver um problema matemático de alta complexidade tem o direito a incluir o próximo bloco.

O novo bloco é encadeado ao anterior através d encadeamento dos hashes

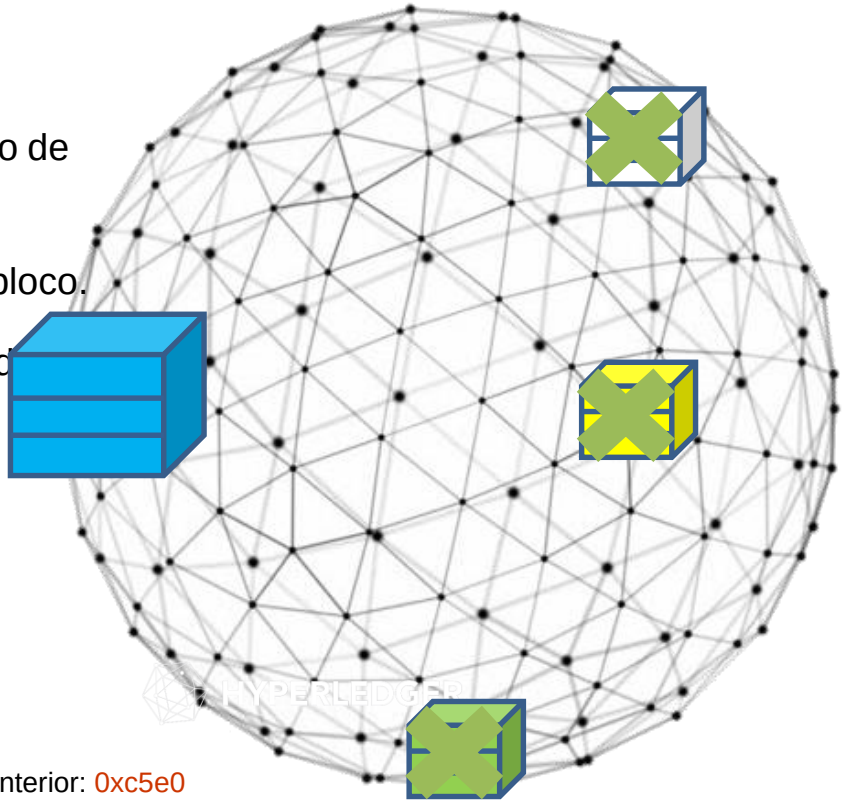
Recompensa para o minerador



0x…
0x59db

0x59bd
0x13fd

Hash anterior: 0x13fd
Hash atual: 0xc5e0



Hash anterior: 0xc5e0
Hash atual: 0xf632

Pela Primeira Vez na História, uma transação..

- Entre duas pessoas ou entidades que **NÃO** se conhecem nem se confiam
- Em uma rede que também **NÃO** é confiável

Foi realizada de forma 100% segura

Porque Satoshi foi Revolucionário

- **Ledger** digital público e distribuído
- Redes **peer-2-peer**
- **Assinatura** digital
- **Ativo** digital (Bitcoin) com conceitos de escassez.
- Validação de saldo em transações não gastas (**UTXO**)
- Consenso e resolução de fraudes com algoritmos utilizando teoria dos jogos (**mineração**)

Bitcoin ontem e hoje

- **2010:** 10.000 Bitcoins compraram **2 pizzas**
- 2022: 1 Bitcoin vale em torno de U$ 21.000
- Mais de **19 milhões** de Bitcoins já foram minerados **(21 milhões** no total**)**
- **Funções**
- Guarda de valor
- Investimentos financeiros
- Meio de pagamento
- Compra de ativos reais
- Garantia
- Moeda e reserva nacional (El Salvador)

Movimento CyberPunk/CypherPunk

- **High Tech – Low Life**
- Tecnologia que oprime pode ser usada para libertar
- A identidade de Satoshi Nakamoto nunca foi revelada
- **Hall Finney**
- Recebeu a primeira transação do Bitcoin
- “The computer can be used as a tool to liberate and protect people”

Ledger Público

- Lista de transações disponível para todas as partes.
- Podem ser não-permissionados ou permissionados (direito de escrita)
- Conta-corrente bancária– **ledger privado**

- Placar de um jogo de futebol – **ledger público**

Protegendo um Ledger Público

Você, Bob, Alice e Charlie querem mostrar pagamentos entre si.

Utilizam um **ledger** para fazer esse processo de registro/verificação.

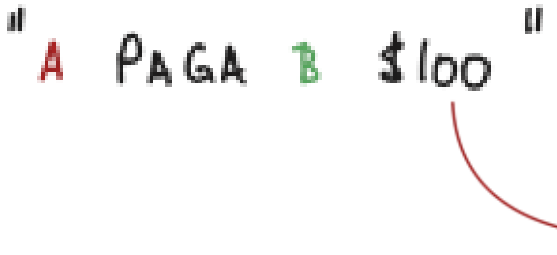
O **ledger** é uma sequencia de transações ordenadas cronologicamente.

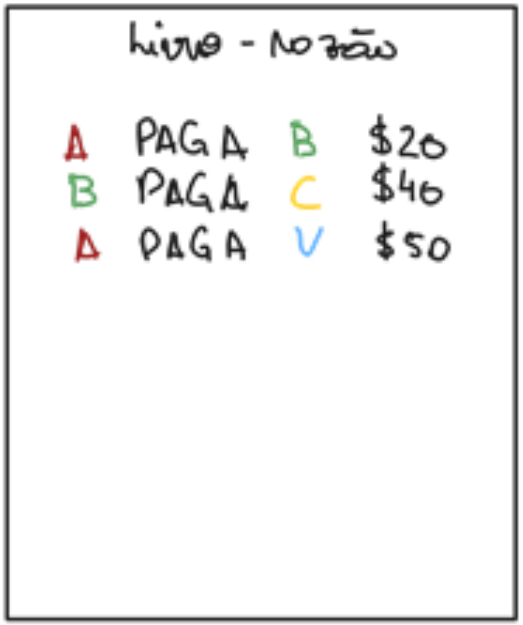
Qualquer um pode adicionar uma linha.

Disponível em lugar público (e.g. um site)

Protegendo contra fraudes

E se **Bob** tentar escrever em nome de **Alice**?





Assinaturas Digitais

Chaves: Chave Pública (*pk*)

Segredo (*sk*)

Funções: Sign(*conteúdo, sk*)

Verify(*conteúdo, assinatura, pk*):**boolean**

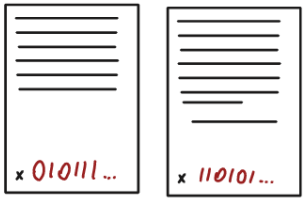
Documentos diferentes, assinaturas iguais.

256 bits

pk: 01001 ...
sk: 10100 ...
Alice

pk: 00101 ...
sk: 10010 ...
Bob

pk: 00010 ...
sk: 10011 ...
Charlie



Documentos diferentes, assinaturas diferentes.

Sign (Conteúdo , sk) = Assinatura

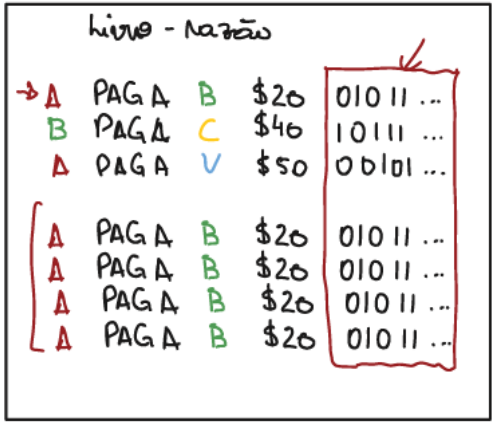
Verify (Conteúdo , Assinatura , pk) = true

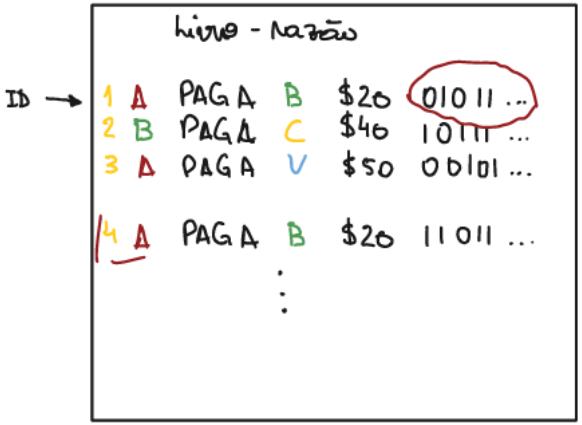
2^{256} assinaturas possíveis

impossível forjar

Assinando o mesmo conteúdo

O que impede **Bob** de copiar e colar uma linha com assinatura válida?





Adição de Ids para cada linha.

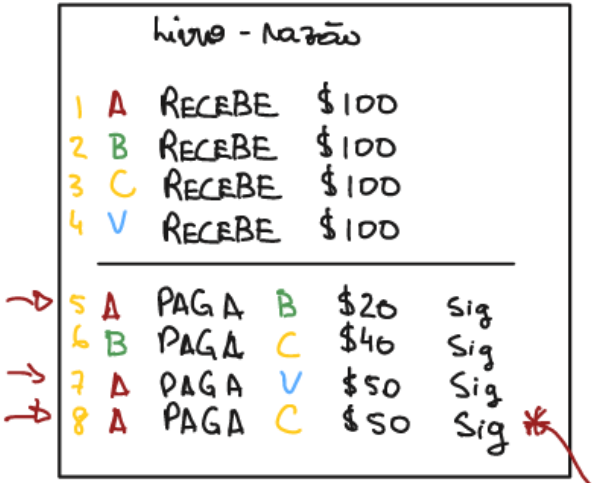
Protocolo até o momento...

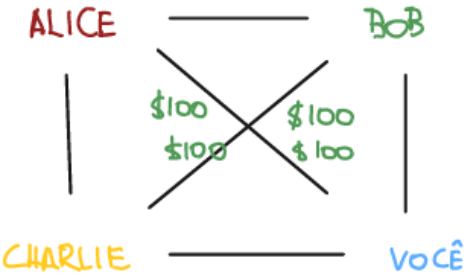
Todos podem adicionar linhas no **ledger**

Os débitos e créditos são acertadas ao final do mês.

Somente transações assinadas são válidas.

Como evitar que Alice gaste mais que tem?





Sem gastar mais do que tem!

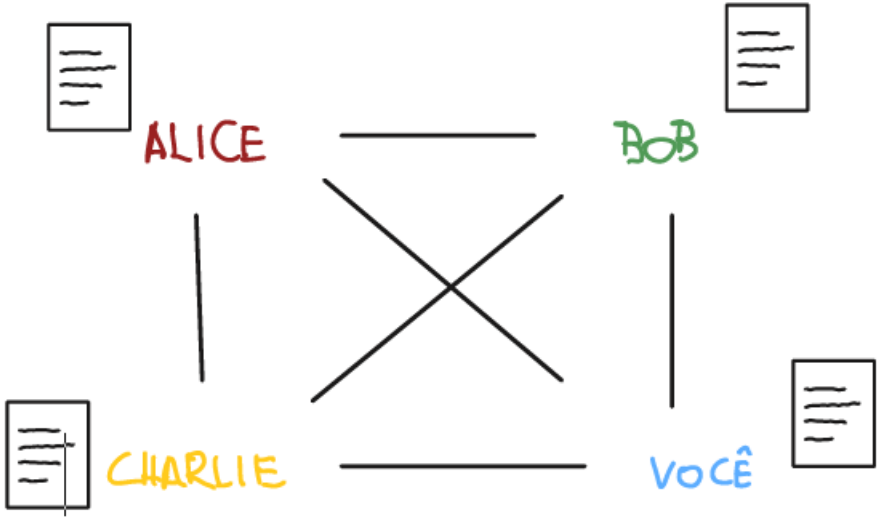
verificação do histórico.

E se todos quiserem o Ledger?

Confiança entre as partes.

Descentralizando a informação com **mensagens** entre as partes.

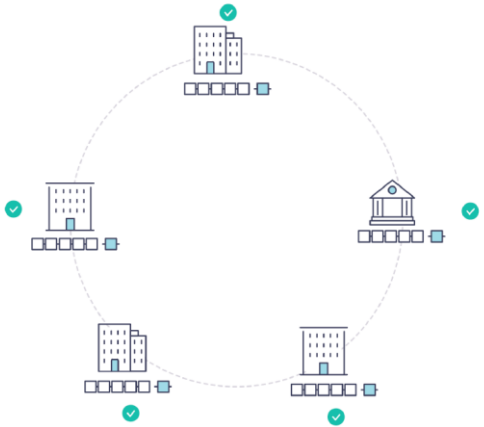
Alice, Bob, Charlie e Você recebem o ledger atualizado.

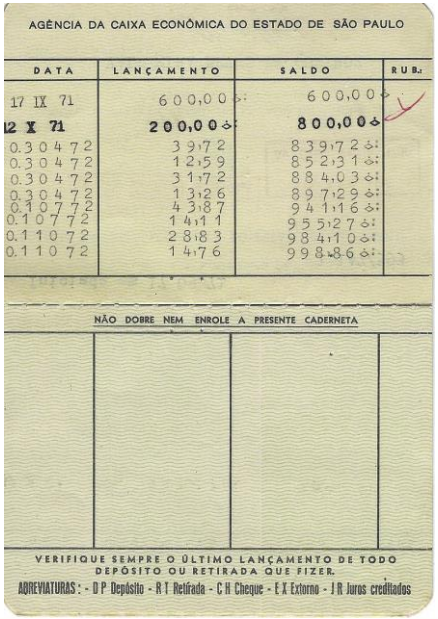


DLT – Distributed Ledger Tecnology

Cópias de um Ledger distribuído entre partes.

Relato de uso de DLT pelo sistema financeiro no **Império Romano**




AGÊNCIA DA CAIXA ECONÔMICA DO ESTADO DE SÃO PAULO

DATA	LANÇAMENTO	SALDO	RUB.
17 IX 71	600,00	600,00	
12 X 71	200,00	800,00	
0.30472	39,72	839,72	
0.30472	12,59	852,31	
0.30472	31,72	884,03	
0.30472	13,26	897,29	
0.10772	43,87	941,16	
0.10772	14,11	955,27	
0.11072	28,83	984,10	
0.11072	14,76	998,86	

NÃO DOBRE NEM ENROLE A PRESENTE CADERNETA

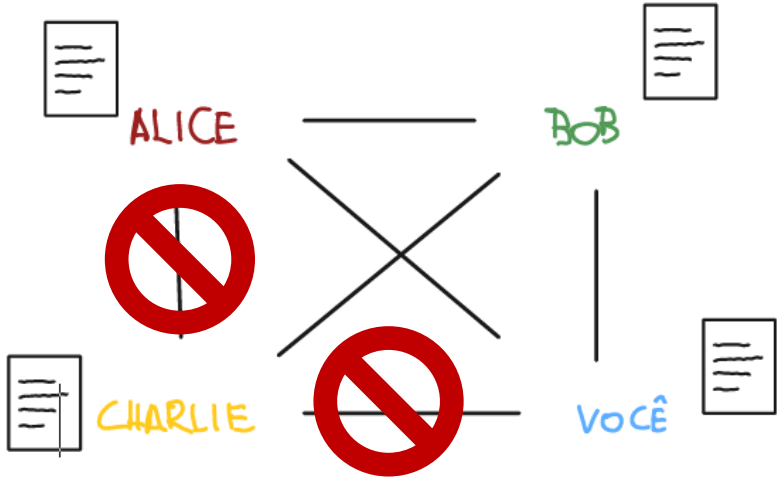
VERIFIQUE SEMPRE O ÚLTIMO LANÇAMENTO DE TODO DEPÓSITO OU RETIRADA QUE FIZER.

ABREVIATURAS: - D P Depósito - R T Retirada - C H Cheque - E X Extorno - J R Juros creditados

Como garantir que todos têm a mesma informação?

Mensagens comprometidas

Como controlar falhas e ataques durante o envio de informações entre as partes?



A resolução de problemas na sincronização deve ser resolvido por um protocolo de

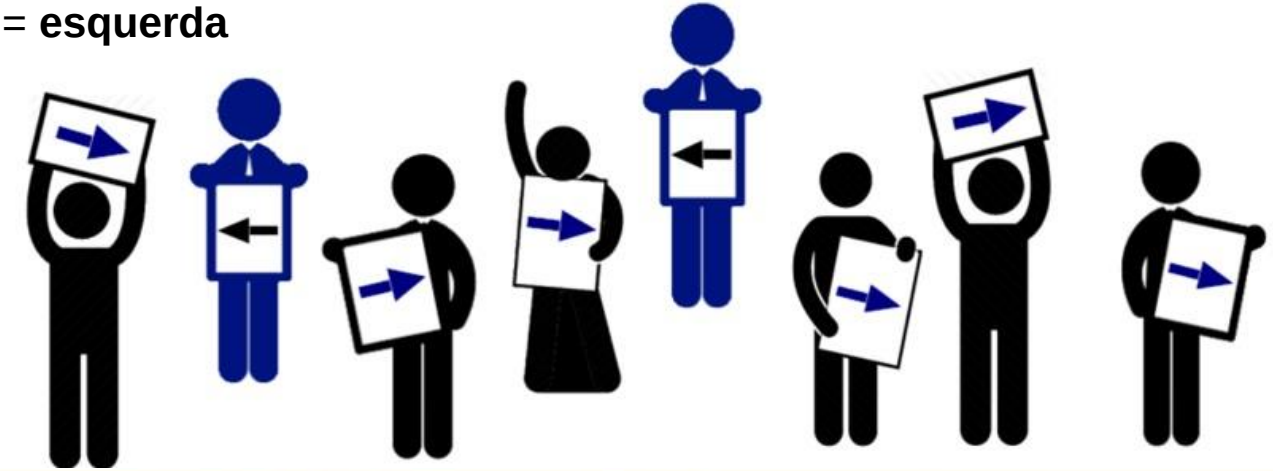
CONSENSO

Consenso

Imagine um grupo precisando de decidir se todos vão para a esquerda ou direita.

Consenso decisório 1: maioria simples = **direita**

Consenso de decisão 2: votos dos personagens azuis tem 3x mais poder de decisão que os outros = **esquerda**



Consenso = Confiança?

Mensagem

Mensagens e transações agrupadas em **blocos.**

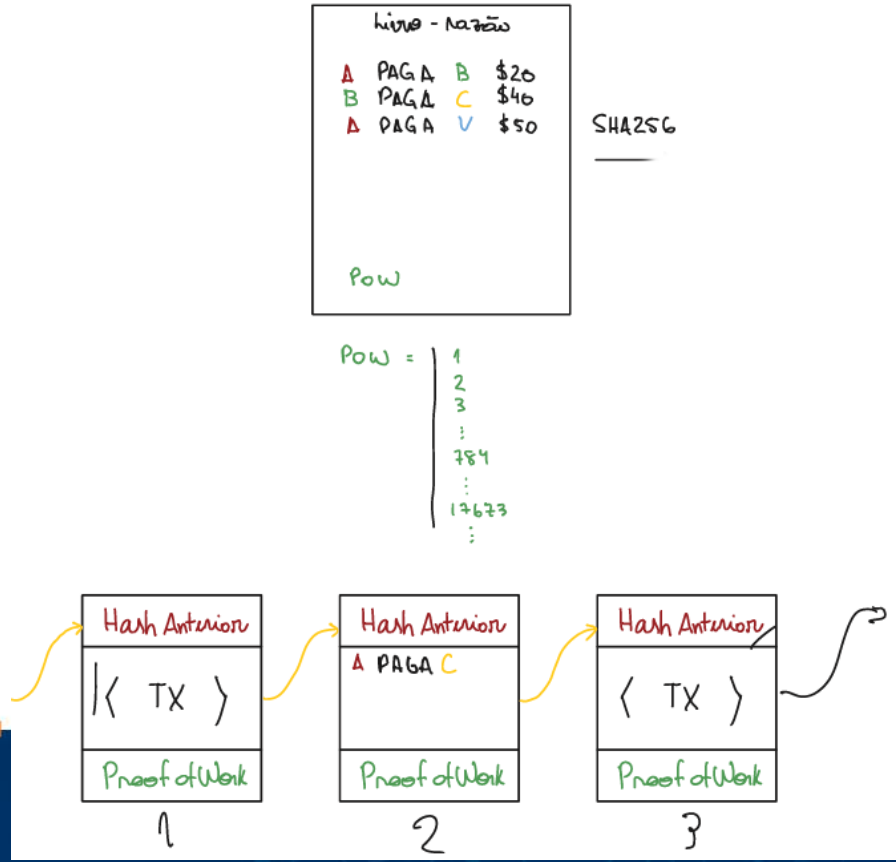
Regra de **consenso** decide a gravação do próximo bloco.

Consenso associa **tempo** e **trabalho** a resultados confiáveis.

Blocos conectados aos blocos anteriores por meio de **hashes.**

Alteração do conteúdo de qualquer bloco modifica os **hashes** do resto da cadeia.

DLT + Consenso + Blocos Conectados



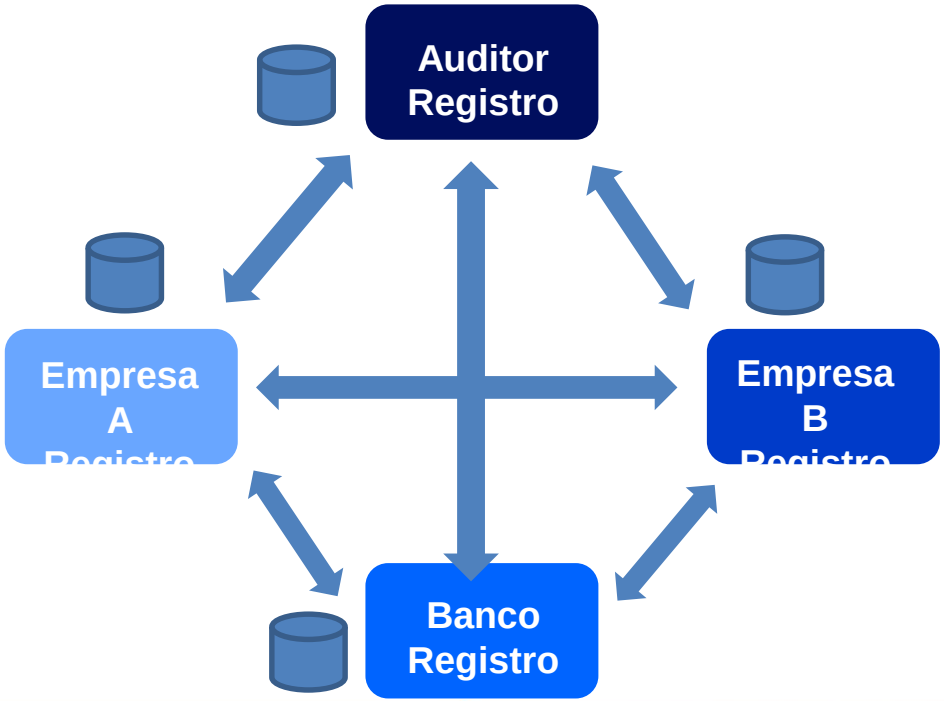
Protocolo da confiança digital

- **Ledger** digital público e distribuído
- **Compartilhamento** transações
- Transações **assinadas**
- **Consenso** para resolução de disputas

BLOCKCHAIN

Modelo Cliente Servidor Web1 Web2

Modelo Cliente Servidor



Cada entidade mantém seus próprios registros

- Separe bancos de dados e ledgers
- Formatos e ferramentas exclusivos
- Duplicação de esforço para manter informações

Requer intermediários

- Danos em registro e liquidação
- Segurança desconhecida dos sistemas
- Sistema comprometido afeta confiança

Precisa de APIs, autenticação

- Conversões de formato e dados
- Diferenciando informações em ledgers

Livro-Razão da Contratação de Serviço - Tradicional

Avaliação

Faturamento

Boletim de Medição

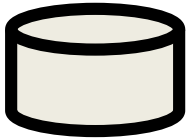
Contratação

Análise de Preços

Solicitação

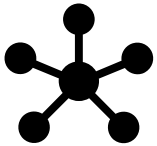
Quando um livro-razão é armazenado em um ponto único, uma fraude pode ser realizada apenas modificando uma página do livro-razão.

Deficiências do Padrão Centralizado

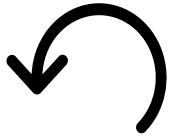


Qualquer **consulta** necessita de um acesso à **base** de dados **centralizada**, que nem sempre está **disponível**.

A realização de qualquer **auditoria** interna ou externa normalmente feita de forma **pontual** e **esporádica**, sem possibilidades de auditorias em **tempo real.**



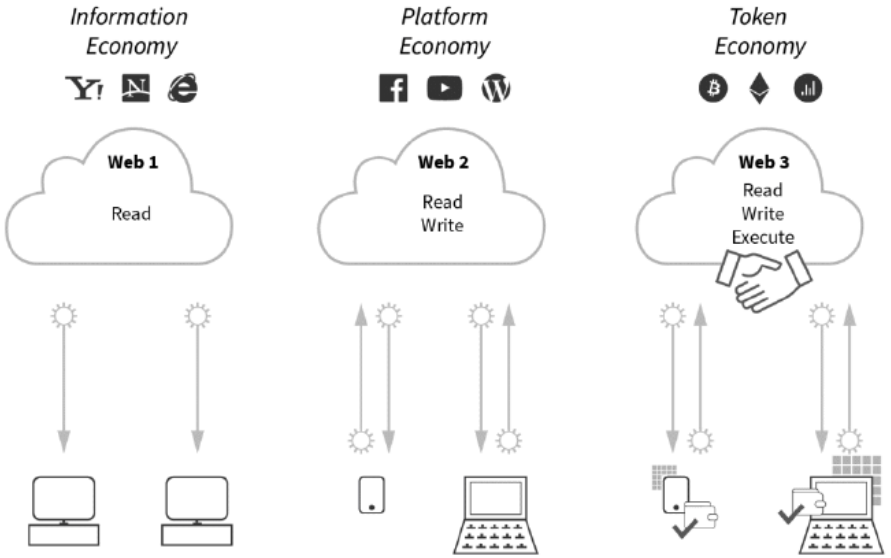
Integração de **bases** de dados centralizadas de órgãos diferentes, utilizam-se **VPNs** e novas **Web APIs**, que trazem as mesmas dificuldades: **disponibilidade** e **escalabilidade**.



Os sistemas **legados** dos diversos participantes têm **dificuldade** manter a **unicidade** e **sincronização** das informações entre os dados **locais** e os dados presentes nas bases **remotas**.

Web3 e a Sociedade Blockchain

História da Web



Web 1: hello world

- Protocolo HTTP, browsers e engine de buscas

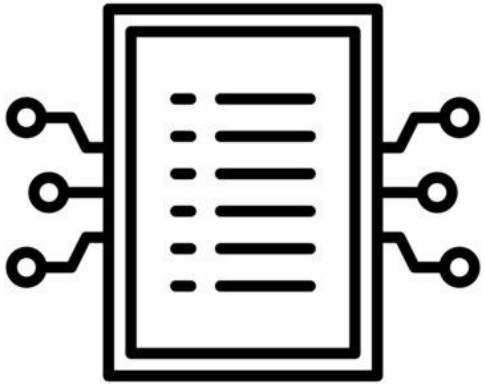
Web 2: frontend revolution

- Media social, e-commerce, mobile banking

Web 3: backend revolution

- Smart contracts, tokens

Sociedade Programável



Agentes automatizados

- Decisões independentes de ações humanas

Regulação

- Autorização legal para tomar decisões digitalmente

Inovação

- IoT, IA

Sociedade Distribuída

Informações distribuídas

- Dados enviados entre bancos de dados e organizações

Processos

- Portabilidade, Indústria 4.0

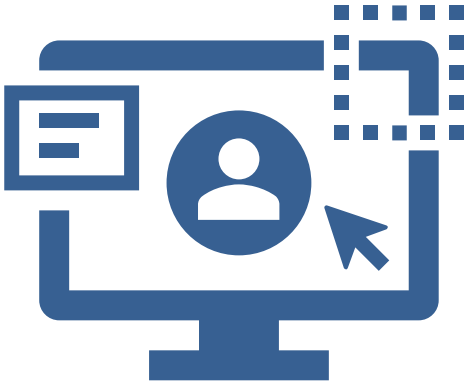
Sistemas

- IPFS, Torrent, Content Delivery (CDN)

Inovação

- BigData, Edge Computing

Sociedade AutoSoberana



Credenciais de uma indivíduo

- O desafio de provar que uma pessoa é ela mesma.
- Silos de crendenciais: Meta (Facebook), Google
- Brokers de credenciais de acesso
- Biometria

Consentimento

- Trilha de auditoria de consentimento, LGPD, GDPR

AutoSoberania

- O indivíduo tem controle sobre as suas credencias de acesso.

Sociedade Distribuída

Informações distribuídas

- Dados enviados entre bancos de dados e organizações

Processos

- Portabilidade, Indústria 4.0

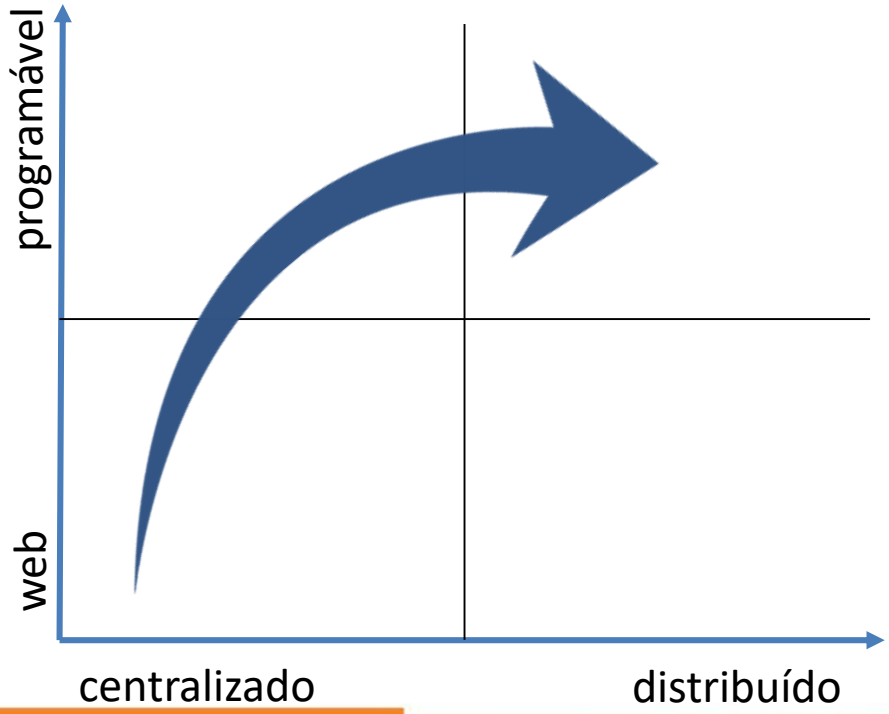
Sistemas

- IPFS, Torrent, Content Delivery (CDN)

Inovação

- BigData, Edge Computing

Sociedade Blockchain



Sociedade Programável

Sociedade Descentralizada

Sociedade AutoSoberana

Sociedade Blockchain

DLT, Smart contracts, DApp

Web3

Interoperabilidade

- Organizações e seus sistemas trocando informações utilizando barramentos distribuídos.

Soberania de dados

- Conceito de propriedade (dono) de conjunto de dados e informações corporativas e pessoais.

Protocolos distribuídos

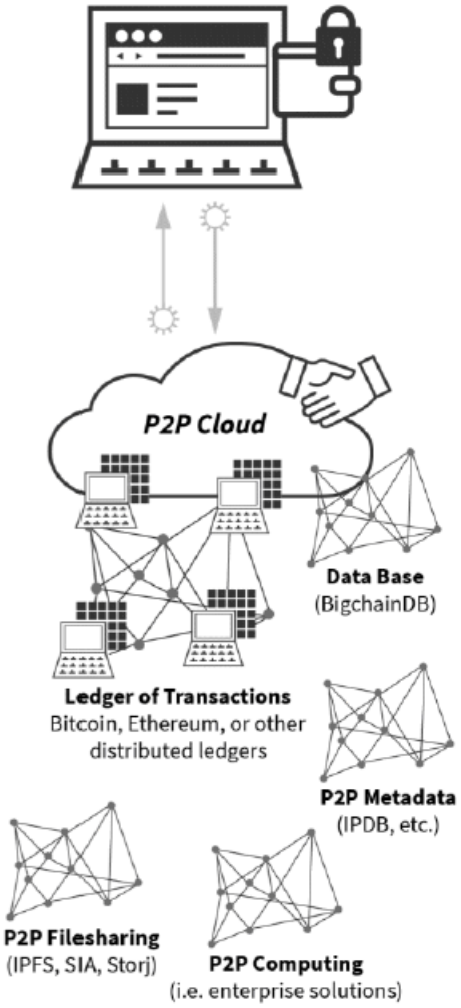
- Blockchains, DLT, armazenamento, edge computing

WWW -> WWL

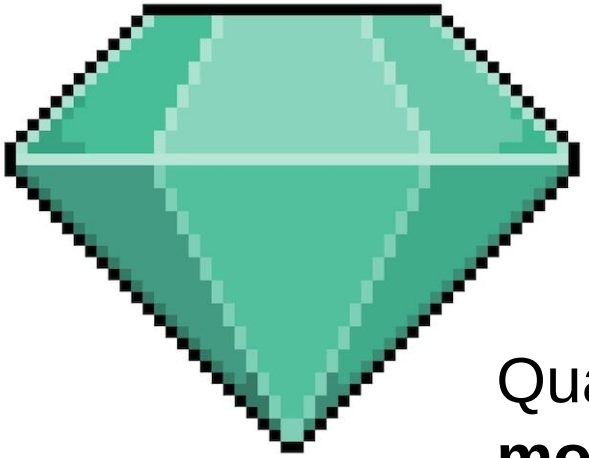
- World Wide Ledger

Tokens

- Ativos digitais de troca de valor



Qual o valor das coisas?



Quais os critérios de **valor** a **sociedade moderna** está atribuindo ao **mundo digital**?

Conceitos Blockchain

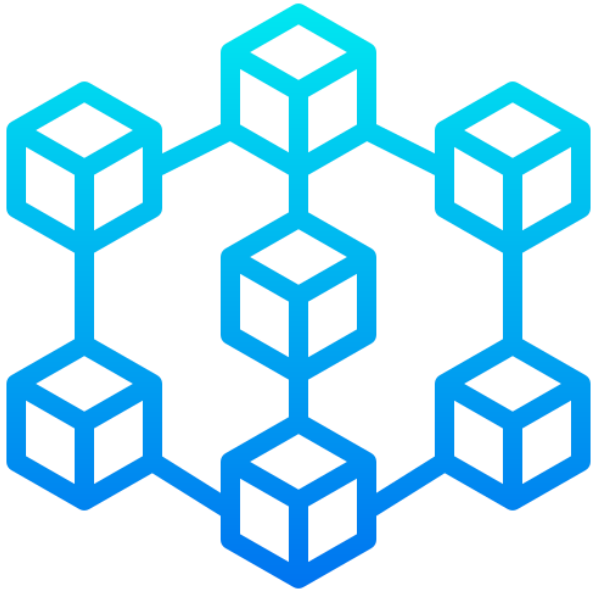
Definição Blockchain *

* Definições de Blockchain podem variar de autor para autor

- DLT com redundância peer-to-peer
- **Assinatura digital** para as transações que são armazenadas grupos de Blocos
- Transações podem conter dados ou programas
- Blocos encadeados em uma lista com o hash do bloco anterior.
- Blocos agrupados em ordem cronológica.
- Regra de consenso para comitar os Blocos.

Pilares de um Blockchain

- Transação
- Bloco
- Ledger
- State
- Smart Contract
- Rede Peer-to-Peer
- Consenso
- Oráculo



World State

Word State representa o último **estado válido** de um Blockchain

Diferentes Blockchains permissionados usam diferentes Bancos de Dados para seus World States.

Previous State: João possui uma BMW

Transação: Mauro compra BMW de João

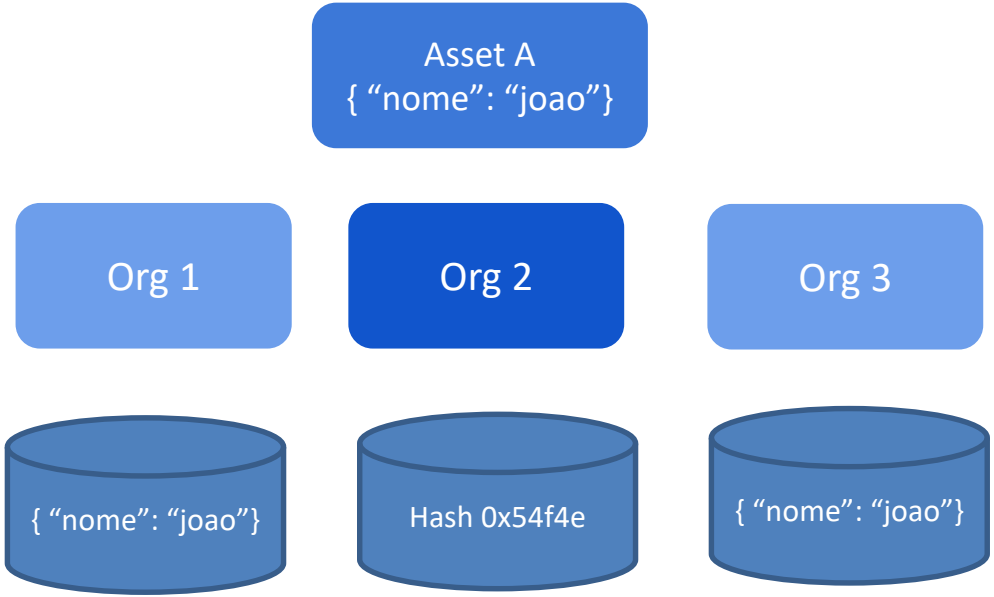
World State: Mauro possui uma BMW

Dados privados

Algumas Blockchains permitem o conceito de private data.

Bancos de dados transientes (fora do ledger) para registros de dados.

Off-chain integrada



Principais Características

Segurança

- Todos os participantes executam o mesmo código
- Histórico imutável

Procedência

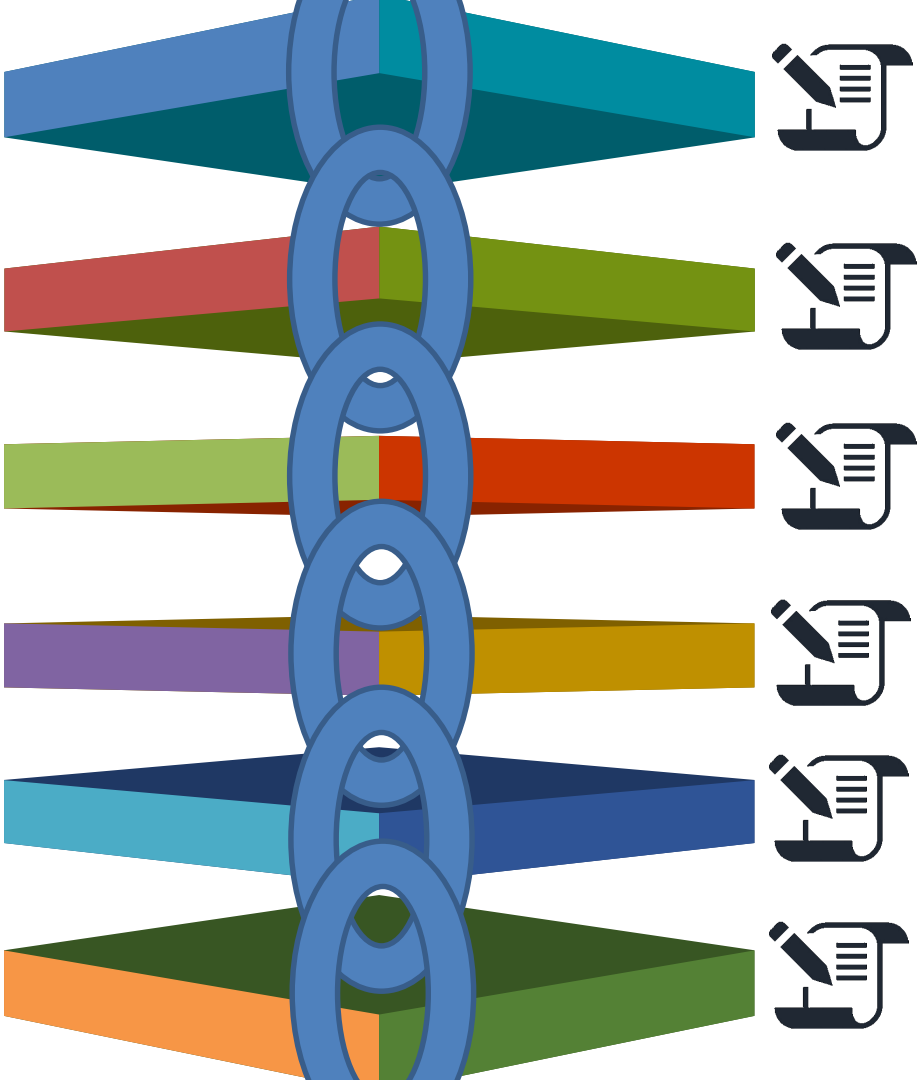
- Assinatura de cada transação referente a um ativo.
- Rastreabilidade do ativo muda ao longo do tempo

Descentralizado

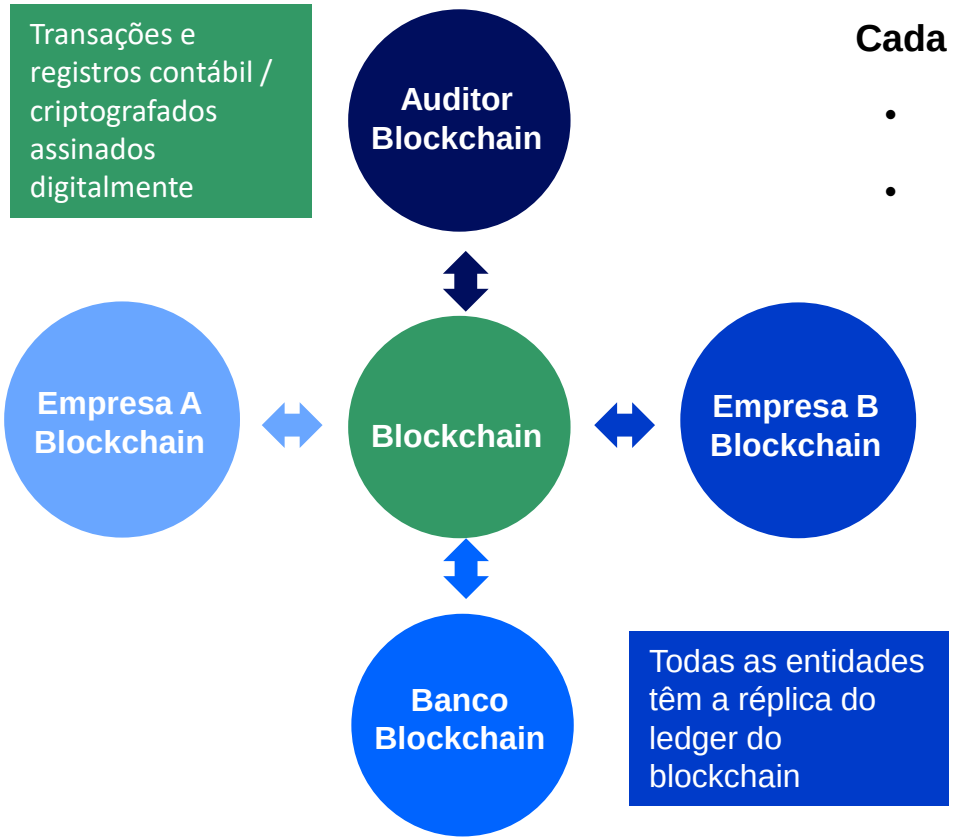
- Não existe um único dono da base de dados
- Administração autônoma ou compartilhada.

Registro em Blockchain

Cada entidade responsável assinaria todos os registros realizados com seu certificado digital.



Interação Empresarial - Blockchain



Cada um mantém réplica do livro

- Ledger é compartilhado e está disponível para todos
- Histórico dos ativos digitais imutável

Identificação das transações

- Assinatura digital identificando a organização
- Confiabilidade dos ativos digitais

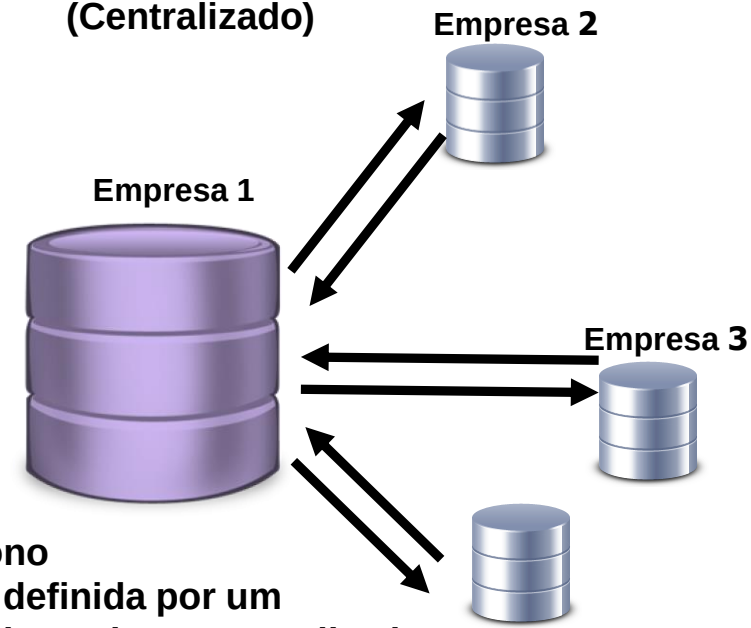
Contrato Inteligente gerando transações

- Garantia do código utilizado.
- Confiabilidade do processo.

Tradicional X Blockchain

TRADICIONAL

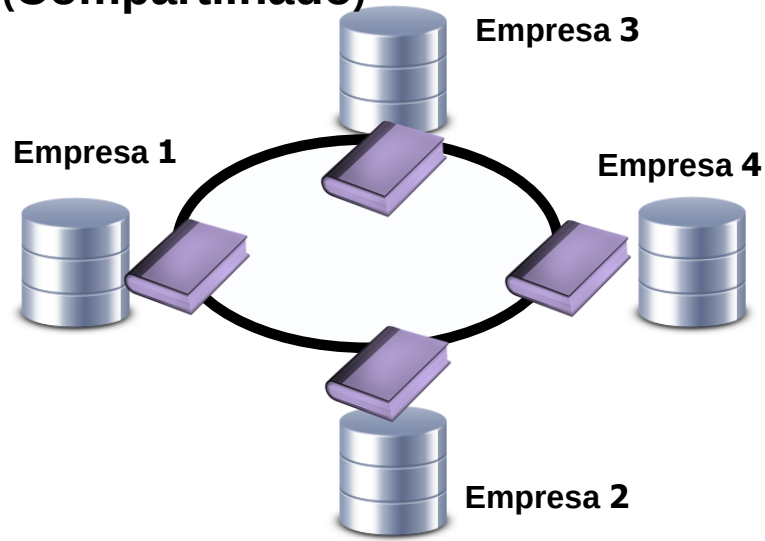
(Centralizado)



- Um dono
- Regra definida por um
- Consulta na base centralizada
- Registro de campos
- VPN para acessar infraestrutura do dono

BLOCKCHAIN

(Compartilhado)



- Administração compartilhada
- Consenso define a regra
- Consulta local
- Cada participante gerindo a sua infra

ESCOLA SUPERIOR DE REDES

Discussão em Grupo

PRÓXIMO MÓDULO:
2
Hyperledger Fabric

GoLedger

RNP
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES