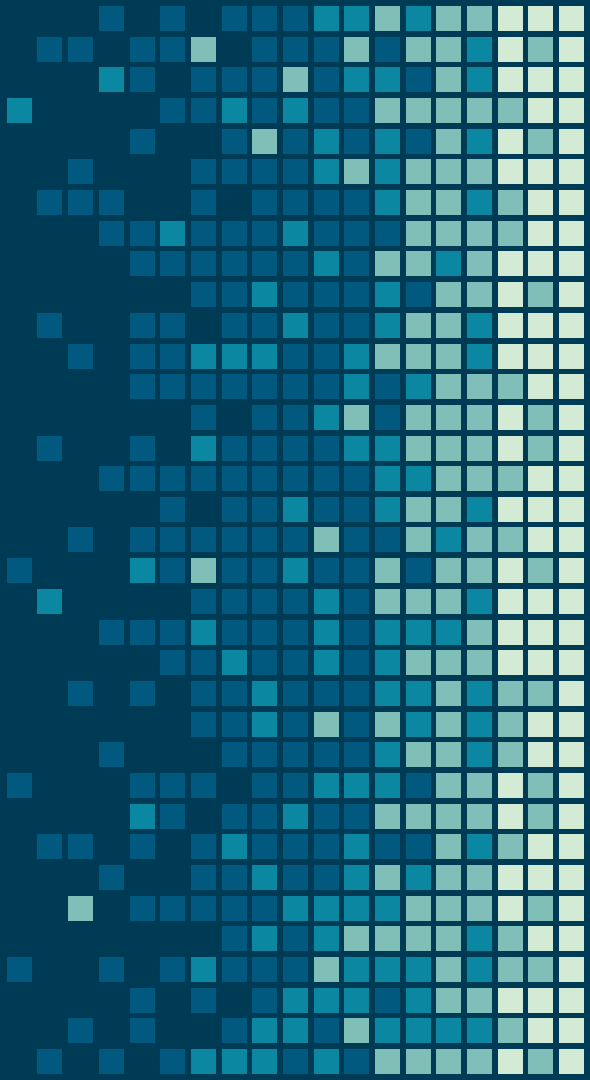
# BLOCKCHAIN

Bruno Ricardo Lucarelli &
Maick Henrique Pereira de Oliveira



# 1.
# INTRODUÇÃO

Entendendo o que é e como funciona o blockchain

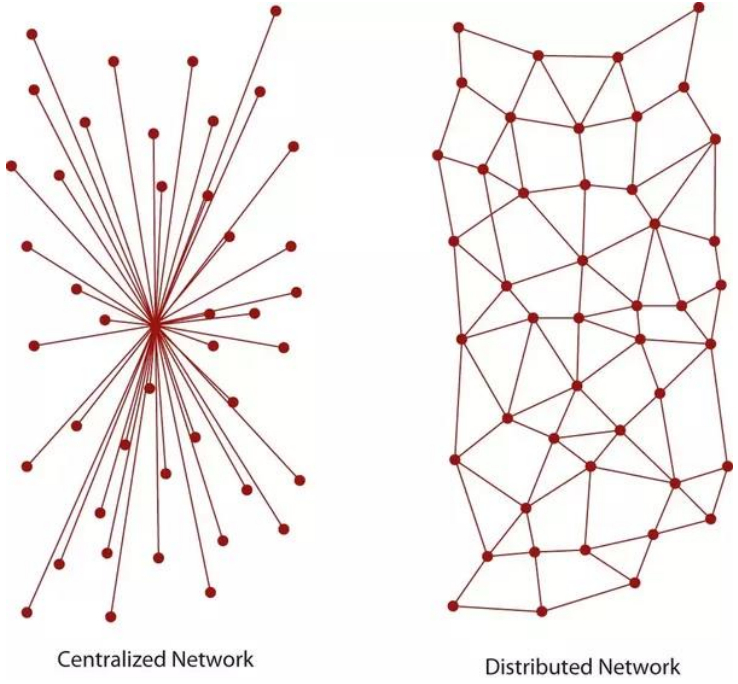
# Vídeo animado: What is Blockchain?

- https://www.youtube.com/watch?v=NTNQMKB0A3A

# A definição das características

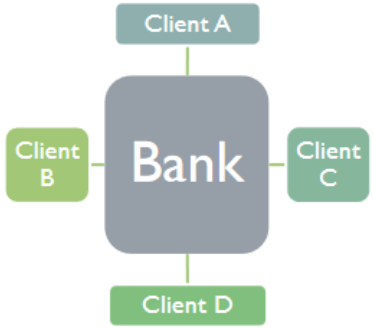
- **Ledger distribuído**: o livro-razão, sistema de registro das transações e blocos, é compartilhado por toda a rede e todos podem ver;
- **Privacidade**: é possível garantir a visibilidade adequada para a rede, já que as transações conseguem ser vericáveis. O termo "adequado" é importante; no bitcoin, todas as informações da transação são públicas. No blockchain, partes sensíveis do ledger podem ser ocultadas (como o endereço de alguém), sem prejudicar a vericação do bloco;
- **Contrato inteligente**: um documento que não pode ser alterado depois de escrito. É possível firmar contratos e autorizar (ou não) transações de acordo com os termos estabelecidos;
- **Consenso**: as transações são verificadas pelos participantes da rede e não podem ser fraudadas.

# O significado de Redes Descentralizadas

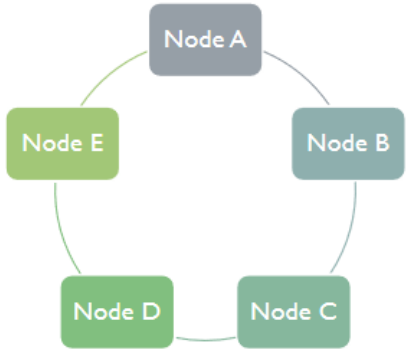


# Continuação...

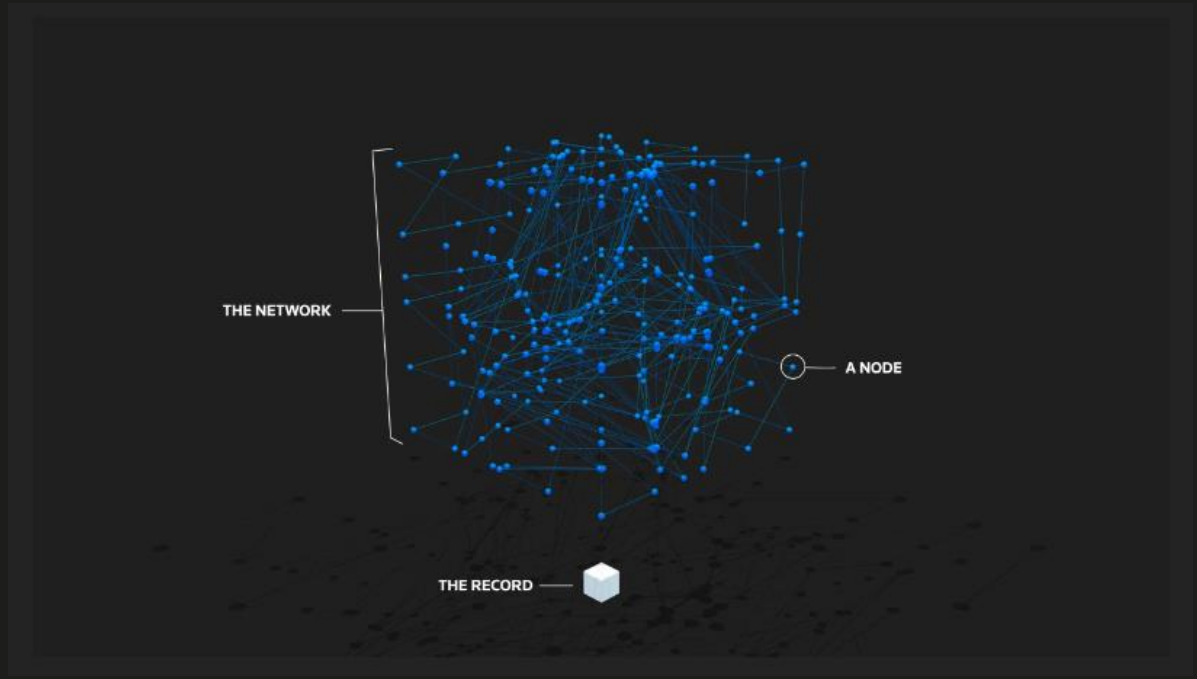
Centralized Ledger




Distributed Ledger

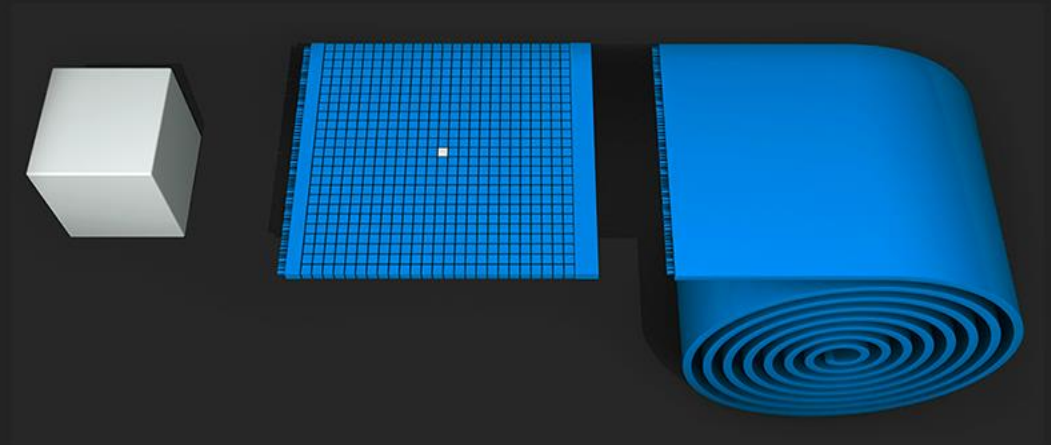


# Como imaginar a rede descentralizada?



# Uma visão da estrutura para a transação

Records are bundled together into blocks and added to the chain one after another. The basic parts:



**THE RECORD**

Can be any information, a deal for example

**THE BLOCK**

A bundle of records

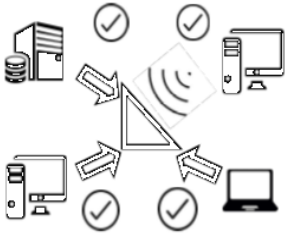
**THE CHAIN**

All the blocks linked together

# E o processo de transação funciona assim:

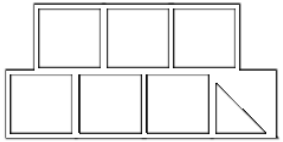
1. A sends information that it wants to transfer assets/information to B

2. Transaction is sent out to computers/participants of P2P network (nods)



3. The network confirms/ validates the transaction

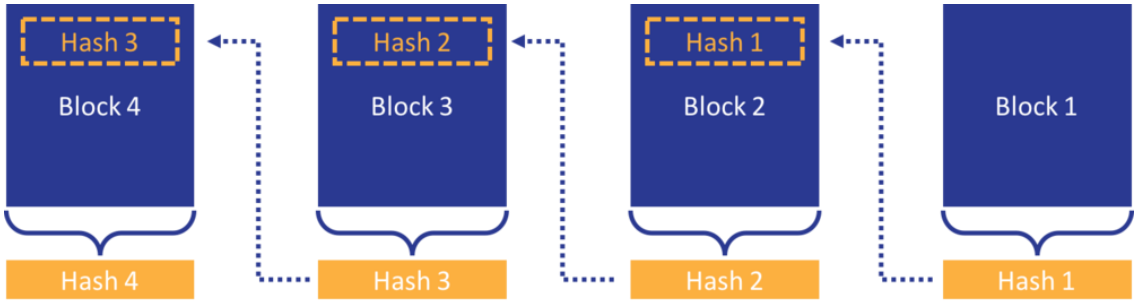
4. Verified transaction is blocked along with other transactions



5. Block can be attached to the chain (next block will include hash of the last block)

6. Transaction is completed

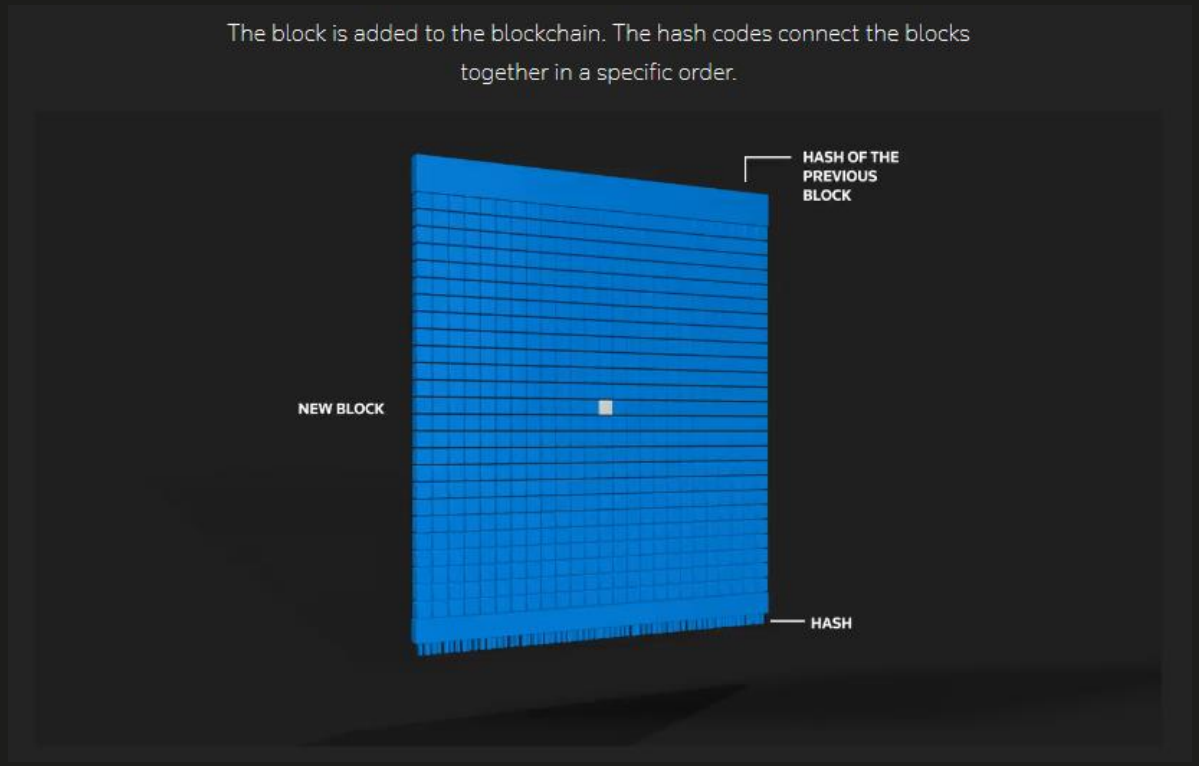
# A estrutura do Hash



# O Hash é um pouco complexo...

| Input | Output (Hash) |
| --- | --- |
| Cat | 93g56gtf229hbno00r45sktrpbs59so9r3t7saer |
| A white cat is outside | js03bbstgo94r6s1z8mg05fgt3sba9tob32bsap7 |
| A white cat is inside | bbr19007go2tsi52bsi50o21nmiseas45on23mjn |
| A whiet cat is inside | 339n5sbk249nb9530gjdl04h92jg02jg9sm93hpz |
| A white cat is insid | 4bbj390osoh9djm395bksh94gf03sg034dfjh31x |

# Esse é o final da transação:



# A lógica por trás do blockchain

- https://www.youtube.com/watch?v=DRcns37waB0&feature=youtu.be

# Recompensas

**Prova de Trabalho:** Para adicionar o bloco à cadeia/corrente e formar o consenso, os nós precisam demonstrar que eles fizeram o "trabalho" resolvendo os Hashs, que nada mais são que funcões matemáticas. O processo é chamado de mineração e utiliza muito processamento computacional. Como recompensa, unidades de criptomoedas são recebidos.

# Fazendo uma analogia

Alex Braz, CTO da Star Labs, explicou na Web.br que esse mecanismo de consenso é comparável ao jogo de puzzle Sudoku: é difícil resolver o problema, mas é fácil velicar se ele está resolvido.

Claro, para que tudo isso funcione, os algoritmos de hash devem ser públicos, para que qualquer entidade possa calculá-lo e validar os dados.

# Genesis block

Genesis block é o primeiro bloco da cadeia blockchain.

Ele define os parâmetros iniciais como nível de dificuldade, algoritmo de consenso etc. para a mineração de blocos.

É diferente na maneira que é criado. Hard-coded e então implantado na rede principal. Para outros blocos, é claro, os clients possuem suas respectivas funções para criá-los.

Dois nós se conectarão à rede apenas se eles possuírem exatamente o mesmo bloco Gênesis. Isso implica que a sincronização dos blocos apenas ocorrerá se os pares tiverem o mesmo bloco Gênesis.

# O famoso ataque de 51%

Caso alguém possua mais de 51% da rede, seria possível modificar e validar as transações.

Difícil, pois quanto mais a rede cresce mais segura ela se torna.

Nao há um ponto central de falha, pois é descentralizada, portanto o hacker deveria invadir todos os PCs da rede para obter sucesso.

# 2.
# Tipos de Blockchain

Das criptomoedas as mais diversas aplicações

# 1. Blockchain público

É o tipo de blockchain mais utilizado pelas criptomoedas, como o bitcoin e o Ethereum. Todas as transações são públicas, os usuários têm direito ao anonimato e qualquer tipo de alteração precisa da validação dos demais participantes. São as cadeias de blocos criptografados mais tradicionais. Foi a partir deles que surgiram todos os demais modelos.

# 2. Blockchain semiprivado

Uma única empresa investe no desenvolvimento de uma rede. Depois, ela fornece acesso a outros usuários, desde que eles atendam a uma lista estabelecida de pré-requisitos. Tecnicamente, essa rede não é descentralizada, já que uma empresa tem controle sobre ela. Suas aplicações podem ser especialmente interessantes para usuários de B2B (business to business).

# 3. Blockchain privado

São áreas restritas, que descaracterizam uma das maiores qualidades do blockchain: o fato de não haver um proprietário único da cadeia de informações. Essas redes costumam ser mantidas e utilizadas por uma única empresa. Na prática, são ambientes restritos corporativos tradicionais, que agregam a segurança que as cadeias de blocos criptografados oferecem.

# 4. Consórcios de blockchain

Modelo mais usado neste momento, são os formados por grupos de corporações ou instituições, que dividem o investimento e estabelecem uma lista de pessoas que têm acesso ao sistema. Dependendo do objetivo da rede, o direito de realizar transações e registrá-las nesse sistema pode ser público, ou fechado apenas para os participantes.

# 3.
# Gerações do Blockchain

As diferentes atividades da tecnologia

# Três grandes categorias:

## Blockchain 1.0

Moedas digitais

## Blockchain 2.0

Contratos inteligentes

## Blockchain 3.0

Aplicações eficientes e coordenadas além das criptomoedas, economia e mercados

# 3.
# Aplicações além do Bitcoin

O futuro da tecnologia

# O blockchain pode ser usado nas indústrias de:

- Serviços financeiros;
- Alimentos;
- Energia;
- Logística;
- Saúde;
- Governo.

# Tendências

- Assistência médica;
- Cidades inteligentes;
- Veículos autônomos.

# E já está sendo usado por algumas empresas e governos

- Telegram pretende lançar sua criptomoeda virtual chamada “Gram”;
- Spotify adquiriu startup que desenvolve sistemas baseados no blockchain;
- Dubai planeja implantar a tecnologia até 2020 e se tornar o primeiro governo do mundo a usar largamente o blockchain.

# IBM explica como essa tecnologia impactará nos negócios

- https://www.youtube.com/watch?v=wgAMF3zITck&feature=youtu.be

# Seria o blockchain o futuro do comércio on-line?

- https://www.youtube.com/watch?v=8AE2HhRyGPI&feature=youtu.be

# 4.
# Vantagens & desvantagens

# As vantagens primeiro

- Transparência nas transações;
- Auditabilidade;
- Criação de acordos sem a necessidade de um terceiro confiável;
- Anonimato;
- Banco de dados confiável.

# Algumas desvantagens

- Baixo nível de amadurecimento da tecnologia;
- Tamanho e largura de banda;
- Alta latência;
- Risco de Ataques;
- Desperdício de Recursos;
- Usabilidade;
- Versionamento.

# Além disso...

- Atualmente a capacidade do blockchain é restrita a 7 transações por segundo devido à restrição do tamanho do bloco, enquanto que, por exemplo, a VISA pode manipular mais que 47000 transações por segundo.
- Minerar Bitcoin desperdiça uma grande quantidade de energia ($15milhões/dia). O desperdício em Bitcoin é causado pelo esforço em solucionar seu Proof-of-Work.

# Conclusão

# Obrigado!