

BLOCKCHAIN

O que é, como funciona,
ferramentas e aplicações da nova
tecnologia



Leandro Martins

Analista de sistema na Cresol

Desenvolvedor nas horas vagas :)

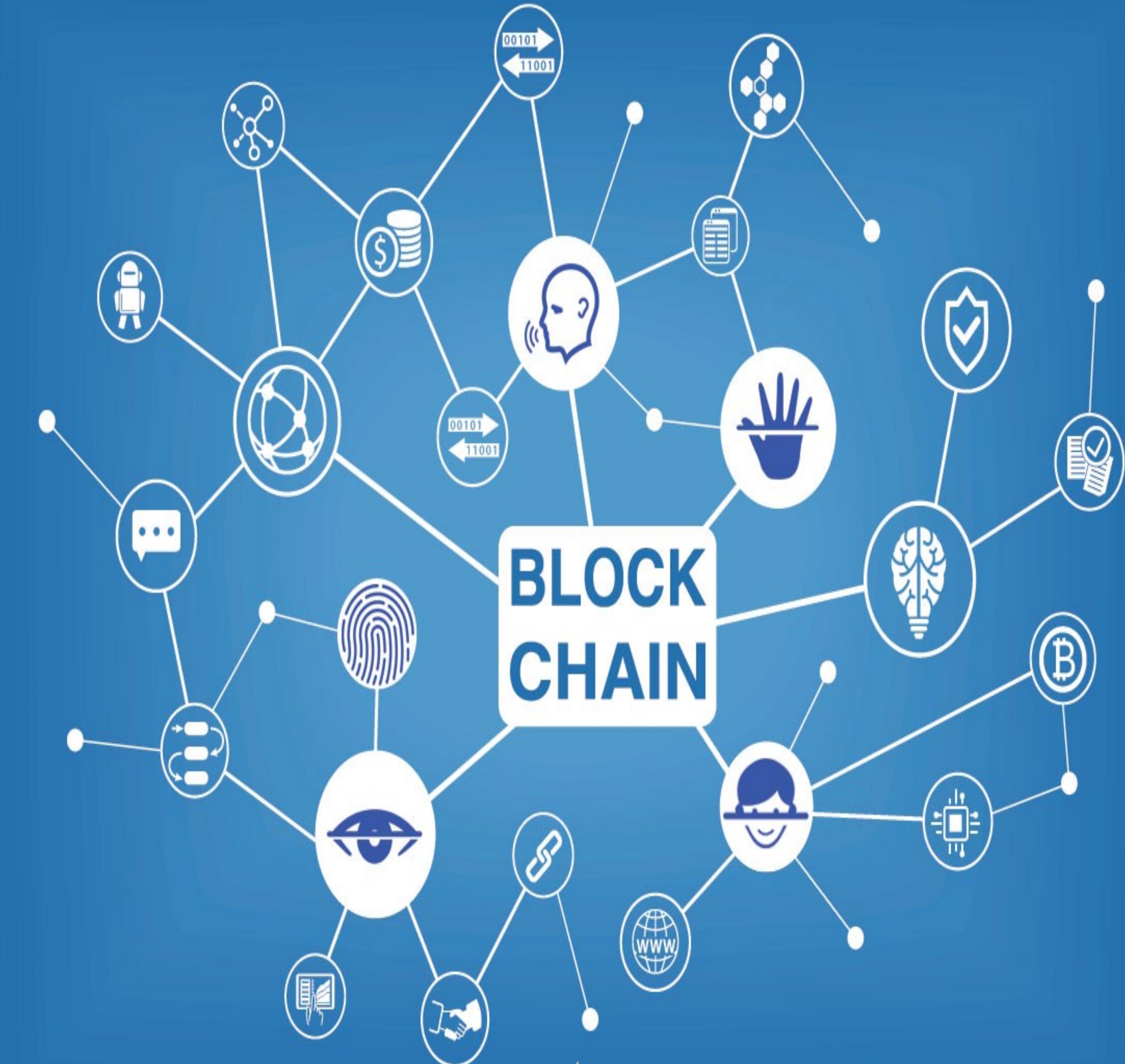
<https://www.linkedin.com/in/leandrojmartins>

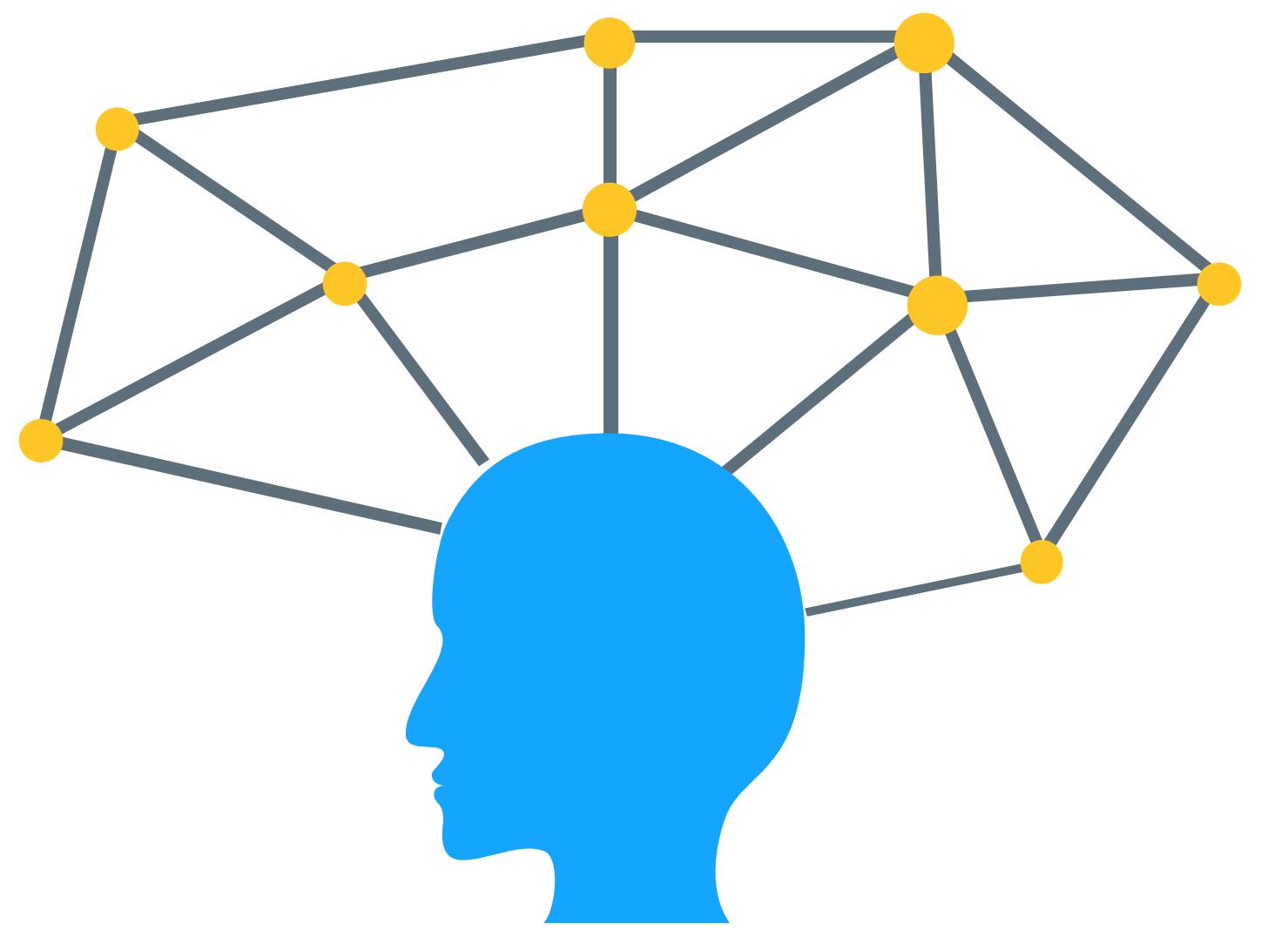
Agenda

- ☑ A origem
- ☑ Como funciona ?
- ☑ Ferramentas
- ☑ Áreas de aplicações
- ☑ Cases no mercado

“ Em sua essência, o blockchain é uma tecnologia que grava transações permanente de uma maneira que não podem ser apagadas depois, somente podem ser atualizadas sequencialmente, mantendo um rastro de histórico sem fim.”

William Mougayar





A Origem



Satoshi nakamoto e bitcoin

Artigo original: <https://bitcoin.org/bitcoin.pdf>

Campos de conhecimento

Teoria de jogos

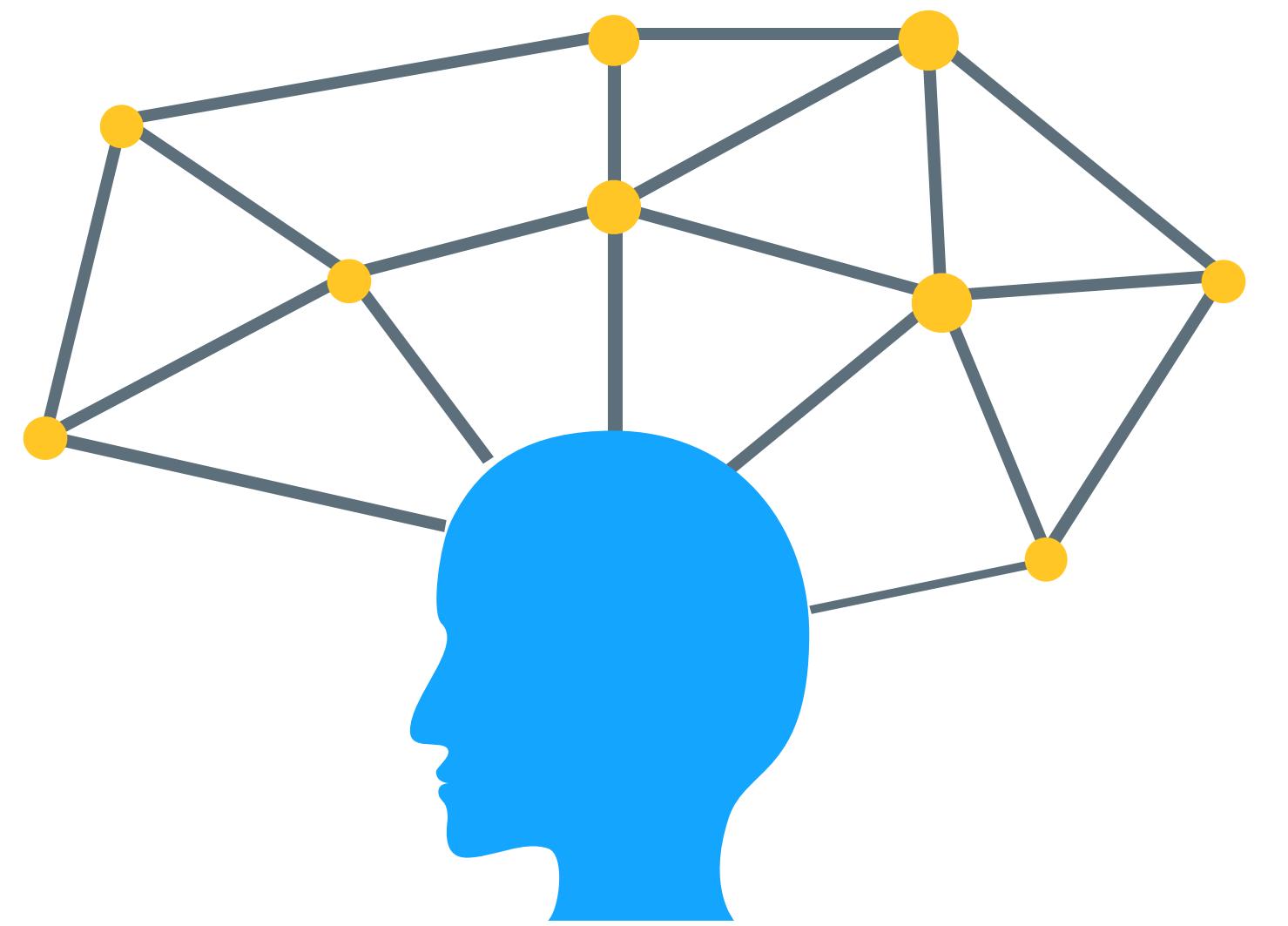
Problema dos Generais Bizantinos, os generais necessitam de chegar num consenso, não pode haver generais traidores para que que a vitória seja um sucesso.

Criptografia

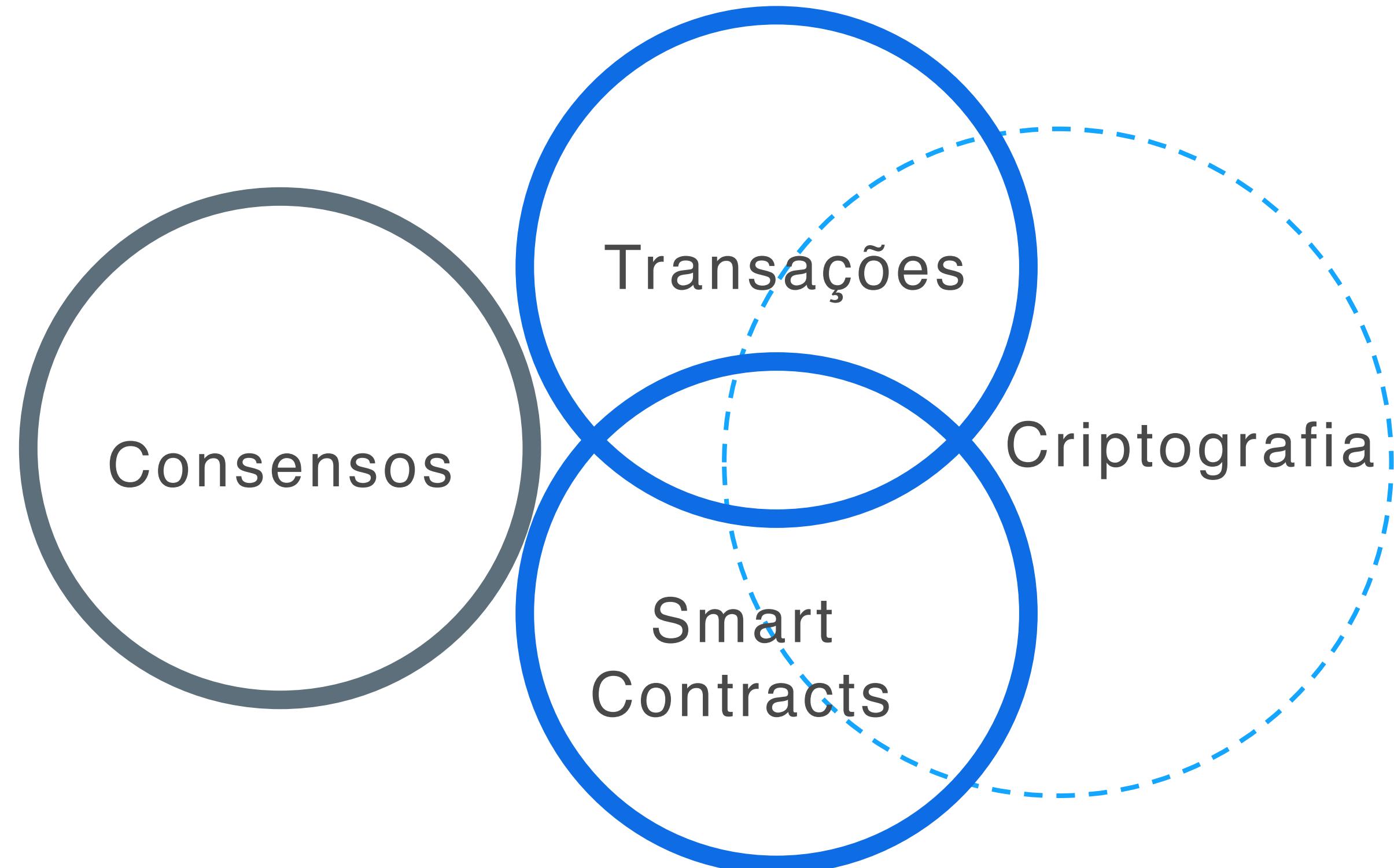
Utiliza hashing, chaves e assinaturas digitais para garantir a segurança da informação.

Eng. de software

Através de programação foi desenvolvido um software para atender as necessidades que resolve o problema dos generais, junto com criptografia e mais outros recursos tecnológicos já existentes.

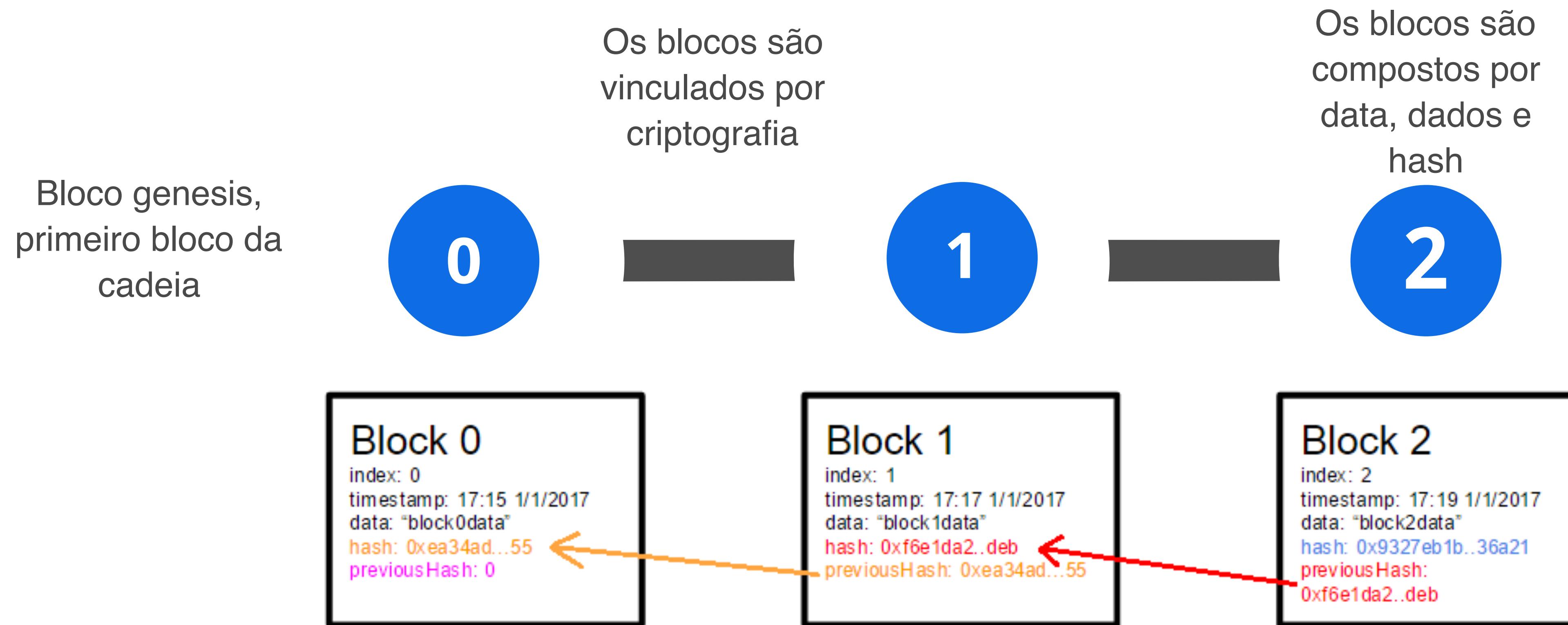


Como
funciona ?



- Livro contábil com transações (Ledger)
- Blocos de dados encadeados usando criptografia (Hash)
- Descentralizado rede P2P (Node)

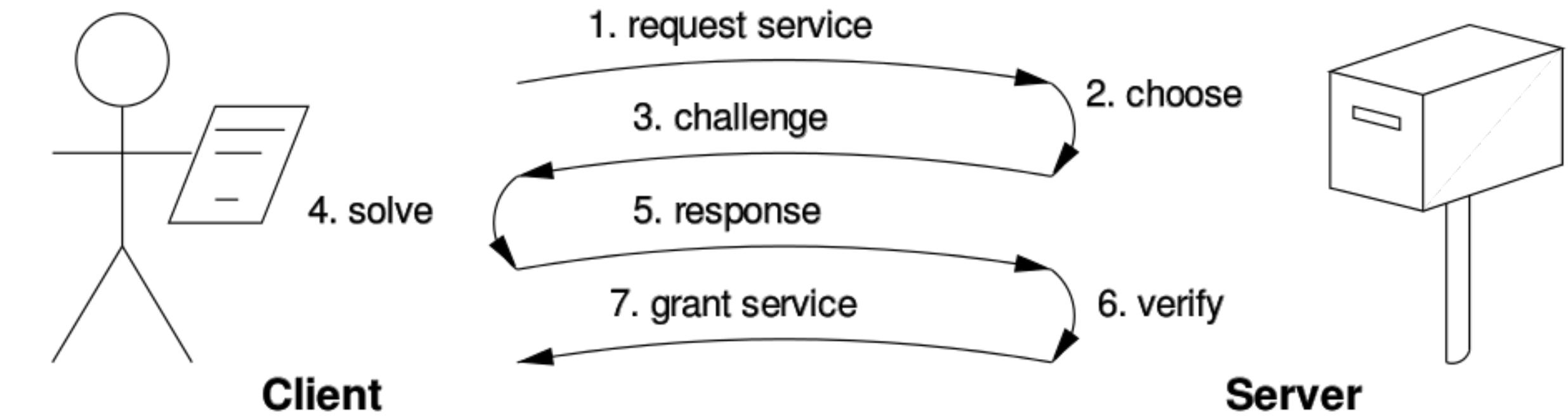
Transações



Consenso

Proof of Work (POW)

- O cliente tem que resolver um problema matemático para garantir a transação;
- São conhecido como mineradores;
- Indicado para redes blockchain abertas;



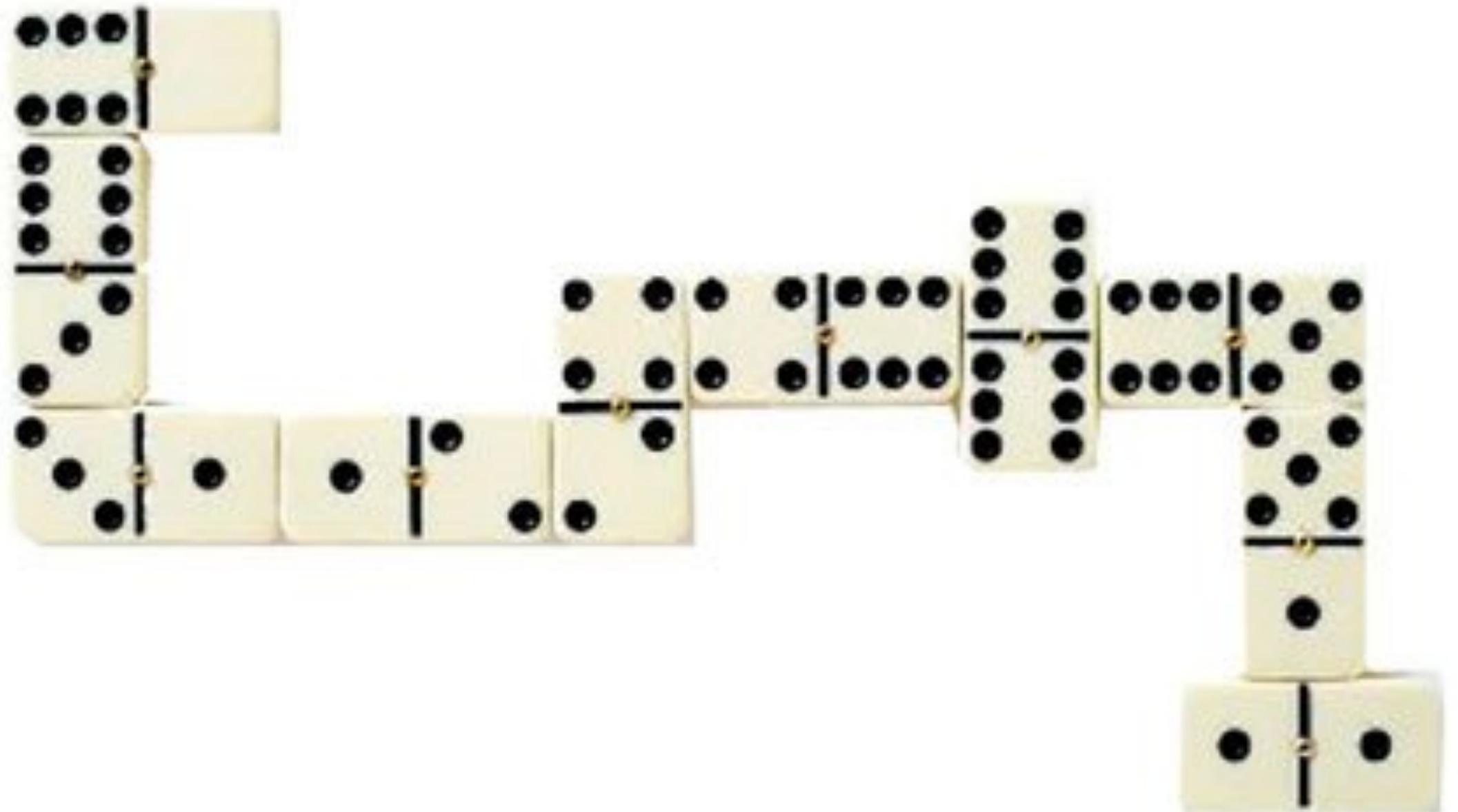
Consenso

Proof of Authority (POA)

- Validam contas se já existem no bloco se baseando em contas já existentes nos blocos para efetuar transação;
- Não realiza mineração
- Indicado para redes blockchain fechadas;

Smart contracts

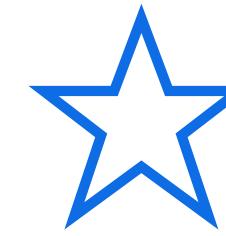
Contratos tradicionais	Contratos inteligentes
1 - 3 dias	Minutos
Remessa manual	Remessa automatica
Garantia necessaria	Garantia opcional
Custoso	Custo menor
Presença fisica (assinatura)	Presença virtual
Advogados necessários	Advogados podem não ser necessários
-	São imutáveis



Jogo de dominó e blockchain!

Peça inicial é bloco genesis;
Cada bloco é ligado com um numero;
Existe um consenso entre os jogadores;
Não é possível remover uma peça da cadeia.

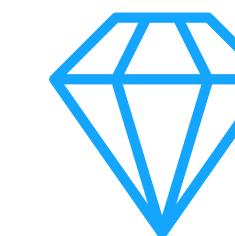
Em resumo...



Distribuido

Os blocos são distribuído na rede P2P, cada nó possui uma replicada do Ledger.

Melhor segurança e disponibilidade.



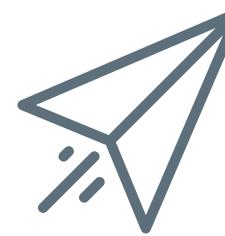
Datado

Toda transação possui uma data e hora, importante para rastreabilidade e auditoria.



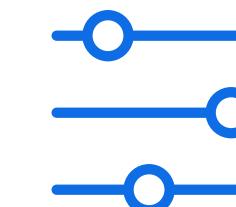
Segurança

Utiliza criptografia para garantir a segurança de transações e blocos.



Imutabilidade

Os dados registrados nos blocos são vinculados criptograficamente, não permitindo alteração.



Consenso

Para efetivação das transações é necessários que haja um consenso entre nós(node).



Programavel

Através de Smart Contracts, a rede pode possuir regras para validar transações.

Demonstração

Blockchain

Block:	# 1
Nonce:	61619
Data:	Dados
Prev:	00000000000000000000000000000000
Hash:	0000bd41d54a952725f4574ccaf6ee6cca0f1
Mine	
Block:	# 2
Nonce:	41773
Data:	Dados2
Prev:	0000bd41d54a952725f4574ccaf6ee6cca0f1
Hash:	0000260fef068f865b616662c95b061b416f0
Mine	

Fonte: <https://anders.com/blockchain/blockchain.html>

Quando usar blockchain ?

Você precisar compartilhar algo em comum ?

Sim

Múltiplas partes envolvidas ?

Sim

Partes não confiam em outras partes ?

Sim

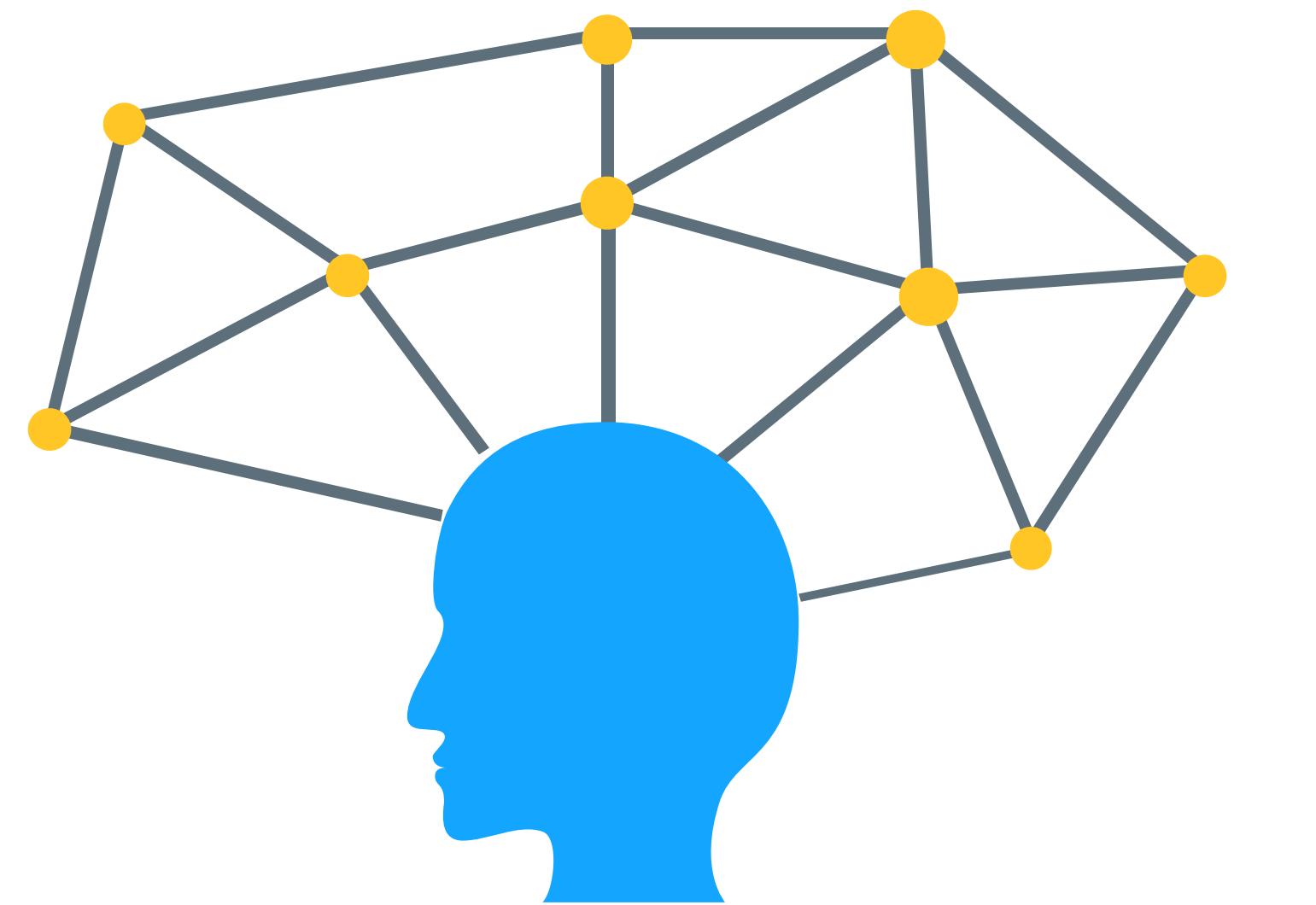
Você precisa de dados imutável ?

Use blockchain!

Para refletir!

Não

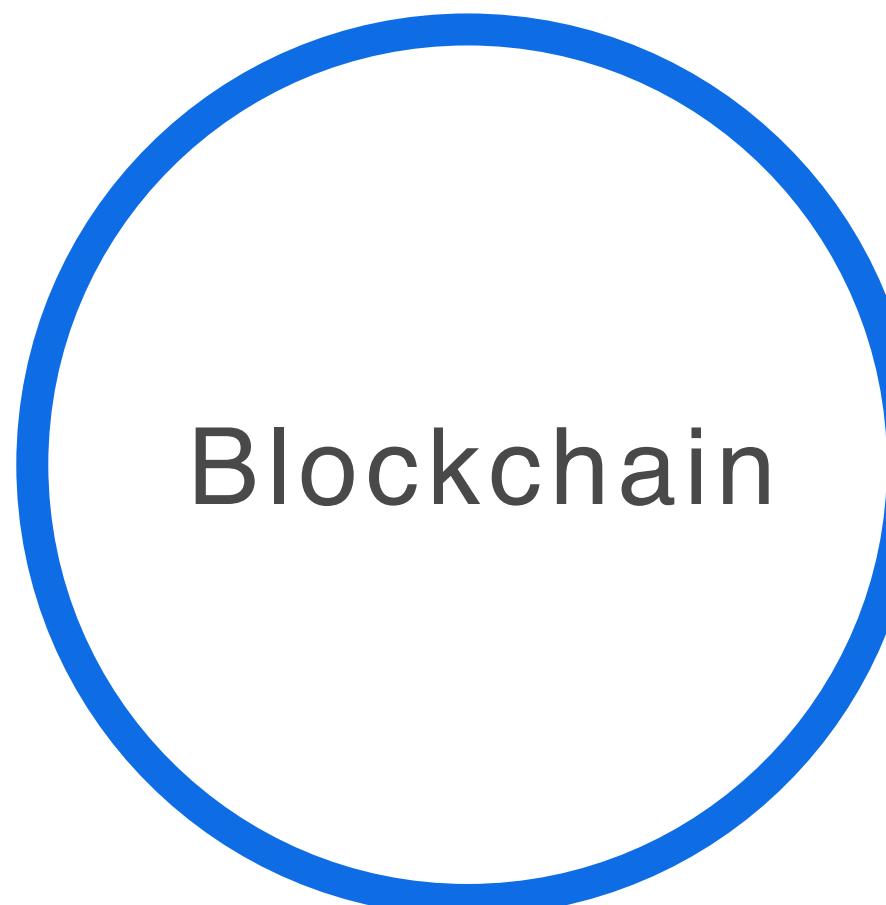
Não use blockchain!



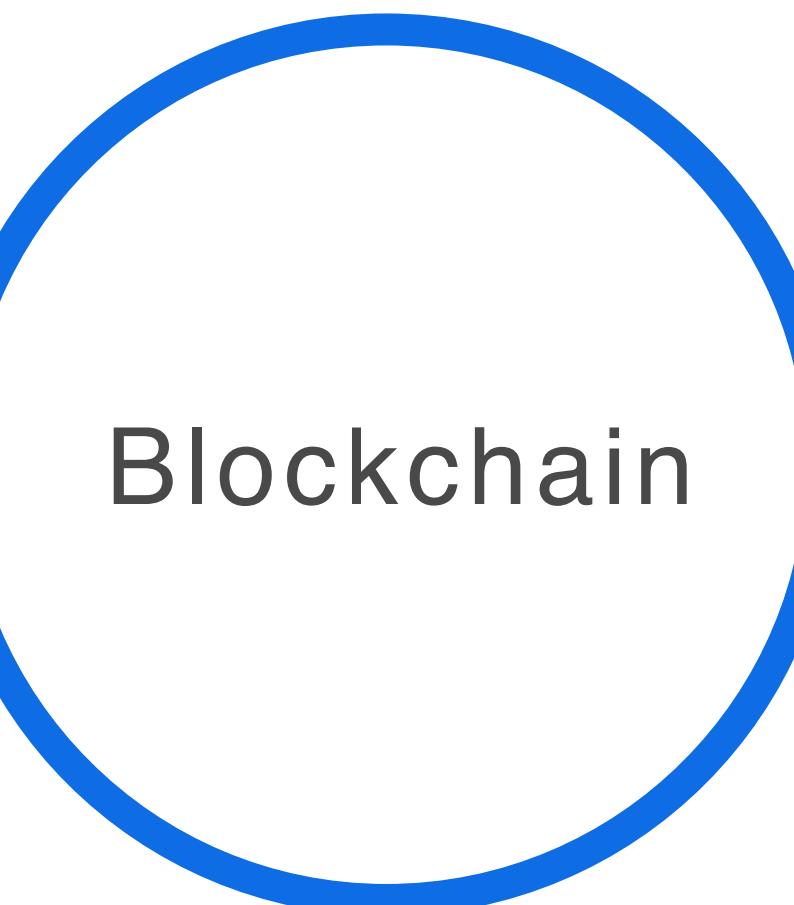
Ferramentas

Tipos de aplicações blockchain

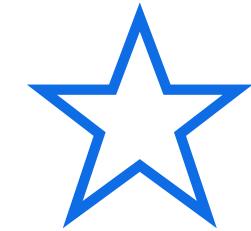
Nativas



Híbridas

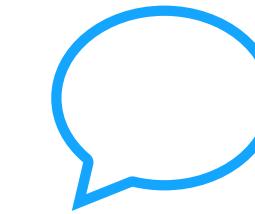


Algumas ferramentas



Banco de dados

DBChain
FlureeDB

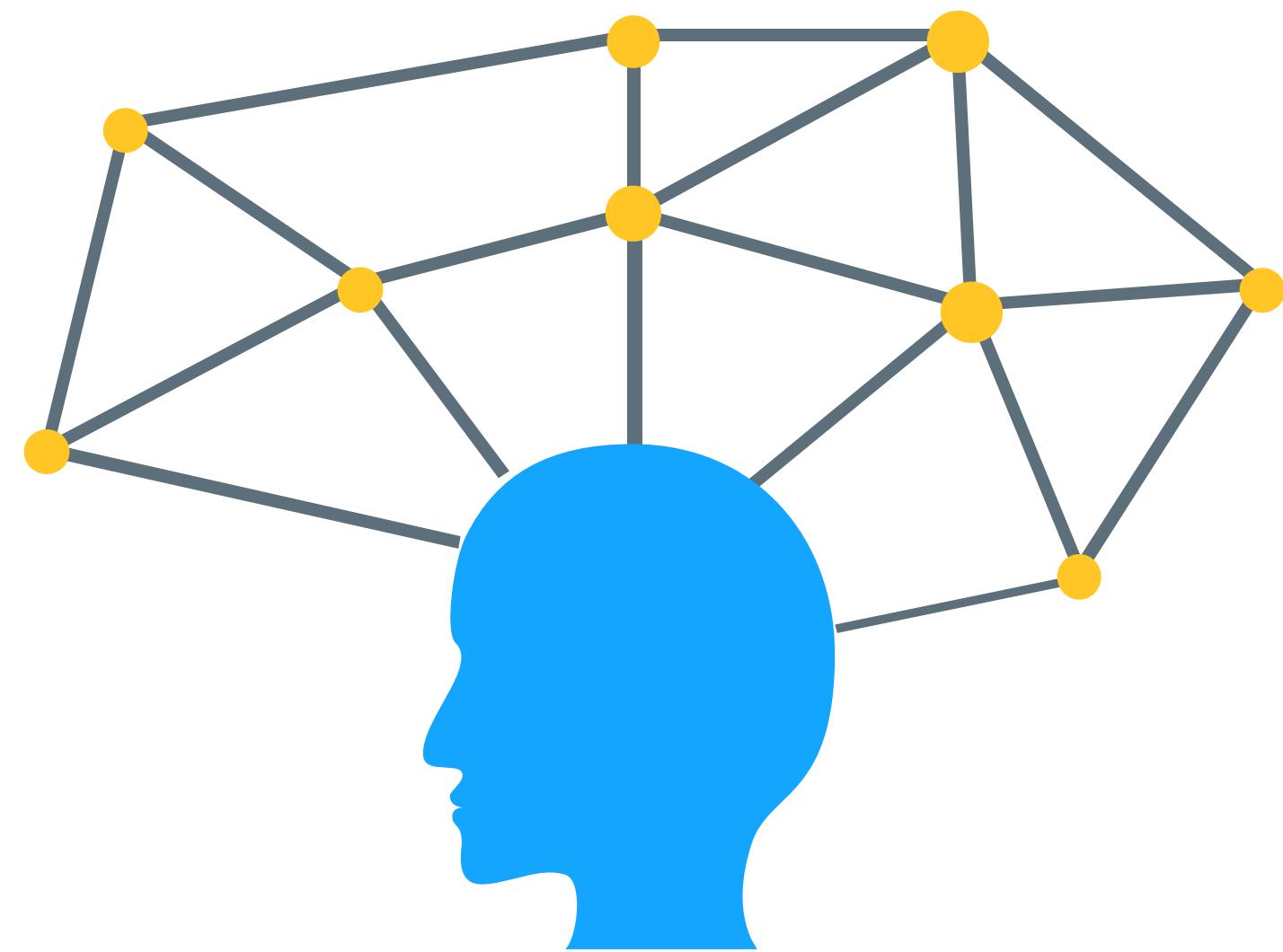


Frameworks

Corda (R3);
Hyper ledger Fabric (IBM);
Ethereum;
Quorum (JP Morgan);
IOTA Tangle (IoT);

Principais frameworks

	Ethereum	Hyperledger	Corda
Descrição da plataforma	Plataforma generica	Plataforma modular	Especializada na industria financeira
Governança	Comunidade Ethereum	Linux Foundation	Consorcio R3
Mode de operação	Sem permissão, privado ou aberto	Privada	Privada
Consenso	Proof of Work	Proof of Authority, outros tipos	Específicos da plataforma
Smart contracts	Linguagem Solidity	Go ou Java	Kotlin ou Java
Moeda	Ether, Tokens	Nenhuma, moeda ou token	Nenhuma



Áreas de aplicações

A photograph showing a person's hands typing on a silver MacBook Air keyboard. To the right is a white cup of coffee with latte art, a pair of sunglasses, a small dark bottle, and a vase with colorful flowers. In the foreground, an open notebook and a white smartphone are visible.

Financeira

Compensação e liquidação

Pagamentos domésticos

Automação de empréstimo

Prevenção de fraude

Auditoria de dados

A photograph showing a person's hands typing on a silver MacBook Air keyboard. On the desk next to the laptop is a white cup of coffee with latte art, a pair of sunglasses, a small dark bottle, and a vase with colorful flowers. In the foreground, a notebook and a smartphone are visible.

Saúde

Registro do Prontuario medico

Rastreamento de medicamento

Carteira virtual com registros medicos

Gestão de ensaios clínicos

**Privacidade e compartilhamento de registros
de saúde do paciente**

A photograph showing a person's hands typing on a silver MacBook Air keyboard. To the right is a white cup of coffee with intricate latte art. In the background, there are two small glass vases with colorful flowers (orange and purple). A pair of sunglasses lies next to the coffee cup. The scene is set on a light-colored wooden table.

Governos

Registro de terras

Gerenciamento de Licenças

Registro de veiculo

Sistemas de votação

Arquivamento e conformidades

A photograph showing a person's hands typing on a silver MacBook Air keyboard. On the desk next to the laptop is a white cup of coffee with latte art, a pair of sunglasses, a small dark bottle, and a vase with colorful flowers. In the foreground, an open notebook and a white smartphone are visible.

Energia

Medição e faturamento

Microtransações de baixo custo

Criações de mercados de pagamentos

Gestão de ativos

Certificação de energia renovável e
permissões de emissão



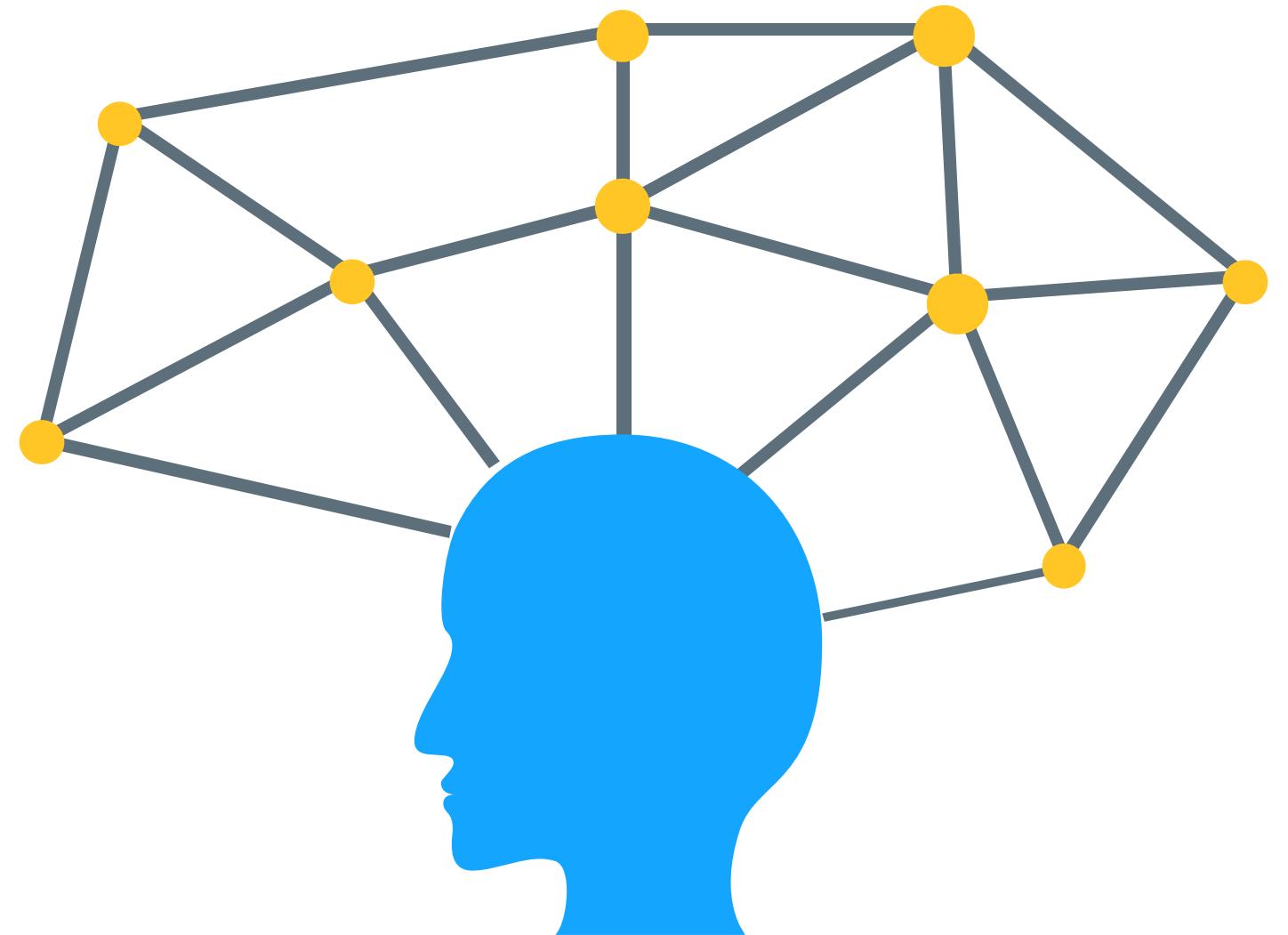
Varejo e Comercio eletrônico

Aumentar a transparência da cadeia de suprimento

Redução de produtos falsificados

Gerenciamento de garantia

Cases



Alguns casos que estão em
produção ou POC!



BANCO CENTRAL DO BRASIL

BACEN

O que é ?

Um cadastro de cliente com capacidade de compartilhamento entre diferentes instituições e atualização em tempo real. POC

Como ?

Usando Ledger compartilhando informações fictícias, como nome, CPF e RG, idade, endereço e telefone, com armazenamento de documentos.

Benefícios

Capacidade de os bancos operarem em regime colaborativo, com garantia de imutabilidade dos dados compartilhados, preservação da privacidade e rastreabilidade das informações.

ABN-AMRO



O que é ?

Reimagine o processo atual de auditoria dispendiosa que exige a integração de dados - muitas vezes inconsistentes e desatualizados - de várias fontes no blockchain.

Como ?

Servidor de Ledger replicado e compartilhado como ponto único de verdade;

Auditores estão garantidos que ninguém adulterou os dados via imutabilidade de blockchain.

Benefícios

Clientes banco e reguladores todos vêem versão única da verdade;

Nenhuma inconsistência de dados => limpar trilha de auditoria;

Permite revisões eficientes de qualidade de ativos de baixo custo (AQR).

Maersk



O que é ?

Uma plataforma aberta e extensível para compartilhar eventos de remessa, mensagens e documentos em todos os atores e sistemas do ecossistema da cadeia de suprimentos.

Como ?

Fornecendo visibilidade compartilhada e estado compartilhado para remessas de contêiner

Benefícios

Aumente a velocidade e a transparência das transações entre fronteiras através do acesso em tempo real a eventos de contêineres.

Custo reduzido e maior eficiência através do comércio sem papel fornecendo uma interface: parceiros de valor agregado Editores e assinantes de eventos



O que é ?

Controle das margens de transações

Como ?

Utilizando como controle de ativo e armazenamento permanente

Benefícios

Essa aplicação permite o armazenamento das informações da negociação em um ambiente virtual seguro e de forma permanente. A ideia de usar a ferramenta para esses ativos, segundo os executivos do banco, vem do fato de o preço dos derivativos não serem acompanhado por um regulador e não poderem ser consultados em uma clearing. Por isso, o valor que as partes transacionam é decidido por meio de uma negociação entre elas. Com a ferramenta, essa transação é fechada virtualmente e fica registrada de forma oficial na rede.



Walmart, Nestle, Unilever

O que é ?

Fornecer uma fonte confiável de informações e rastreabilidade para melhorar a transparência e a eficiência em toda a rede de alimentos.

Como ?

Ledger compartilhado para armazenamento de documentação de conformidade digital, resultados de testes e auditoria de rede de certificados.

Benefícios

Reducir o impacto dos recalls de alimentos por meio de acesso instantâneo a dados de rastreabilidade de ponta a ponta para verificar o histórico na rede de alimentos e na cadeia de suprimentos.

Ajudar a abordar as 1 em cada 10 pessoas doentes e as 400.000 mortes que acontecem todos os anos devido a doenças causadas por alimentos.



U.S. FOOD & DRUG ADMINISTRATION

FDA

O que é ?

Crie e promova uma troca segura, eficiente e escalável de dados de saúde usando a tecnologia blockchain.

Como ?

A tecnologia Blockchain será usada para criar um Ledger de onde e como os dados são transferidos e trocados.

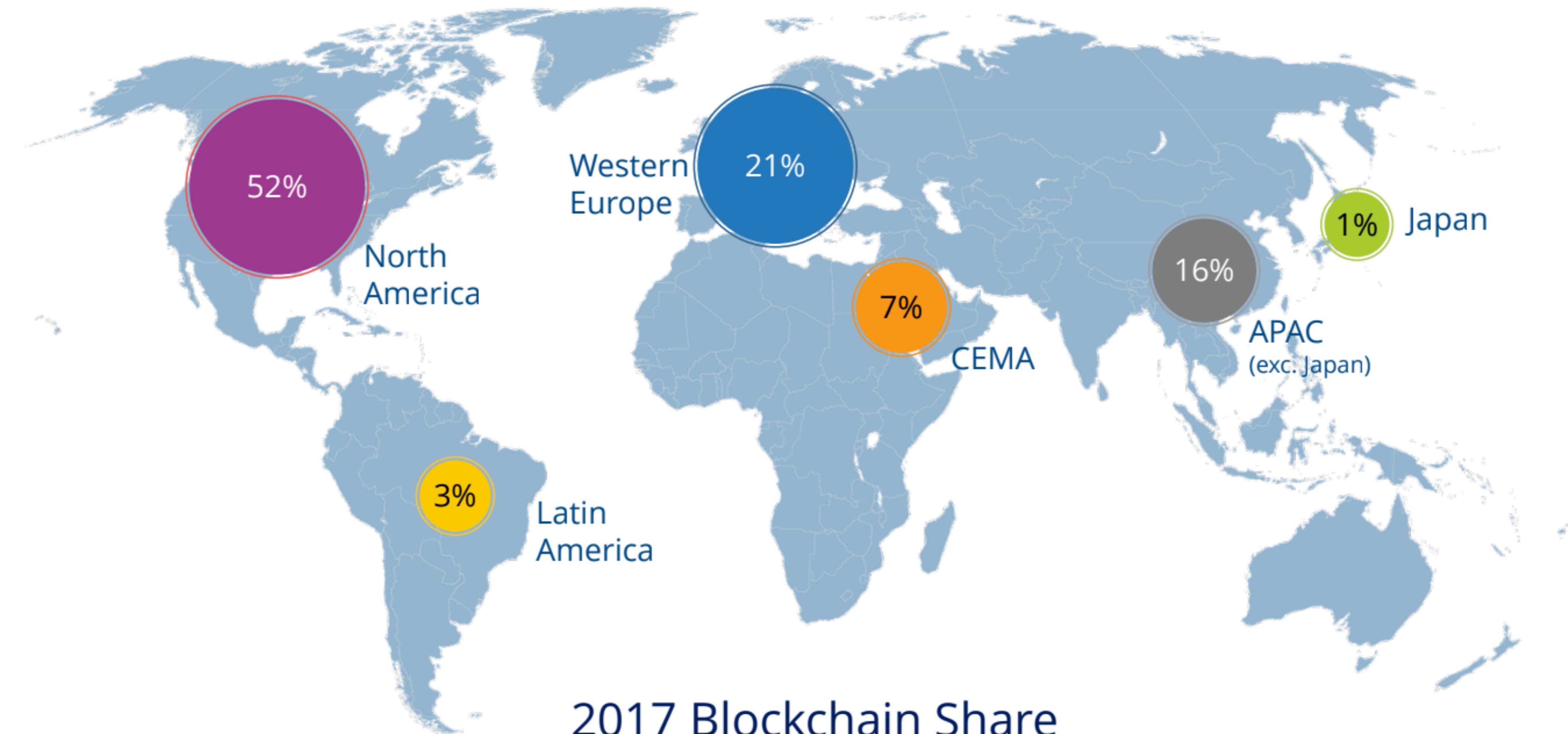
Ensaio inicial de foco em dados de oncologia.

Benefícios

Criando uma trilha de auditoria através do Ledger, os profissionais de saúde serão capazes de:

- manter os vazamentos de informações responsáveis
- manter a transparência em relação aos dados que estão indo
- proteger os pontos fracos no processo de compartilhamento

\$945 Million spent in 2017 - Blockchain Technology Investments Will Reach \$9.7 Billion by 2021



Para refletir...

Necessidade de utilizar blockchain e qual tipo de rede, utilizar modelo decisões!

Contratos são imutáveis, o que fazer quando achar um bug ?

Ciclo de desenvolvimento (Requisitos, Designer, Desenvolvimento, Teste, Produção e Suporte)

Material para estudo

IBM - E-Book Blockchain for Dummies

<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN>

Frankfurt School Blockchain Center - Segurança

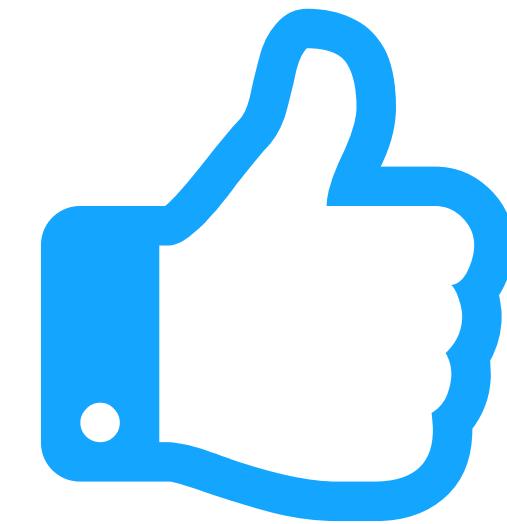
<https://medium.com/@fsblockchain/security-in-blockchain-applications-43e73193512d>

Banco Central do Brasil - Paper do POC

[https://www.bcb.gov.br/htms/public/microcredito/
Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf](https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf)

IBM Blockchain Cloud - PlayGround

<https://www.ibm.com/blockchain/getting-started.html>



Obrigado!

Duvidas ?

<https://www.linkedin.com/in/leandrojmartins>

leandro.jm@gmail.com