

Blockchain e Aplicações Descentralizadas

Edilson Osorio Junior

OriginalMy.com

Mar/2017



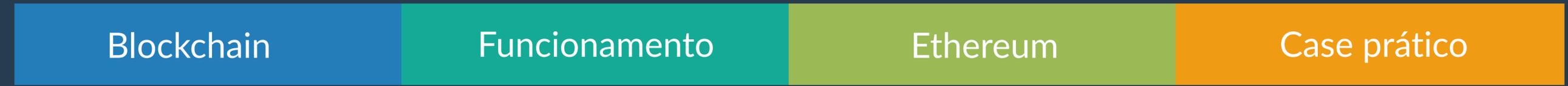


Agenda

Tópicos que serão abordados durante a palestra

O que é um Blockchain
Como surgiu e por quê usar blockchain

O Ethereum
Diferenças entre os principais blockchains existentes



Como os blockchains funcionam
Conceito de transação, blocos e consenso

Apresentação de Case
Caso de uso para criação de ativos, emissão de moedas e plataforma de negociação



História do Bitcoin e Blockchain

—



Do Dinheiro ao Bitcoin

Como se deu essa evolução?



Controle central de emissão, controlado por governos e normalmente depende de intermediários para gerar confiança



Satoshi Nakamoto e o Bitcoin

Whitepaper em Out/2008

Dinheiro eletrônico

equivalente à moeda tradicional



Escasso

com emissão finita e conhecida



P2P - Peer to Peer

transferível/trocada entre pessoas



Armazenável

onde pessoas pudessem guardar seguramente



Recompensa o esforço

Engaja uma comunidade de auditores (mineradores)

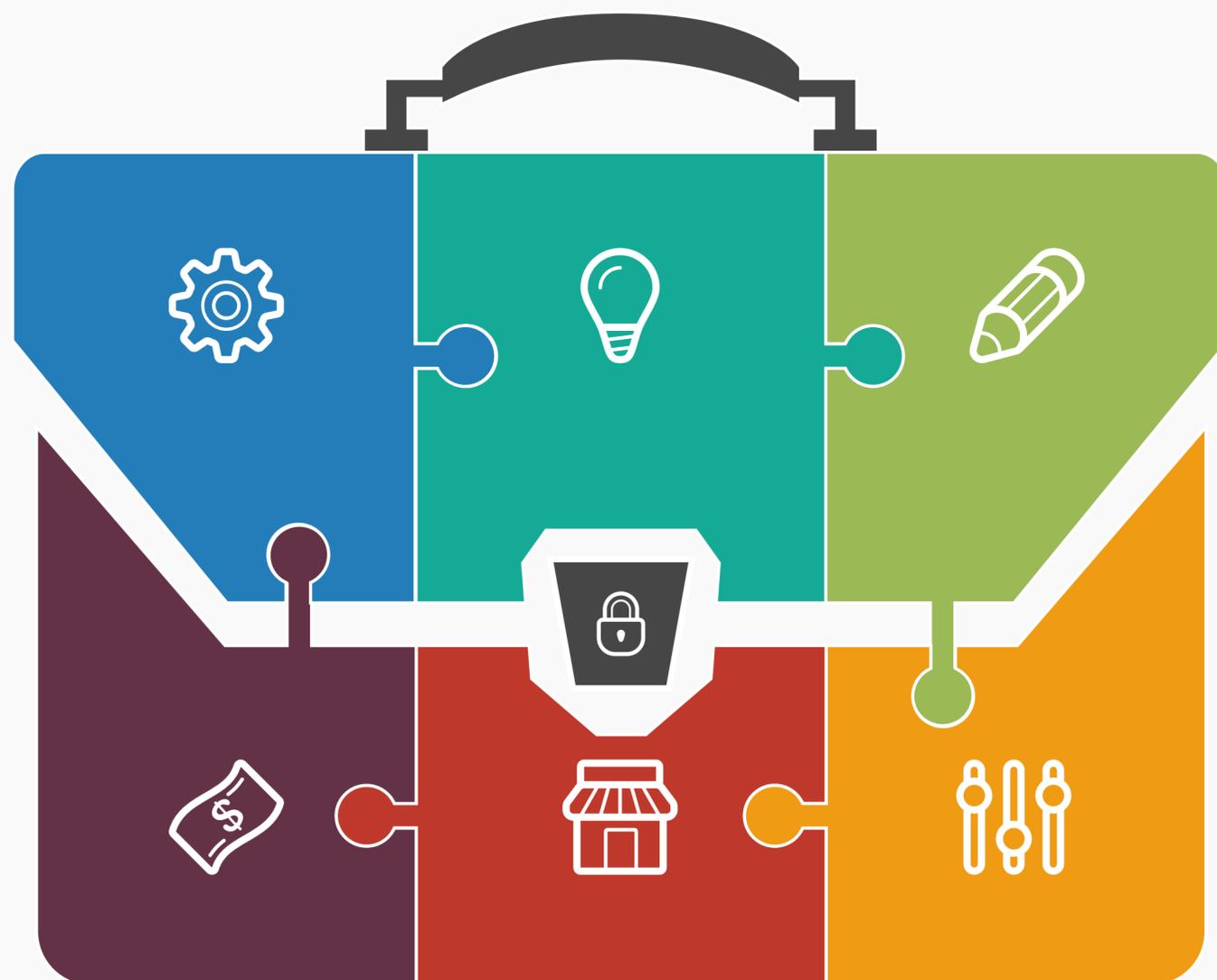


Consensual

onde todos os envolvidos conseguissem chegar a um acordo, mesmo sem se conhecer

O problema dos Generais Bizantinos

O grande problema que o Bitcoin resolveu



- 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



O Blockchain

Infraestrutura de suporte à rede da criptomoeda



O Blockchain é o livro de registros público onde ficam armazenadas todas as transações efetuadas utilizando **criptomoedas**.

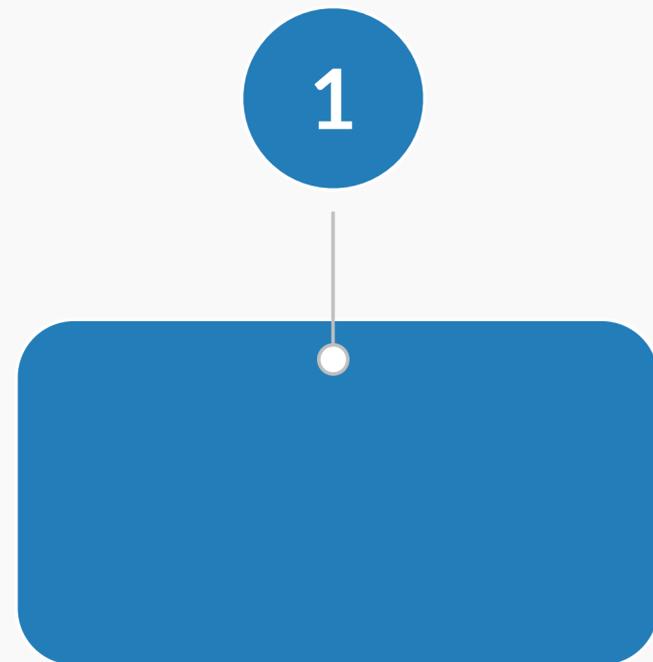
Mecanismos de consenso





O que é um Blockchain?

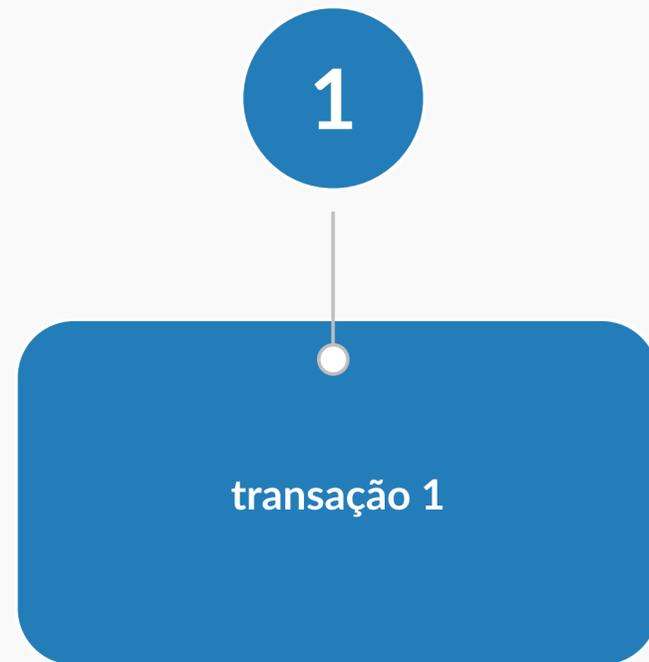
Como funciona essa cadeia de blocos





O que é um Blockchain?

Como funciona essa cadeia de blocos





O que é um Blockchain?

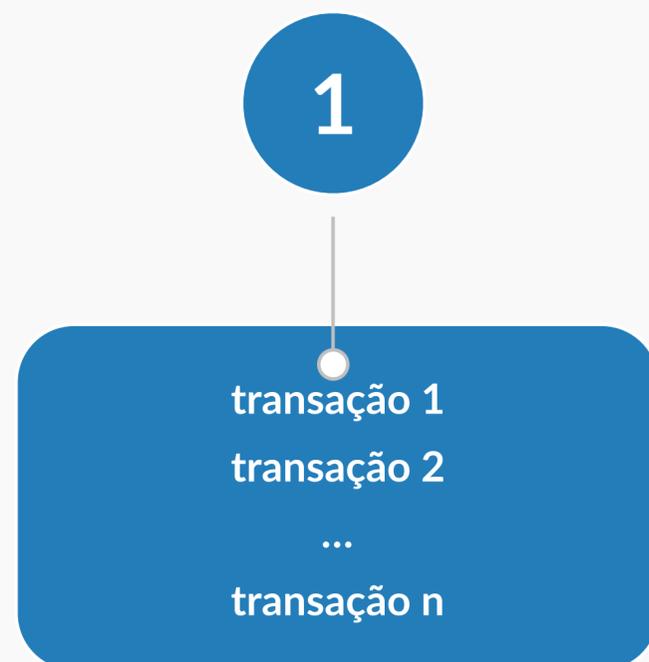
Como funciona essa cadeia de blocos





O que é um Blockchain?

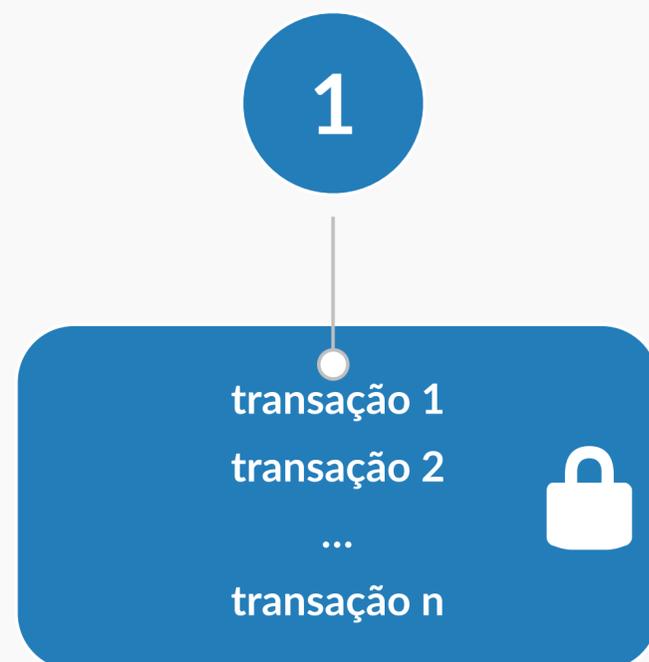
Como funciona essa cadeia de blocos





O que é um Blockchain?

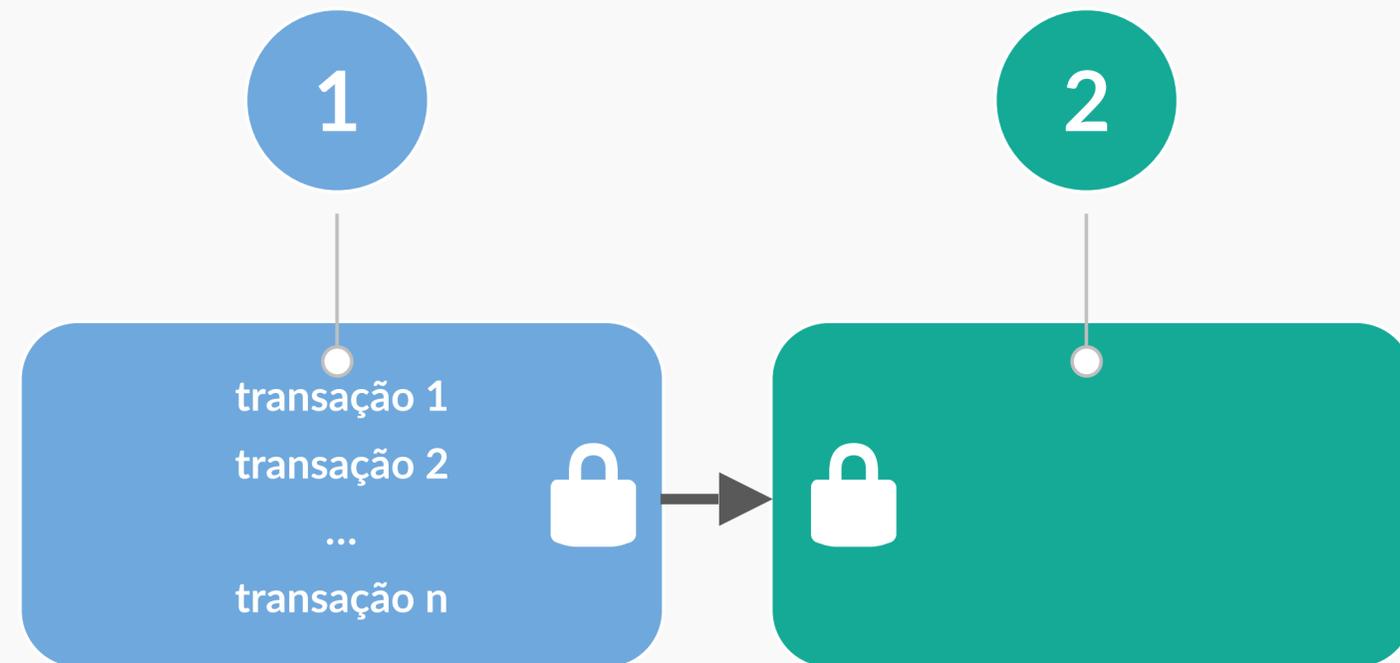
Como funciona essa cadeia de blocos





O que é um Blockchain?

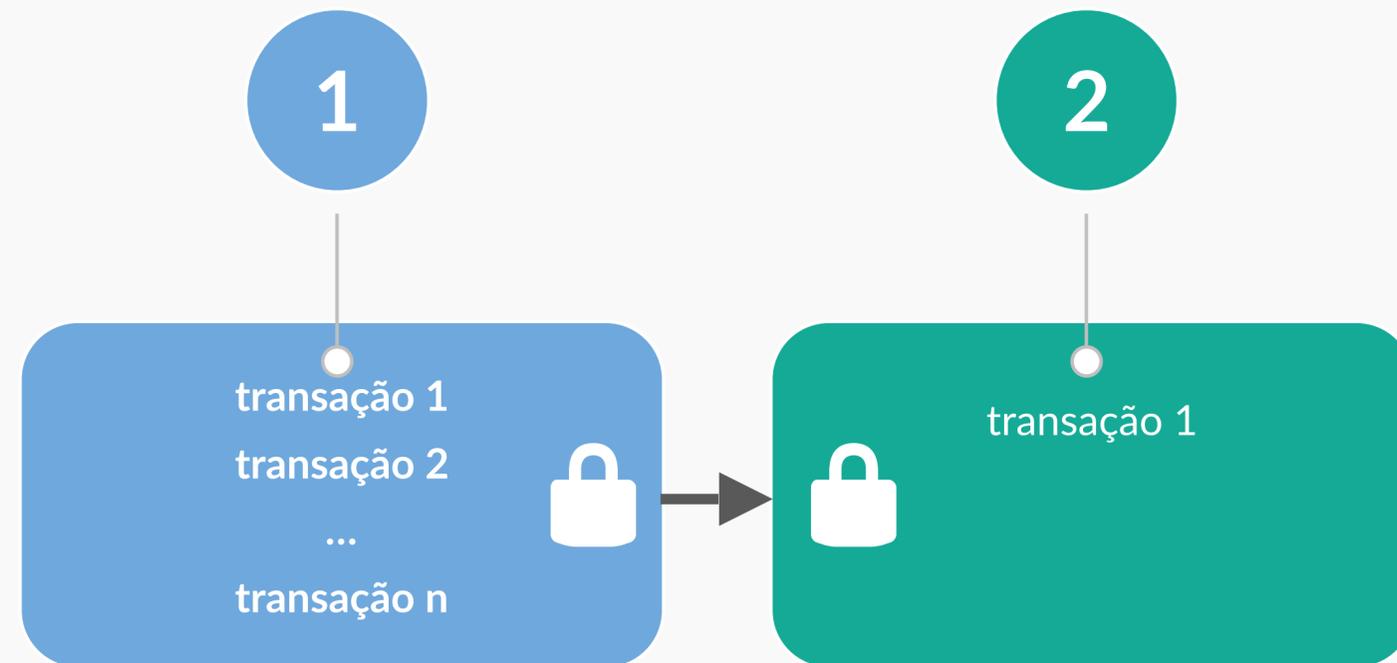
Como funciona essa cadeia de blocos





O que é um Blockchain?

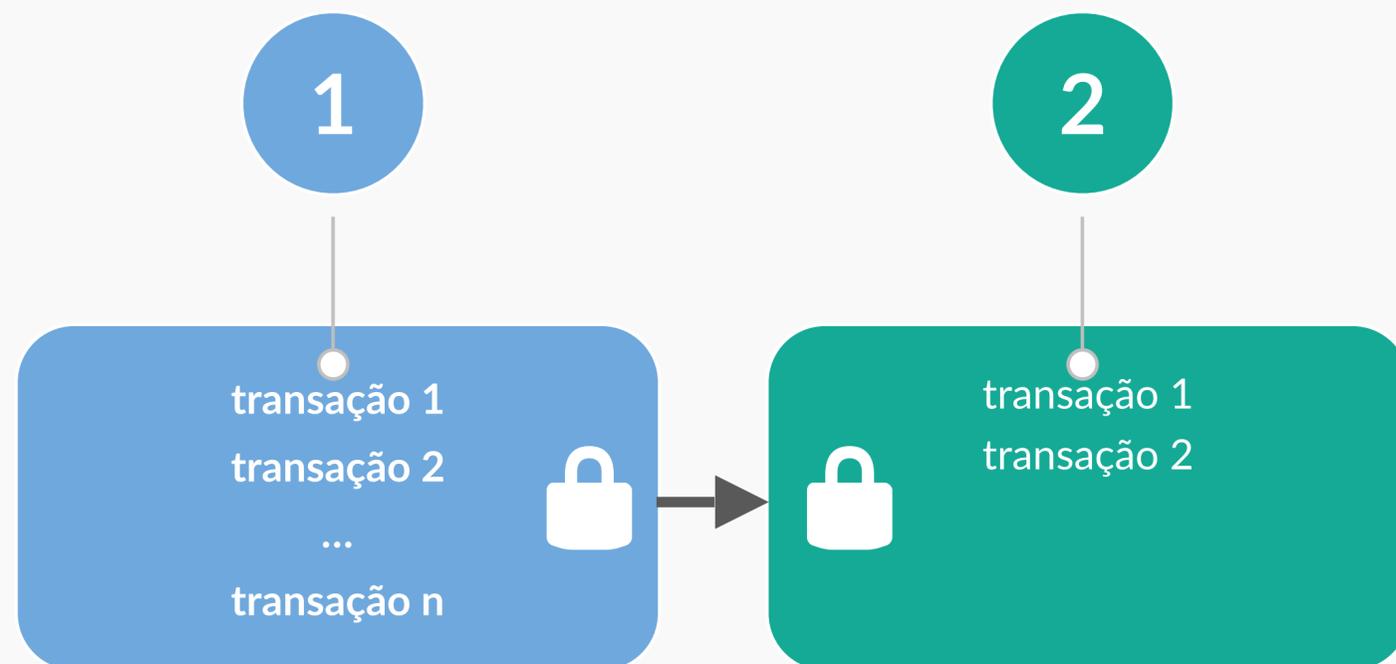
Como funciona essa cadeia de blocos





O que é um Blockchain?

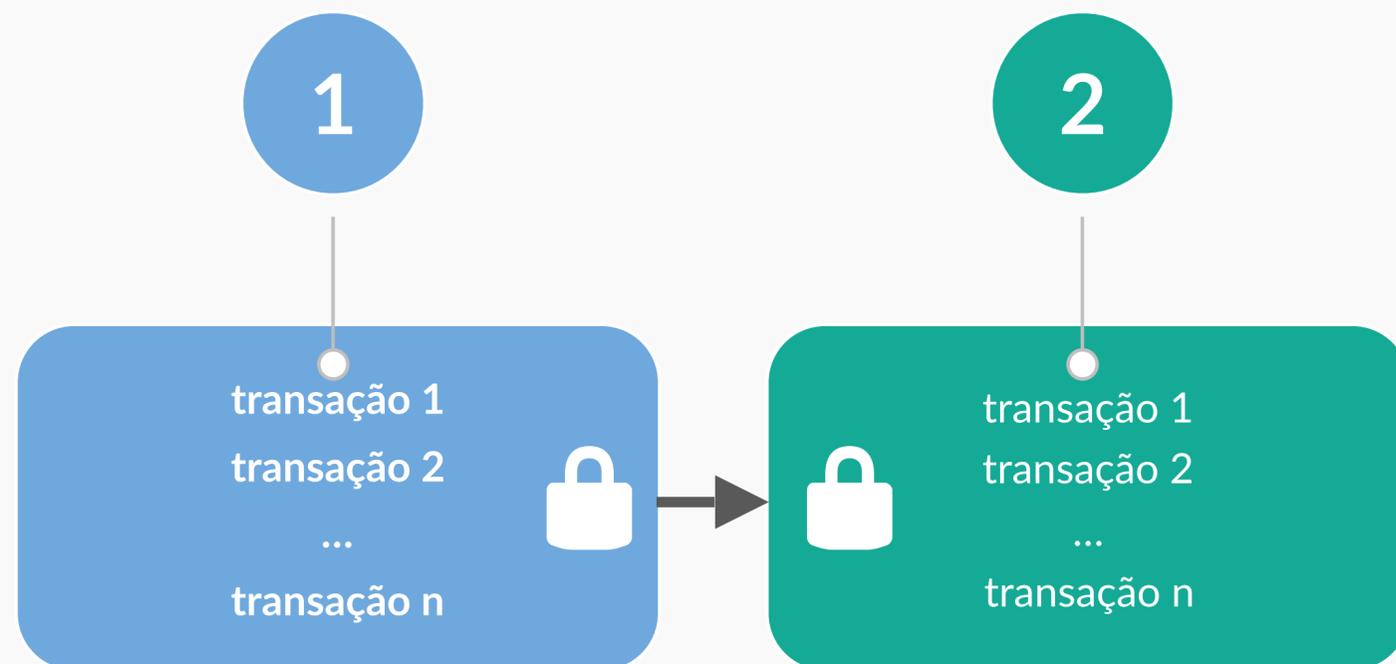
Como funciona essa cadeia de blocos





O que é um Blockchain?

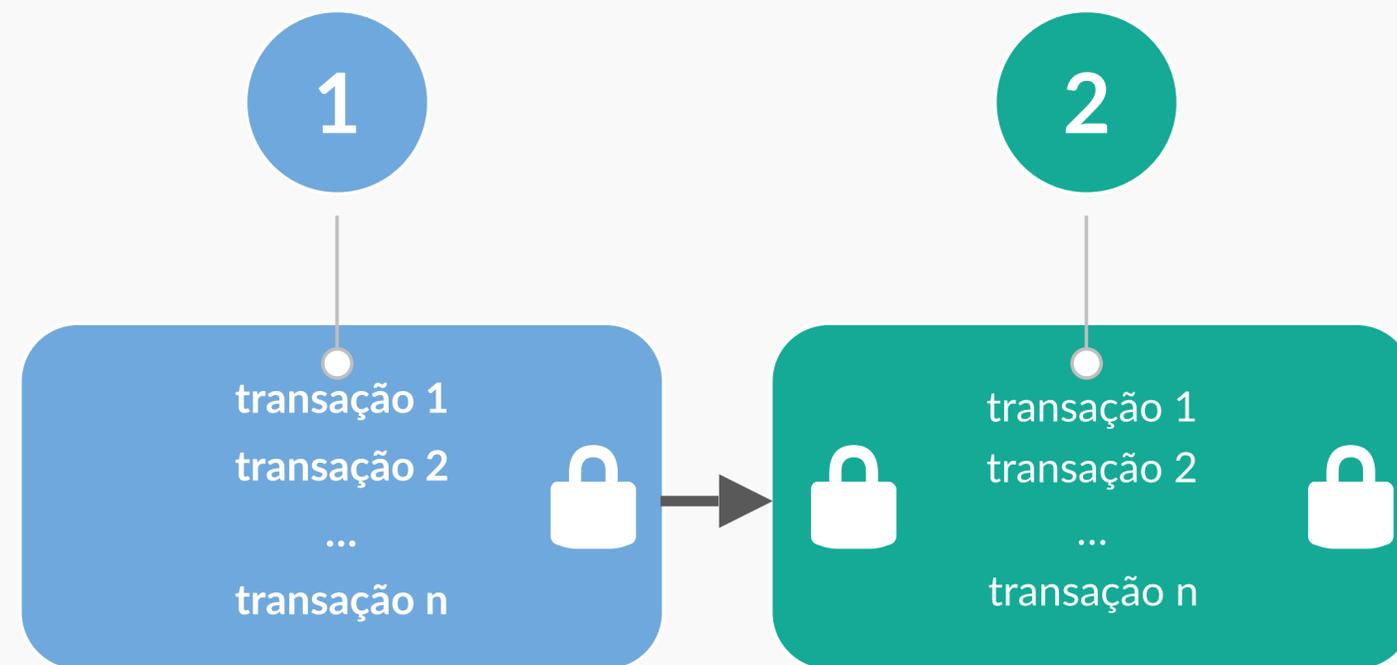
Como funciona essa cadeia de blocos





O que é um Blockchain?

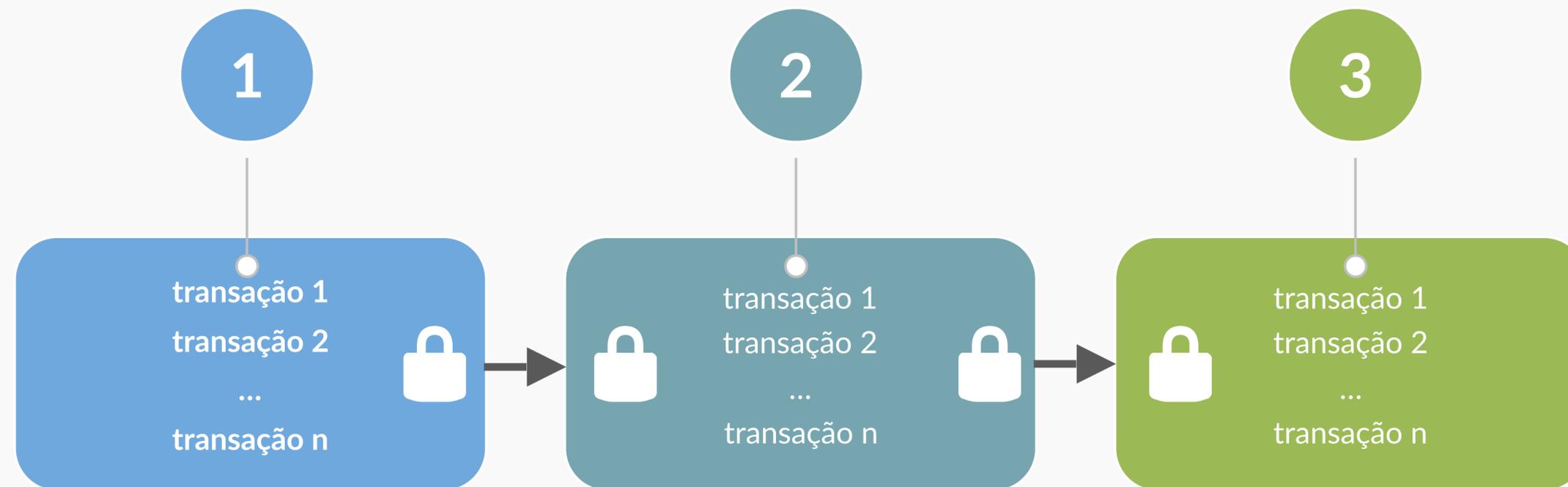
Como funciona essa cadeia de blocos





O que é um Blockchain?

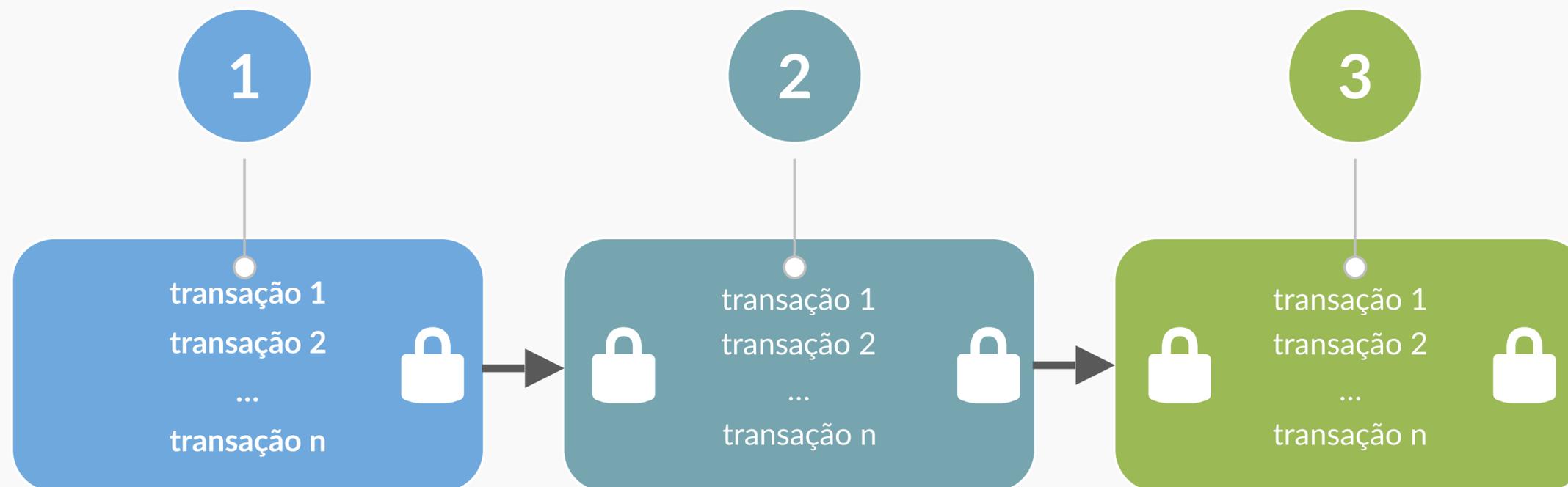
Como funciona essa cadeia de blocos





O que é um Blockchain?

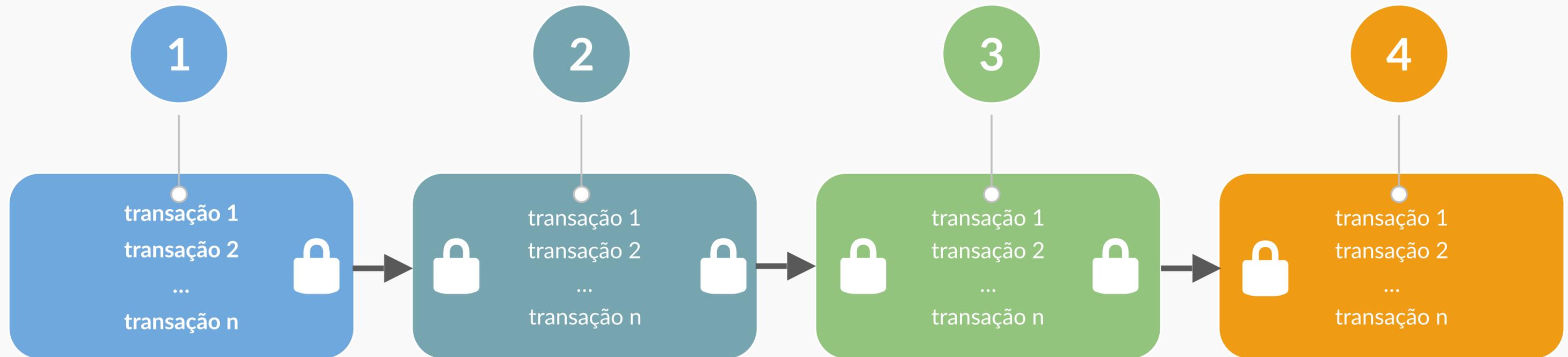
Como funciona essa cadeia de blocos





O que é um Blockchain?

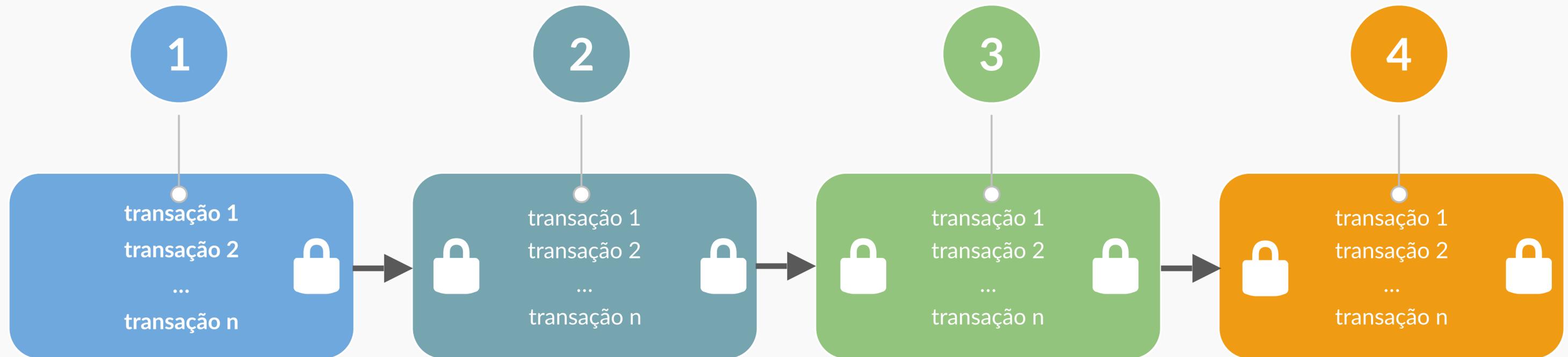
Como funciona essa cadeia de blocos





O que é um Blockchain?

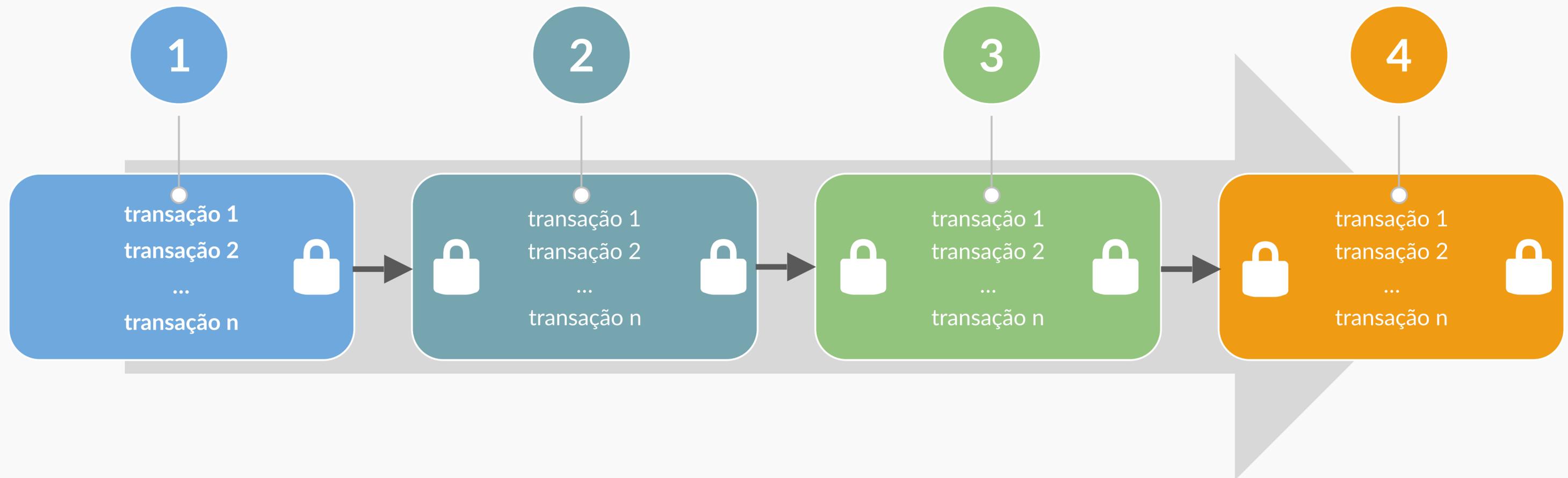
Como funciona essa cadeia de blocos





O que é um Blockchain?

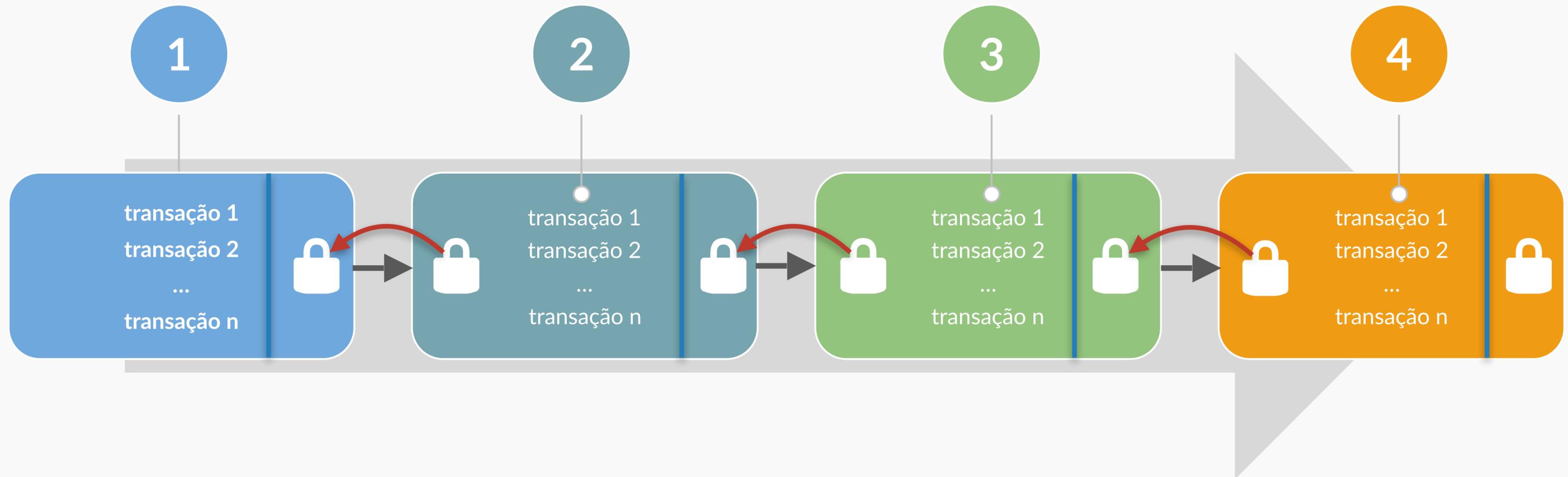
Como funciona essa cadeia de blocos





O que é um Blockchain?

Como funciona essa cadeia de blocos





Da centralização à descentralização

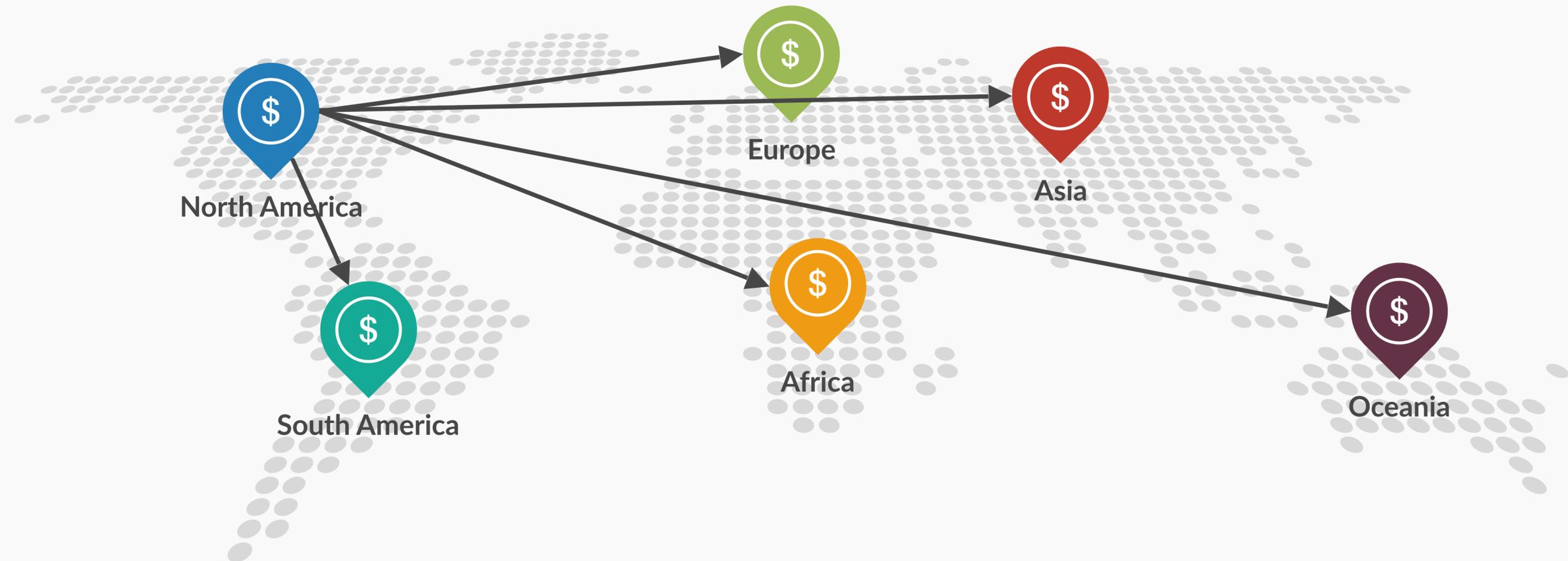
a disrupção do modelo tradicional





Da centralização à descentralização

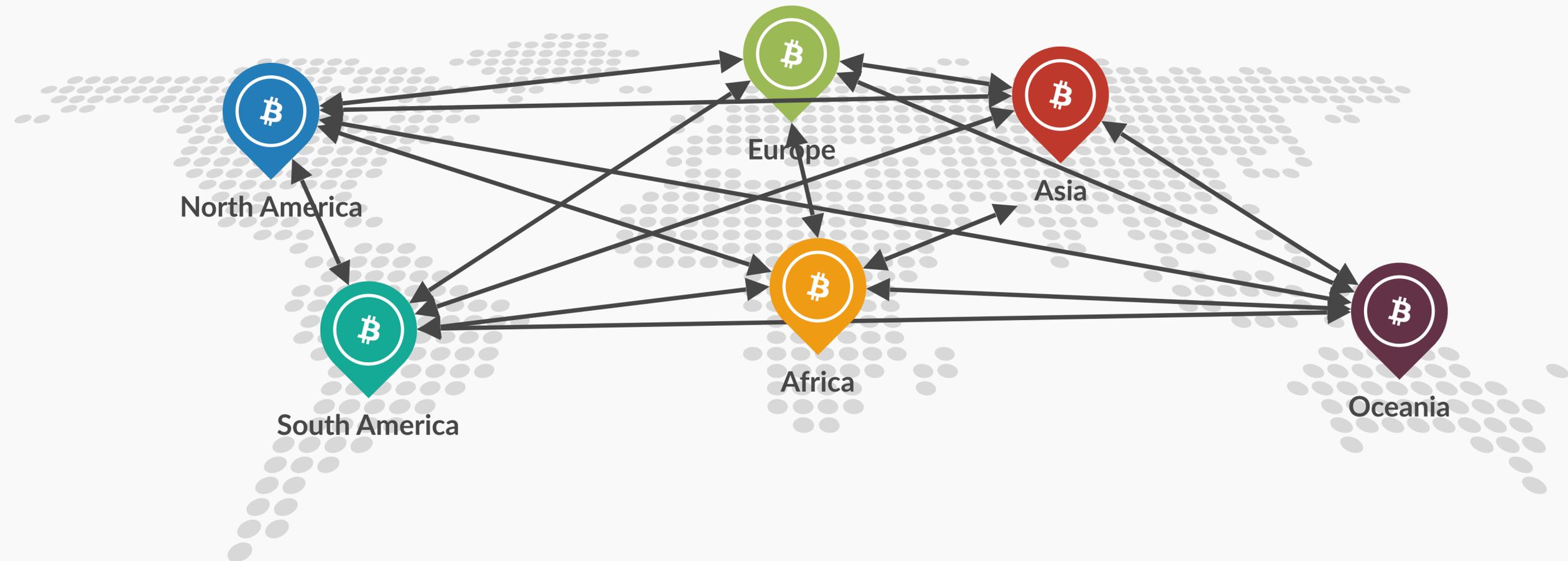
a disrupção do modelo tradicional





Da centralização à descentralização

a disrupção do modelo tradicional





Modelo Híbrido

Os dois modelos juntos



Desmistificando o paradigma Bitcoin-Blockchain

Bitcoin moeda + Bitcoin blockchain

A Criptomoeda, O Blockchain, a referência principal de todas as outras



Bitcoin moeda + Não-bitcoin blockchain

Ref: Blockstream, Blockstack, Rootstock

Side-chains 'pegadas' no blockchain bitcoin de diversas formas



Não-bitcoin moeda + bitcoin blockchain

Ref: Factom, Counterparty, Namecoin

Blockchain do bitcoin é usado, mas a moeda nativa apenas abastece a plataforma



Seis modelos emergentes



Não-bitcoin moeda+Não-bitcoin blockchain

Ref: Ethereum, Z-Cash e 600+ outras

É a independência do Bitcoin



Consenso sem blockchain

Ref: Ripple, Hyperledger, R3CEV

Consenso e confiança descentralizada, sem um blockchain no core

Blockchain neutro

Ref: Tezos, Peernova, Eris

Empresas que utilizam mais de um blockchain para complementar as necessidades





O Blockchain como protocolo



ethereum



O Blockchain como Protocolo

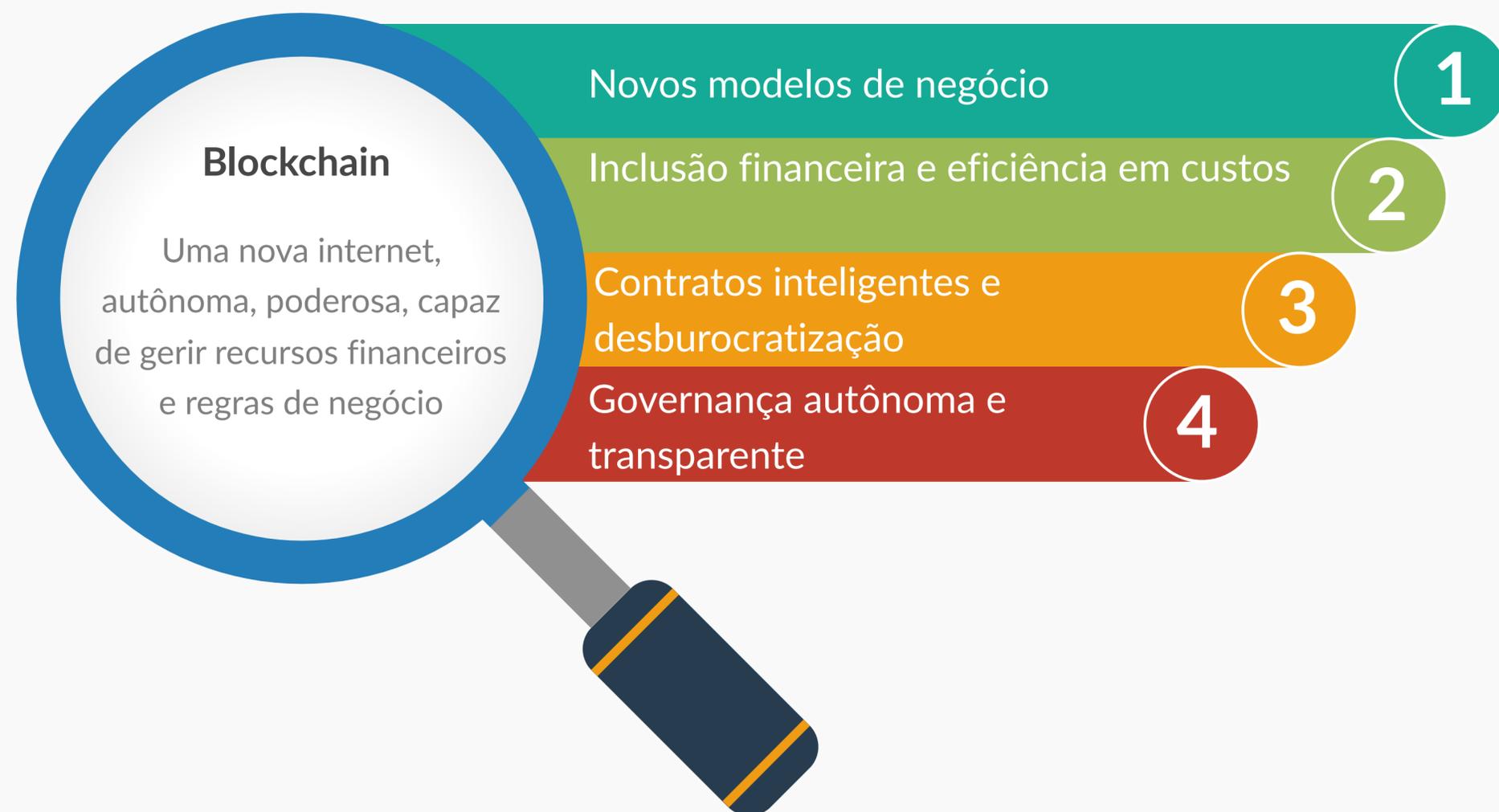
O poder do Blockchain para outros usos além da moeda

Contratos inteligentes

Um **contrato inteligente** é um protocolo de computador feito para facilitar, verificar ou reforçar a negociação ou desempenho de um [contrato](#), sendo capaz de ser executado ou de se fazer cumprir por si só.

Para que seja considerado um contrato inteligente, a transação:

- deve envolver mais do que uma simples transferência de moeda virtual entre duas pessoas (como uma transferência de pagamento, por exemplo),
- deve envolver duas ou mais partes (como todo contrato),
- e a implementação do contrato não deve requerer envolvimento humano direto a partir do momento em que o contrato foi firmado.





Usos potenciais

O Blockchain melhora a eficiência da governança





Distributed Ledger



BIGCHAIN DB

Quorum
by JP Morgan

R3CEV - Corda - Distributed Ledger

Basicamente o melhor do blockchain sem necessidade de criptomoeda (mineração), com novos modelos de consenso, sigilo e permissividade



Distributed ledger tem o potencial de alterar profundamente os serviços financeiros assim como a Internet mudou a mídia e o entretenimento - R3CEV

Comparativos

Comparando as principais tecnologias de Blockchain

	Hyperledger	Ethereum	Bitcoin
Descrição	Blockchain de uso geral	Blockchain de uso geral	Blockchain de transações
Governança	Linux Foundation/IBM	Ethereum Developers	Bitcoin Developers
Moeda	✘	Ether	Bitcoin
Recompensa por mineração	✘	Ether	Bitcoin
Rede de consenso	Plugável	Mineração	Mineração
Rede	Privada ou Pública	Pública ou Privada	Pública
Privacidade	Aberta e/ou Privada	Aberta	Aberta
Smart-contracts	Programável em múltiplas linguagens	Programável em múltiplas linguagens	Limitado a poucos scripts



Casos de uso

—



Slock.it

Fechadura inteligente que faz a própria gestão da sua receita



OneName

Identidade única global



BitNation

plataforma global de governo descentralizado



Nasdaq

Leilões privados
Estônia e-residentes votam
Transferência de ações



Arcade City

'Uber' descentralizado

Exemplos de aplicações

Centenas de empresas pelo mundo estão explorando as possibilidades que o blockchain proporciona



Ujo Music

Streaming de músicas com pagamento direto para artistas



Storj

Armazenamento descentralizado baseado em blockchain



Augur

Plataforma de previsões descentralizadas



La'Zooz

Compartilhamento de carona para destinos similares



Transactive Grid

Permite a geração, compra e venda de energia elétrica para vizinhos

Exemplos de aplicações

Centenas de empresas pelo mundo estão explorando as possibilidades que o blockchain proporciona



Trust Stamp

Compartilhamento de informações pessoais

Reach Incubator



UPort

Vencedores do International Blockchain Week

Consensys



Smart ID (Smart Identity)

Deloitte



ShoCard's

Mobile ID verified in real time

AME Cloud Ventures



OneName BitNation

Veteranos na identificação de pessoas com ID em Blockchain

Exemplos de aplicações para Identidade

Centenas de empresas pelo mundo estão explorando as possibilidades que o blockchain proporciona

OriginalMy.com - 1a empresa brasileira



rankeada no Top100 das empresas mais influentes em Blockchain no mundo

Prova de Autenticidade

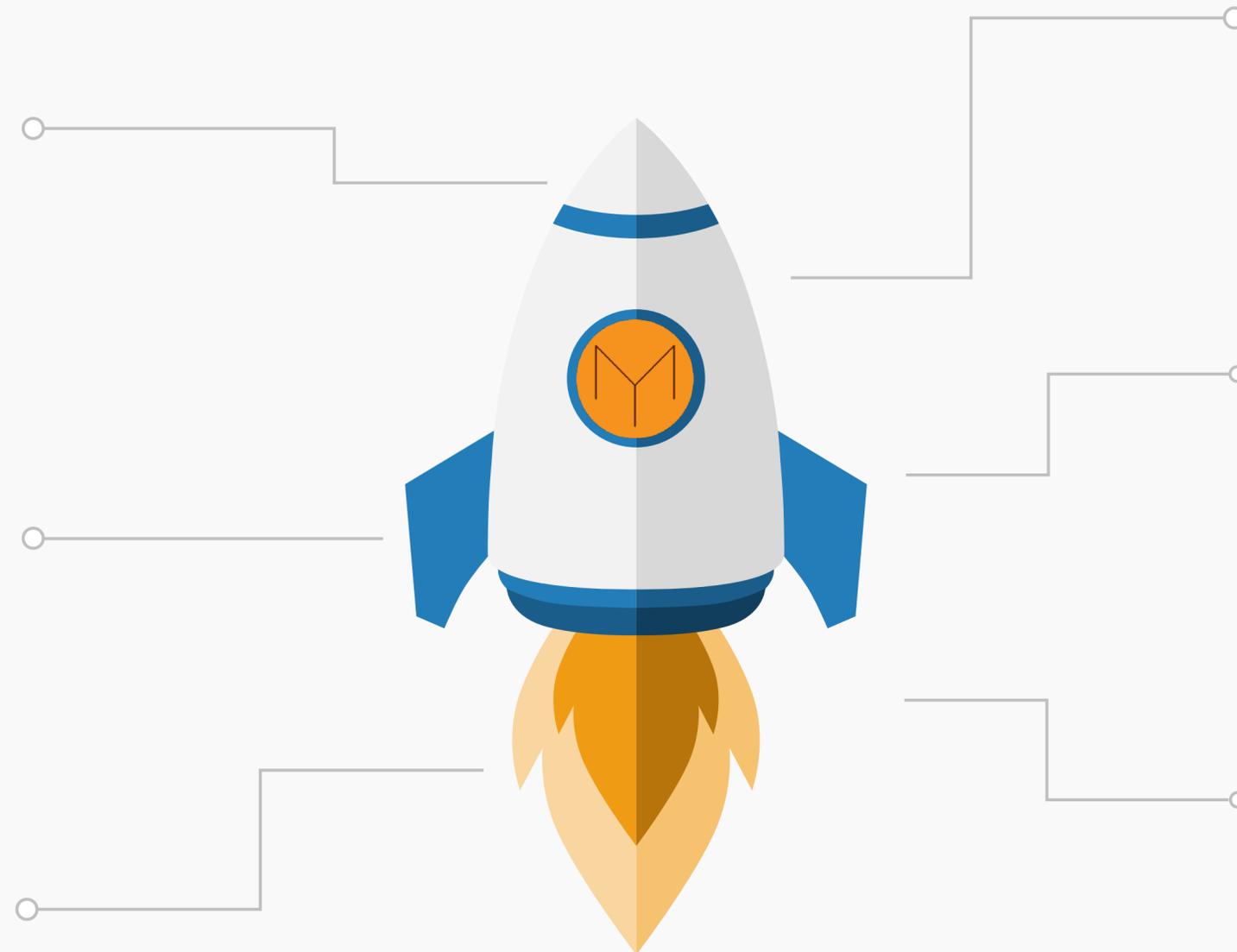
para qualquer tipo de documento digital

Propriedade intelectual

resguarda o direito autoral sobre obras artísticas

Assina contratos

de maneira confidencial, vinculando as partes ao documento e garantindo validade jurídica



Integridade de documentos

comprova a integridade de documentos, mesmo sem armazená-los

Autentica conteúdo na web

emite laudo relatando que determinado conteúdo se encontrava na web em determinado momento

Desenvolve protótipos e provas de conceito

Desenvolvemos provas de conceito em blockchain customizadas para a necessidade do cliente



Conclusões e perguntas

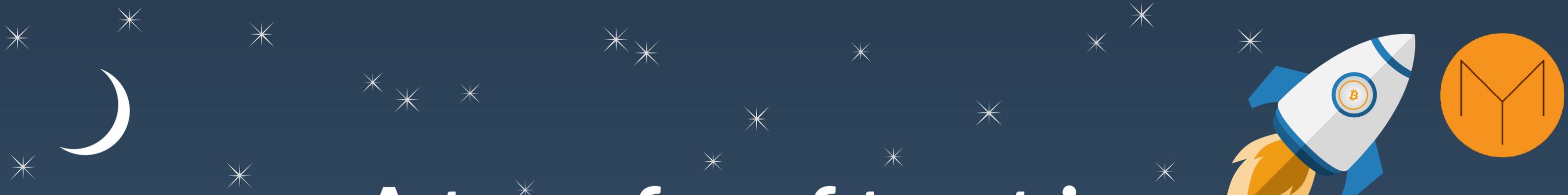
O Blockchain resolve muita coisa (mas não tudo) e impacta diretamente governança



O conceito Blockchain

Se eu declaro que "isto está correto", imediatamente o consenso em rede distribuída pode afirmar em conjunto: "nós concordamos com isto", ou minha afirmação é descartada.

Uma vez que há consenso, há também controle de integridade e imutabilidade. Nada pode ser alterado ou removido, somente adicionado.



A transfer of trust in a trustless world

Blockchain e aplicações

Mar/2017

Edilson Osorio Junior



originalmy.com



osoriojr@originalmy.com



[@eddieoz](https://twitter.com/@eddieoz)



fb.com/osoriojr



github.com/eddieoz



ORIGINAL MY

SIGN CERT