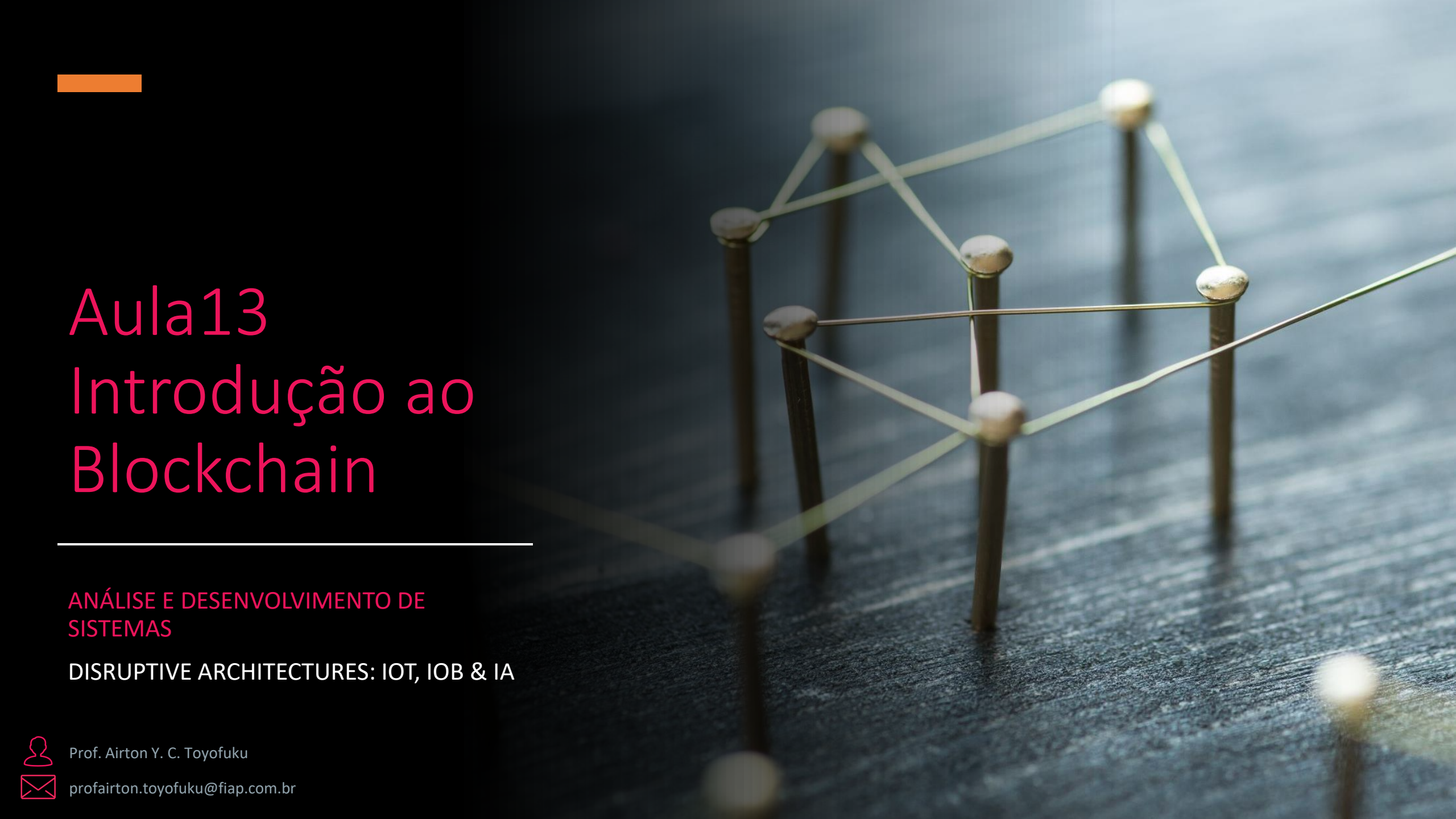
SLIDER

Aula13 Introdução ao Blockchain

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

DISRUPTIVE ARCHITECTURES: IOT, IOB & IA

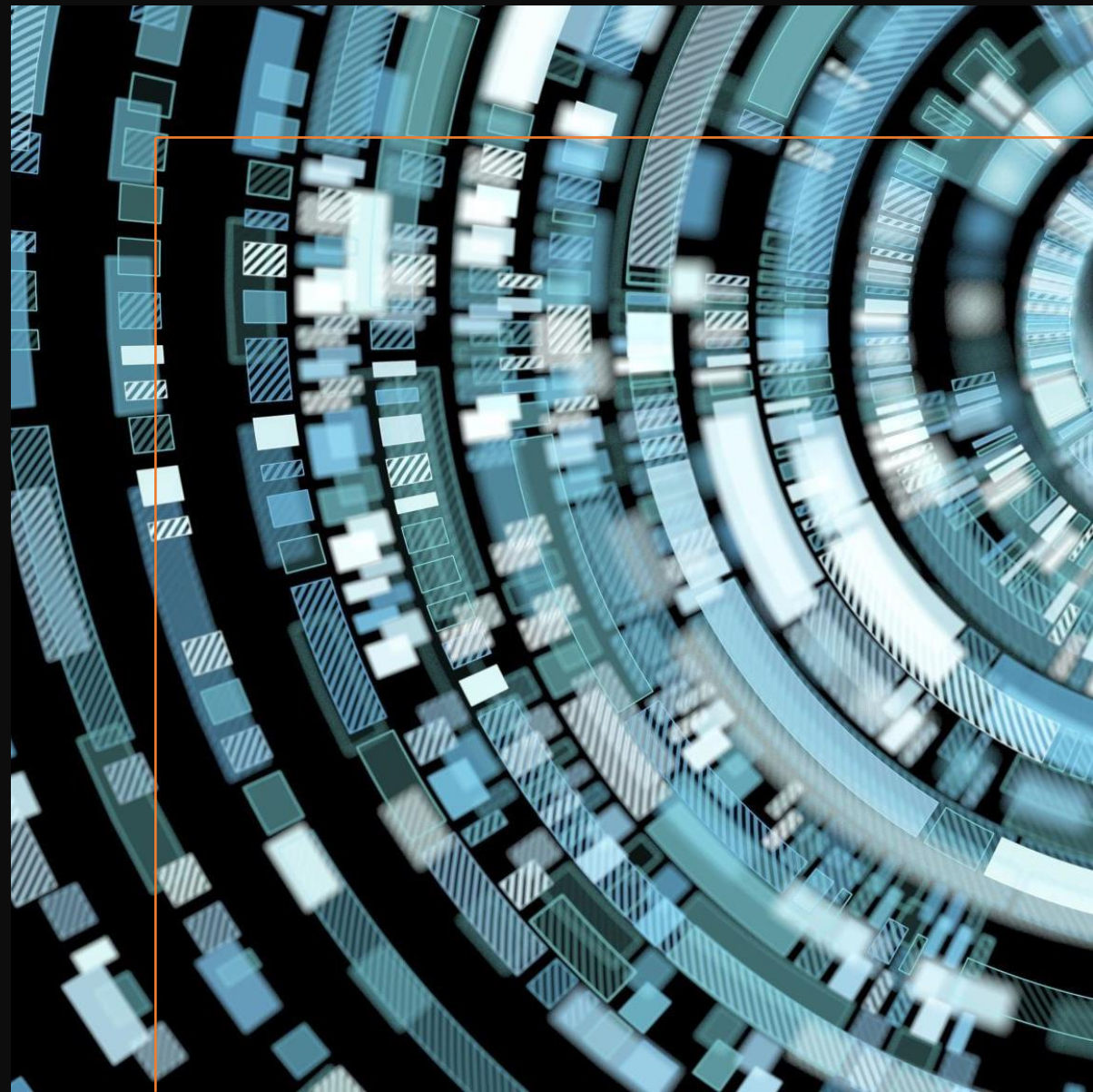


Prof. Airton Y. C. Toyofuku

profairton.toyofuku@fiap.com.br

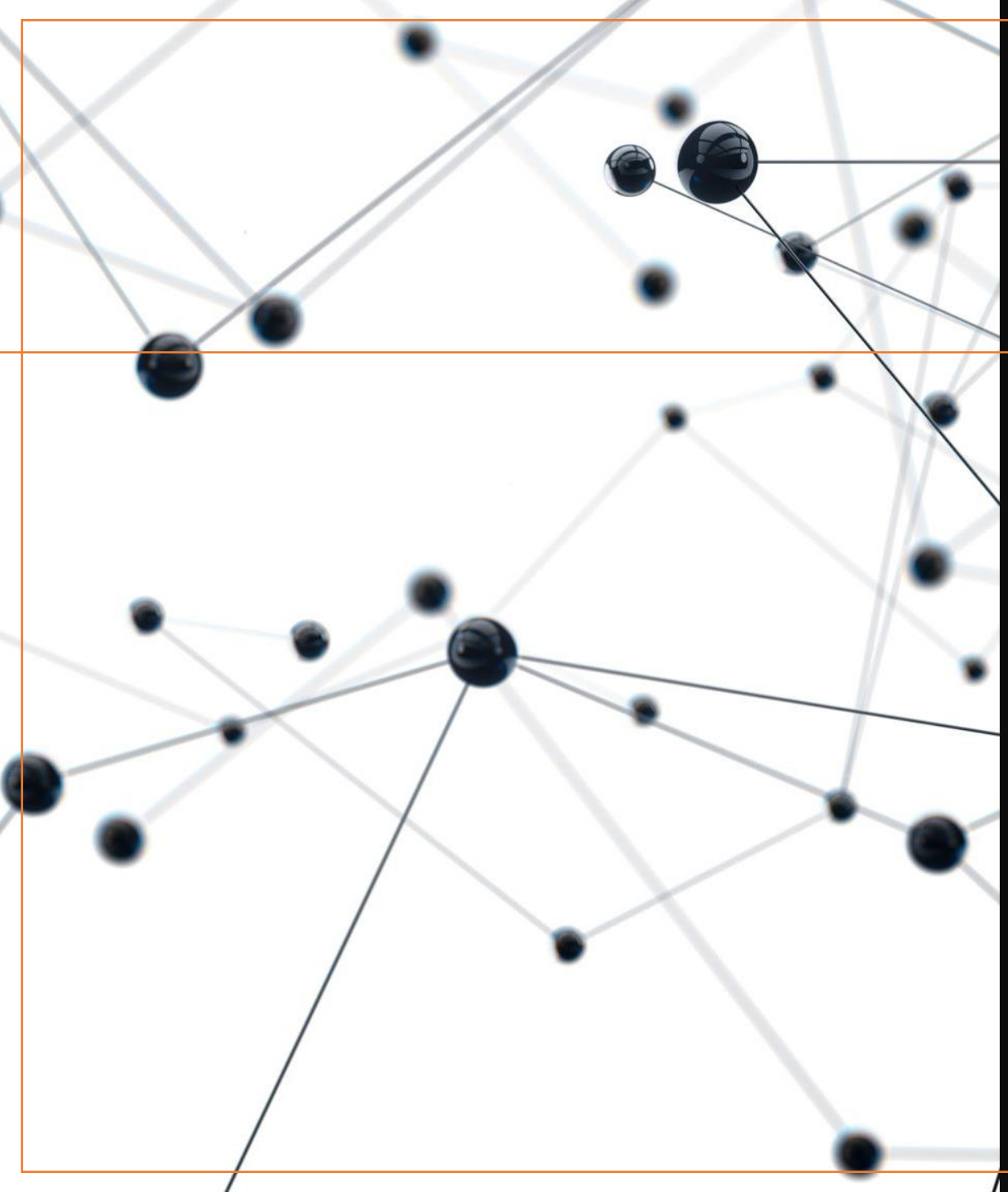
Agenda

- O que é Blockchain?
- Como funciona o Blockchain?
- Quais são as vantangens do Blockchain?
- Quais são as limitações do Blockchain?
- O que é uma Hash?
- O que é um Bloco?
- O que é a Mineração?



O que é Blockchain?

- Blockchain é uma tecnologia de registro distribuído que permite a criação de um banco de dados seguro e imutável. Ela funciona como um livro-razão digital, onde cada transação é registrada em blocos interligados, formando uma cadeia de informações.
- Essa tecnologia foi criada em 2008 para sustentar a criptomoeda Bitcoin, mas hoje é usada em diversas outras aplicações, como contratos inteligentes, votações online, rastreamento de produtos e muito mais.

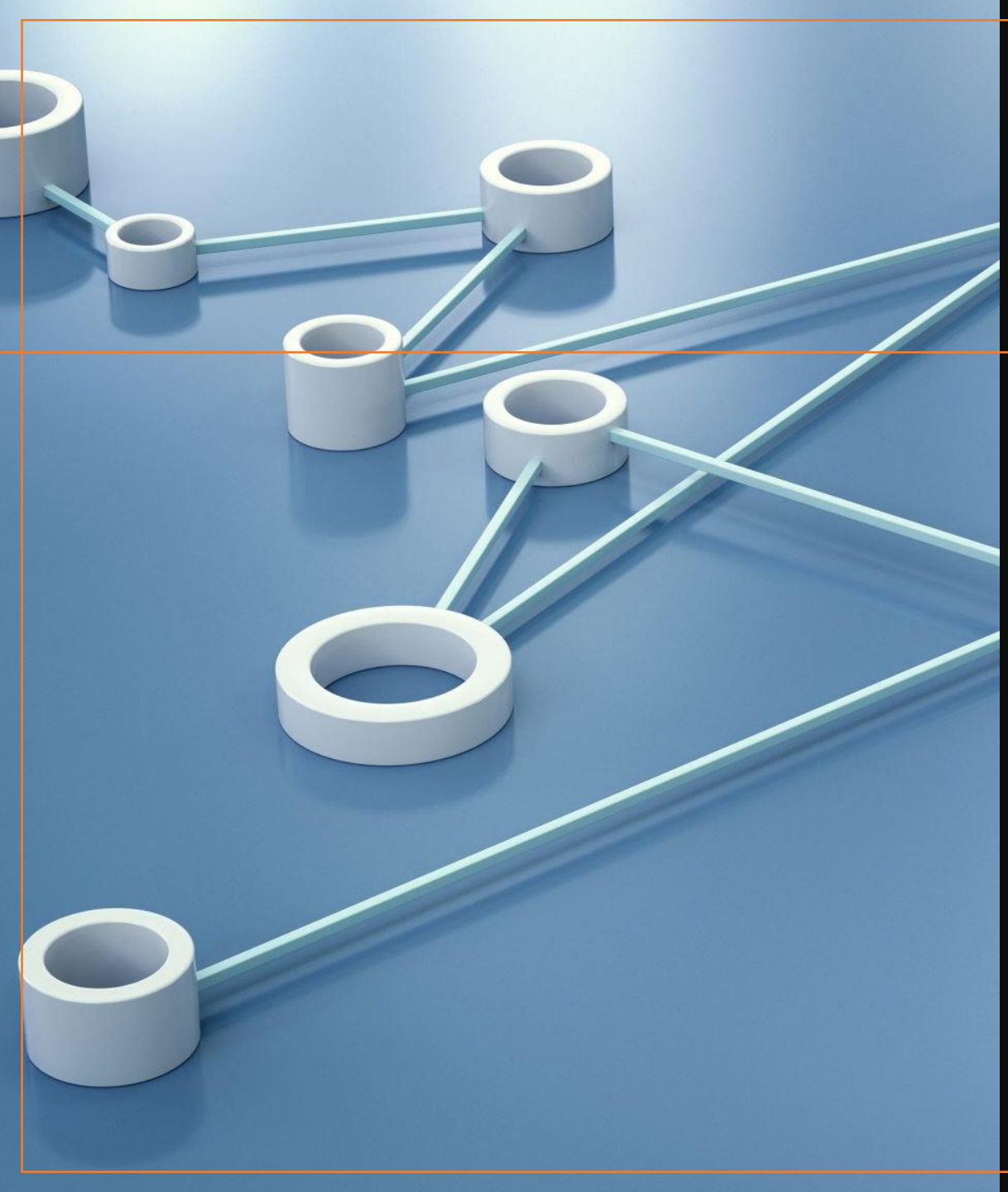


Como funciona o Blockchain?

- O blockchain é composto por uma rede descentralizada de computadores, chamados de nós, que validam e registram as transações.
- Cada bloco contém um conjunto de transações verificadas pelos nós da rede.
- Para garantir a segurança e a integridade dos dados, cada bloco é criptografado e vinculado ao bloco anterior, formando uma cadeia de blocos.
- Isso torna quase impossível alterar ou excluir qualquer informação registrada no blockchain.

Quais são as vantagens do Blockchain?

- Uma das principais vantagens do blockchain é a segurança. Como os dados são criptografados e distribuídos entre vários nós da rede, é muito difícil hackear ou corromper o sistema.
- Além disso, o blockchain é transparente e confiável. Todas as transações são registradas e verificadas pelos nós da rede, eliminando a necessidade de intermediários e reduzindo os riscos de fraudes e erros.



Quais são as limitações do Blockchain?

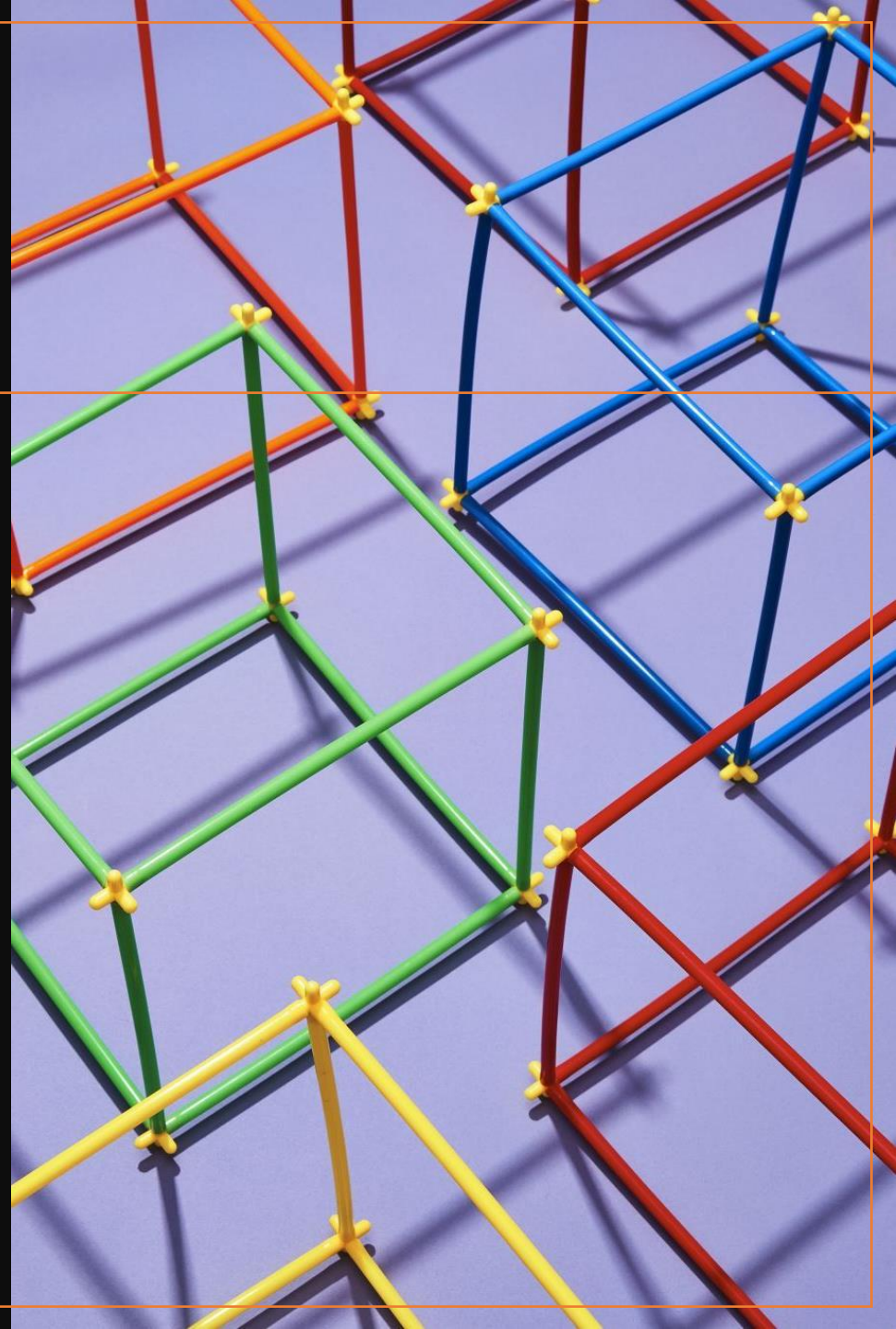
- Apesar de suas vantagens, o blockchain ainda apresenta algumas limitações. Uma delas é a escalabilidade. Como cada nó da rede precisa validar todas as transações, o sistema pode ficar lento e congestionado em momentos de alta demanda.
- Outra limitação é a falta de regulamentação. Como o blockchain é uma tecnologia nova e em constante evolução, ainda não existem leis claras sobre seu uso e aplicação em diferentes setores.

O que é uma Hash?

- hash é uma função matemática que converte dados de entrada de tamanho arbitrário em um valor de tamanho fixo.
- Uma das principais características das funções de hash é que elas são unidirecionais, o que significa que é fácil calcular a hash a partir dos dados de entrada, mas é computacionalmente inviável obter os dados de entrada a partir da hash. Além disso, uma pequena alteração nos dados de entrada resulta em uma hash completamente diferente, o que torna as hashes úteis para detectar qualquer manipulação ou corrupção dos dados.
- As hashes são amplamente utilizadas na tecnologia blockchain para garantir a integridade e a segurança dos dados armazenados na cadeia de blocos. Em um blockchain, cada bloco contém um cabeçalho que inclui um hash. Esse hash é calculado com base nos dados do bloco, como transações, timestamp e hash do bloco anterior.
- A hash de cada bloco é usada para encadear os blocos em uma sequência imutável. Qualquer tentativa de modificar os dados em um bloco posterior resultaria em uma alteração em sua hash, o que por sua vez afetaria as hashes dos blocos subsequentes. Isso torna extremamente difícil alterar retroativamente os dados armazenados em uma blockchain, proporcionando segurança e confiança aos participantes da rede.

O que é um Bloco?

- Um bloco na blockchain é uma estrutura de dados fundamental que compõe a cadeia de blocos. Ele contém um conjunto de transações e outras informações relevantes que são armazenadas de forma segura e imutável na rede.
- Cada bloco geralmente possui os seguintes componentes:
  - Cabeçalho do bloco: É composto por metadados, como um hash do bloco anterior, um timestamp (carimbo de data e hora) que indica quando o bloco foi minerado, um nonce (número arbitrário usado na mineração) e outros campos utilizados para verificar a integridade do bloco.
  - Dados das transações: São as transações que foram agrupadas no bloco. Isso pode incluir informações sobre remetentes, destinatários, valores transferidos e quaisquer outros dados relevantes.
  - Hash do bloco: É um valor numérico único e fixo que é gerado a partir do cabeçalho do bloco e dos dados das transações. Essa hash serve como identificador exclusivo do bloco e ajuda a garantir a integridade dos dados.
- Após serem validados e verificados pelos participantes da rede, os blocos são adicionados à cadeia de blocos em uma sequência cronológica. Cada bloco contém o hash do bloco anterior, formando assim uma cadeia contínua de blocos interligados.
- A adição de novos blocos à cadeia é geralmente feita por meio de um processo chamado mineração, no qual os mineradores competem para resolver problemas computacionais complexos. O minerador que encontrar a solução primeiro tem o direito de adicionar o próximo bloco à cadeia e recebe uma recompensa pelo trabalho realizado (como criptomoedas).



O que é Mineração?

- A mineração em blockchain é um processo fundamental que permite a adição de novos blocos à cadeia de blocos (blockchain). É um mecanismo essencial para manter a segurança e a integridade da rede blockchain, especialmente em blockchains baseadas em prova de trabalho (Proof of Work), como é o caso do Bitcoin.
- Na mineração, os participantes da rede, conhecidos como mineradores, competem entre si para resolver um problema computacional complexo. Esse problema requer poder computacional significativo e consome recursos, como eletricidade e tempo de processamento. O primeiro minerador a encontrar a solução correta para o problema recebe o direito de adicionar o próximo bloco à blockchain.
- O problema computacional a ser resolvido é projetado de tal forma que exige um esforço computacional considerável para encontrá-lo, mas é relativamente fácil de verificar uma vez que a solução é encontrada. Esse mecanismo garante que os mineradores gastem tempo e recursos para adicionar um novo bloco, o que evita a criação arbitrária de blocos e protege a rede contra ataques maliciosos.
- Ao encontrar a solução correta, o minerador cria um novo bloco contendo transações válidas e outras informações relevantes, como o hash do bloco anterior. Em seguida, o novo bloco é propagado pela rede para que outros participantes possam verificar e validar as transações. Uma vez que o bloco é validado pelos nós da rede, ele é adicionado à blockchain e se torna parte da sequência imutável de blocos.
- Além de adicionar novos blocos, a mineração também desempenha um papel importante na segurança da blockchain. Como a mineração exige um grande poder computacional, qualquer tentativa de modificar ou reverter transações anteriores exigiria uma quantidade impraticável de recursos, tornando a rede blockchain altamente segura contra ataques de hackers.
- Vale ressaltar que nem todas as blockchains utilizam a mineração como mecanismo de consenso. Existem outras abordagens, como a prova de participação (Proof of Stake) e a prova de autoridade (Proof of Authority), que não exigem o processo de mineração, mas utilizam outros métodos para validar e adicionar blocos à blockchain.

Copyright © 2023 Prof. **Airton Y. C. Toyofuku**

This presentation was totally made with Microsoft AI