Blockchain e aplicações, criando um bloco na prática

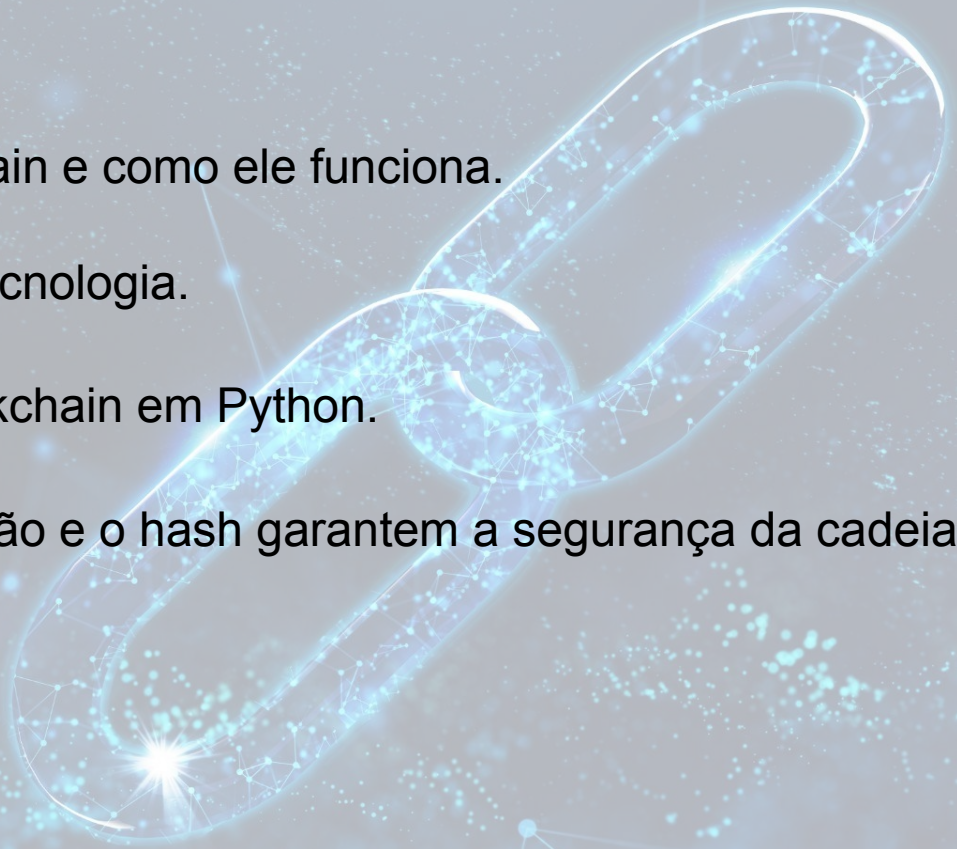
Aula 08

Prof. Msc. Francisco de Assis de Souza Rodrigues

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO

🧠 Objetivos

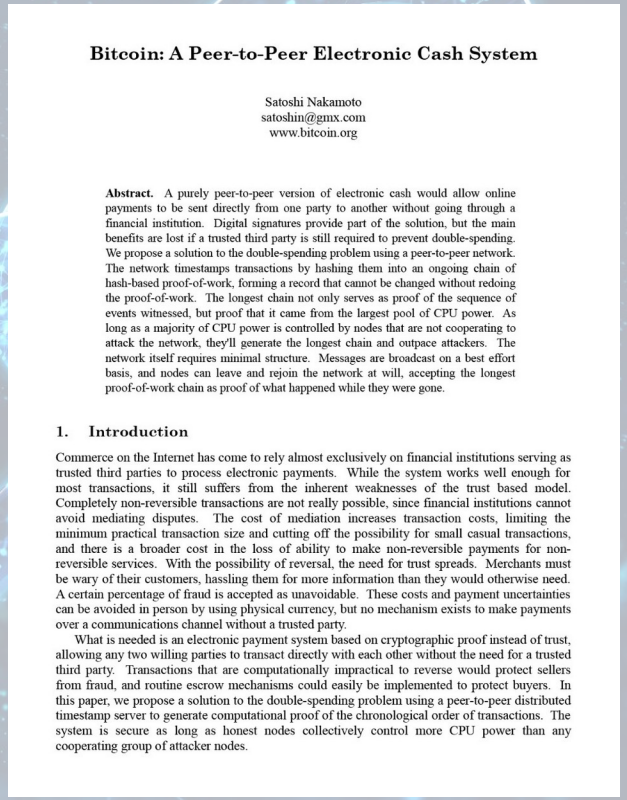
- Compreender o que é blockchain e como ele funciona.
- Explorar aplicações reais da tecnologia.
- Implementar um bloco de blockchain em Python.
- Discutir como a descentralização e o hash garantem a segurança da cadeia.



Origem do Blockchain: Breve História

Primeira Publicação:

- **Título:** *"Bitcoin: A Peer-to-Peer Electronic Cash System"*
- **Autor:** Satoshi Nakamoto
- **Data:** 31 de outubro de 2008
- **Link:** bitcoin.org/bitcoin.pdf
- **Resumo:** Proposta de um sistema descentralizado para transferências de dinheiro sem necessidade de intermediários (como bancos), utilizando uma cadeia de blocos e prova de trabalho para validar transações.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

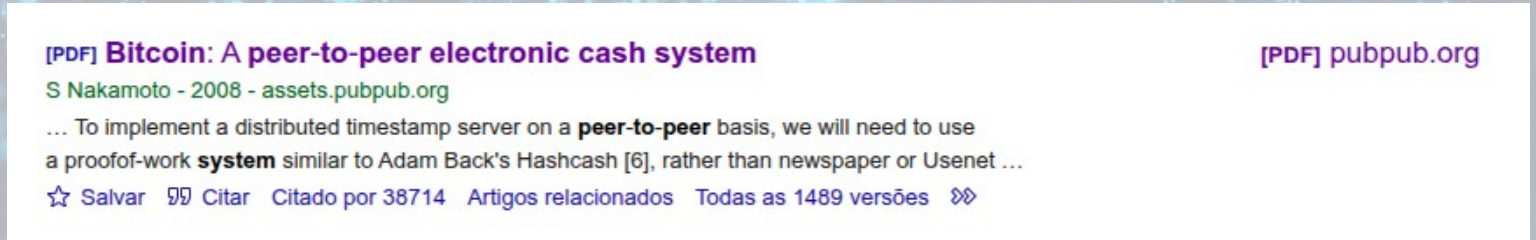
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

https://assets.pubpub.org/d8wct41f/31611263538139.pdf

🕰️ Origem do Blockchain: Breve História

🗒️ Linha do tempo resumida:

- **1991** – Stuart Haber e W. Scott Stornetta propõem um sistema de carimbo do tempo usando criptografia.
- **2008** – Publicação do white paper de Satoshi Nakamoto.
- **2009** – Lançamento do software do Bitcoin e mineração do **bloco gênese**.
- **2015** – Lançamento do **Ethereum**, com suporte a contratos inteligentes.
- **2020+** – Expansão para NFTs, DeFi e uso em governos e empresas.



O que é Blockchain?

Blockchain é uma estrutura de dados distribuída e imutável, que registra transações de forma segura e transparente. Em vez de estar armazenado em um único servidor, o registro é compartilhado entre diversos participantes de uma rede.

Estrutura de um bloco:

- **Dados:** informações da transação (ex: valor, remetente, destinatário).
- **Hash:** código único gerado a partir do conteúdo do bloco (função hash).
- **Hash do bloco anterior:** conecta os blocos em sequência, formando uma cadeia.

Cadeia de blocos (Blockchain): cada novo bloco é vinculado ao anterior por seu hash. Isso torna praticamente impossível alterar dados anteriores sem modificar todos os blocos seguintes — o que exige consenso da rede.

Principais Características do Blockchain

🔒 **Imutabilidade:** uma vez gravado, o dado não pode ser alterado sem consenso da rede.

🔍 **Transparência:** todos os participantes têm acesso ao mesmo histórico.

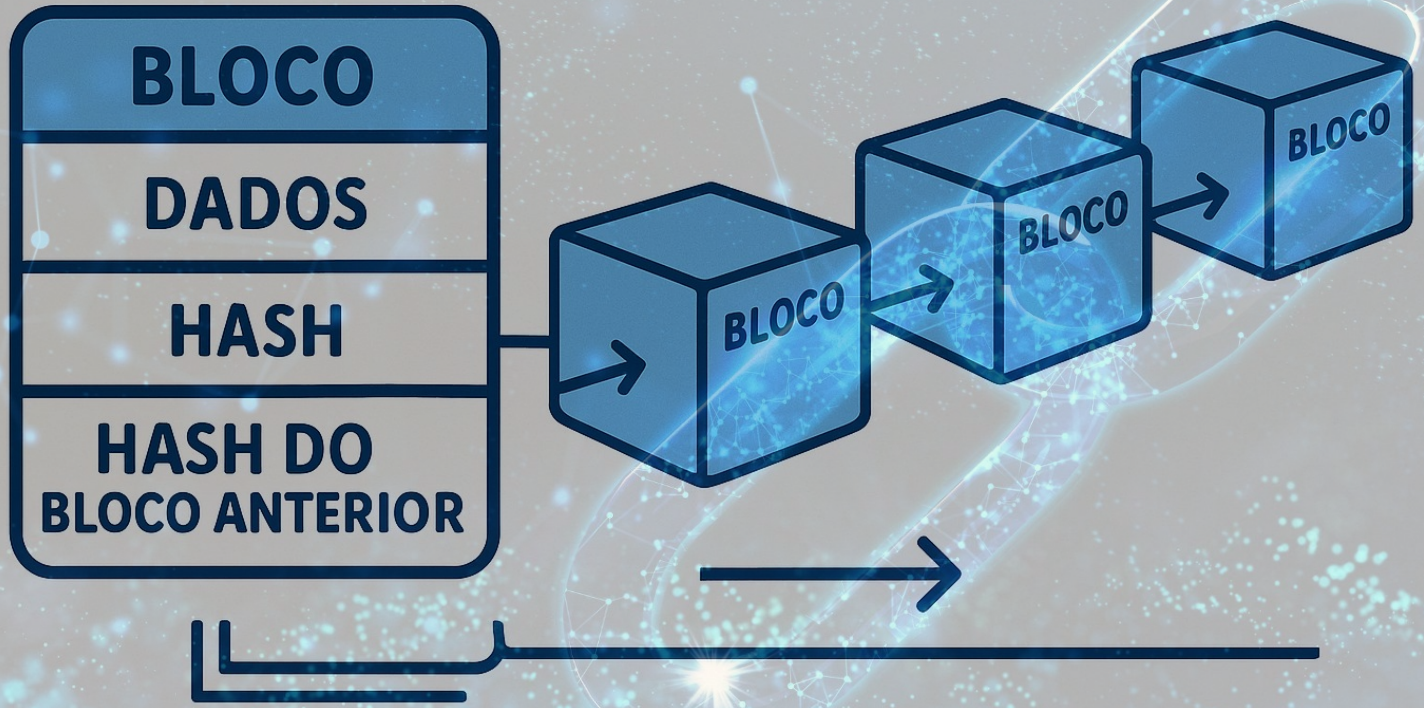
🌐 **Descentralização:** não depende de uma autoridade central. A rede é distribuída entre os participantes (nós).

🔐 **Segurança via criptografia:** utiliza funções hash (ex: SHA-256) para garantir integridade e autenticidade dos dados.

Aplicações Reais do Blockchain

- 💰 **Criptomoedas:** como Bitcoin e Ethereum — usam blockchain para registrar transações sem um banco central.
- 🚚 **Supply Chain (cadeia de suprimentos):** rastreamento de produtos da origem até o consumidor, aumentando a confiabilidade e reduzindo fraudes.
- 📜 **Contratos Inteligentes (Smart Contracts):** códigos executáveis armazenados na blockchain que são autoexecutáveis quando condições são atendidas (ex: liberar pagamento automático).
- 🧾 **Certificação e Registro Digital:** diplomas, certificados ou propriedade de ativos podem ser registrados de forma pública e verificável.
- 🗳️ **Votação Digital:** sistemas de votação baseados em blockchain aumentam a confiança e reduzem a possibilidade de fraudes.

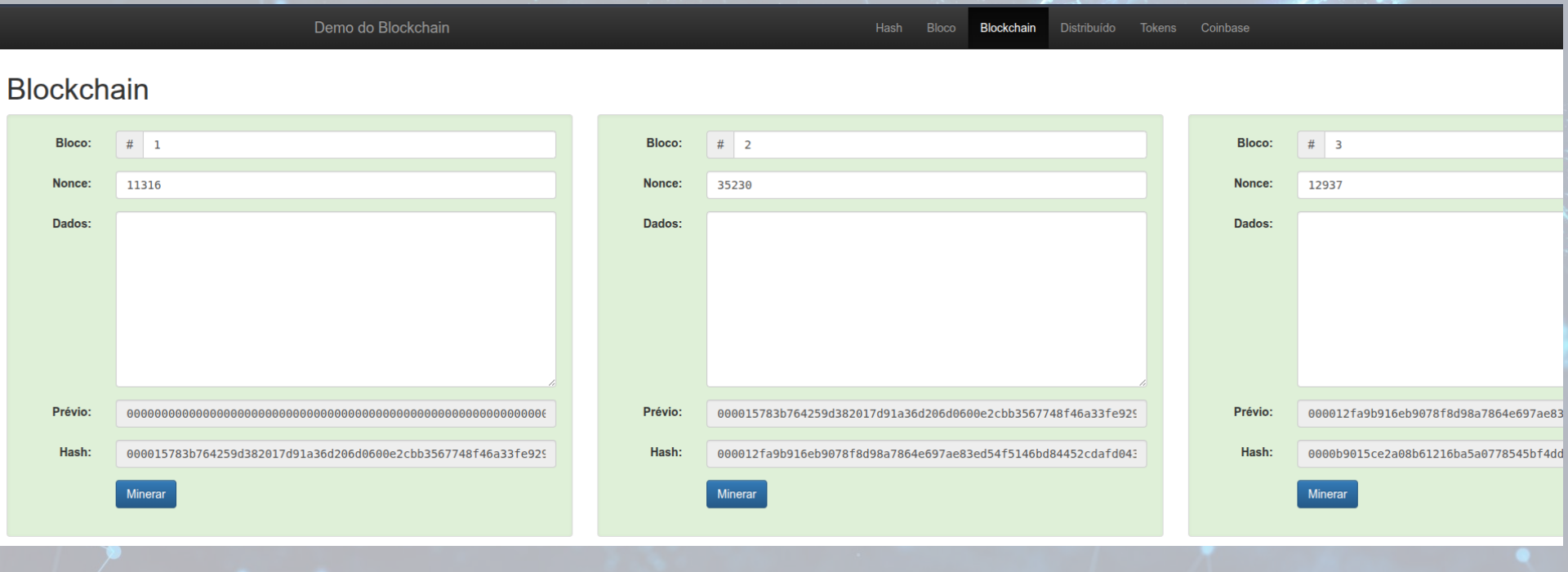
ESTRUTURA DE UM BLOCO



CADEIA DE BLOCOS

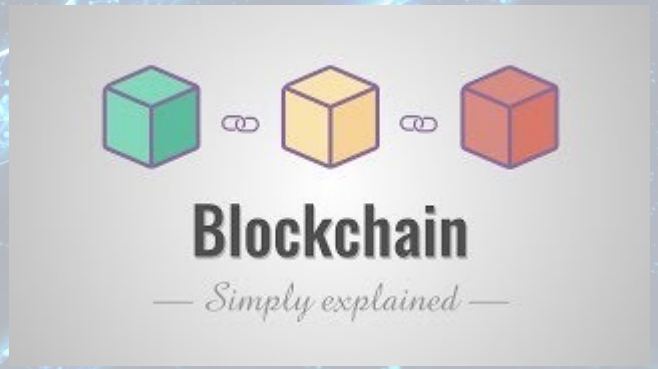
Blockchain Demo

https://andersbrownworth.com/blockchain



Indicação de Vídeo

https://www.youtubeeducation.com/watch?v=SSo_EIwHSd4



Conceitos Técnicos Básicos

🧮 **Hashing com SHA-256:** função criptográfica que transforma qualquer entrada em uma sequência de 256 bits. Muito usada no Bitcoin.

⛏️ **Prova de Trabalho (Proof of Work – PoW):** mecanismo que exige que os nós resolvam problemas matemáticos complexos para validar blocos. Garante segurança, mas consome muita energia.

🔗 **Encadeamento de blocos:** cada bloco armazena o hash do anterior, criando uma ligação entre eles. Se um bloco for alterado, o hash muda, invalidando toda a cadeia.

Criar um bloco simples em Python

https://colab.research.google.com/drive/1xiONxpsSm7VJrH3DdnPh0Fr3Qvmt7jZ1?usp=sharing



Criar um bloco simples em Python

https://colab.research.google.com/drive/1xiONxpsSm7VJrH3DdnPh0Fr3Qvmt7jZ1?usp=sharing



Bibliografia

KUNTZ, João. Blockchain Ethereum: fundamentos de arquitetura, desenvolvimento de contratos e aplicações. São Paulo, SP: Casa do Código, 2022. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/212861. Acesso em: 09 maio 2025.



Bibliografia

CHAVES, Iara. Blockchain e criptomoedas. 1. ed. Curitiba: Intersaberes, 2021. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/194850. Acesso em: 09 maio 2025.



Bibliografia

CAVAGNARI, Daniel Weigert; MUNHOZ, Antonio Siemsen. Blockchain e criptomoedas. Curitiba, PR: Contentus, 2021. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/219983. Acesso em: 09 maio 2025.



Bibliografia

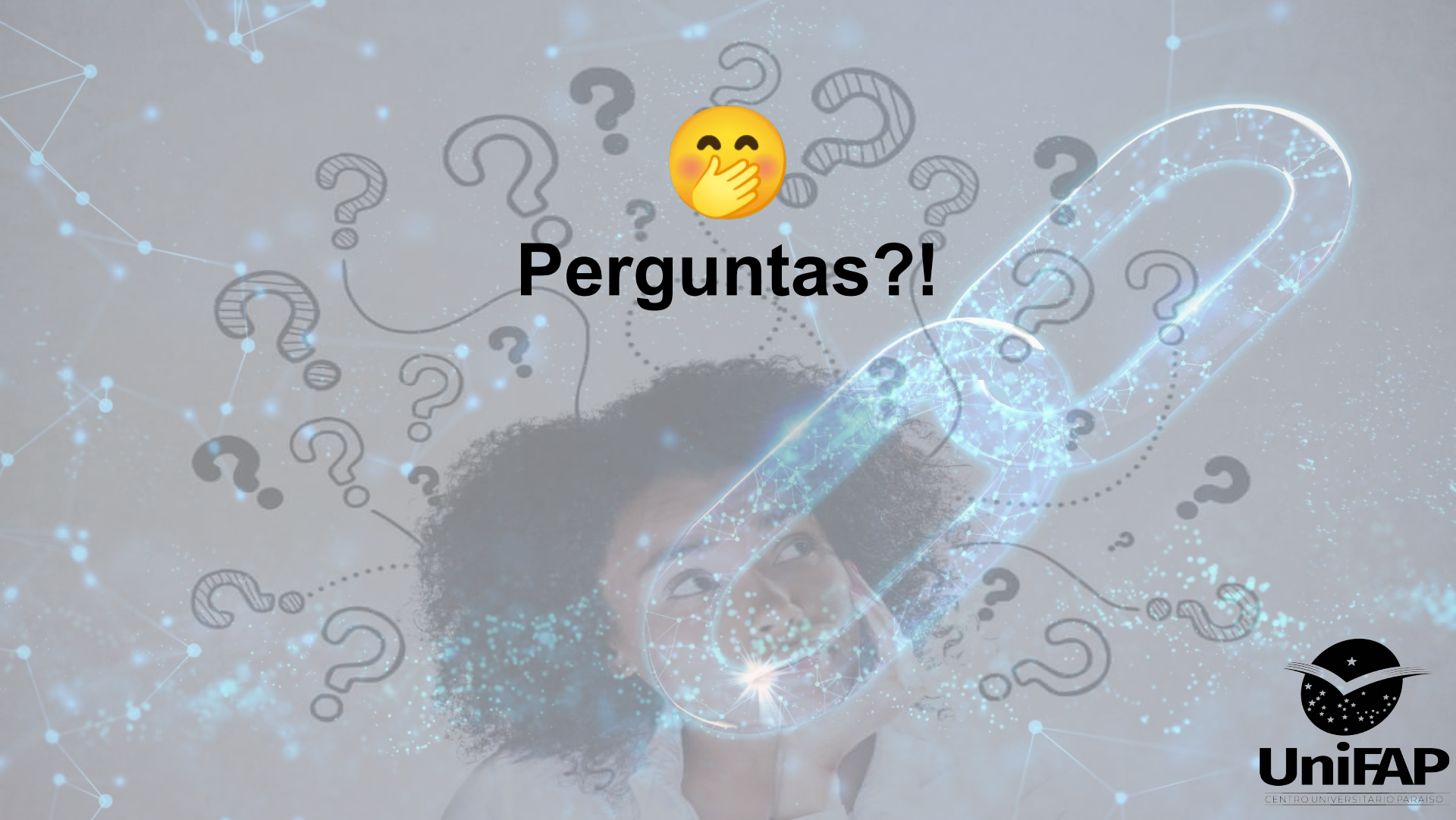
AZEVEDO, Ricardo. Blockchain e negócios: por dentro das engrenagens da nova economia. Rio de Janeiro, RJ: Brasport, 2023. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/216102. Acesso em: 09 maio 2025.

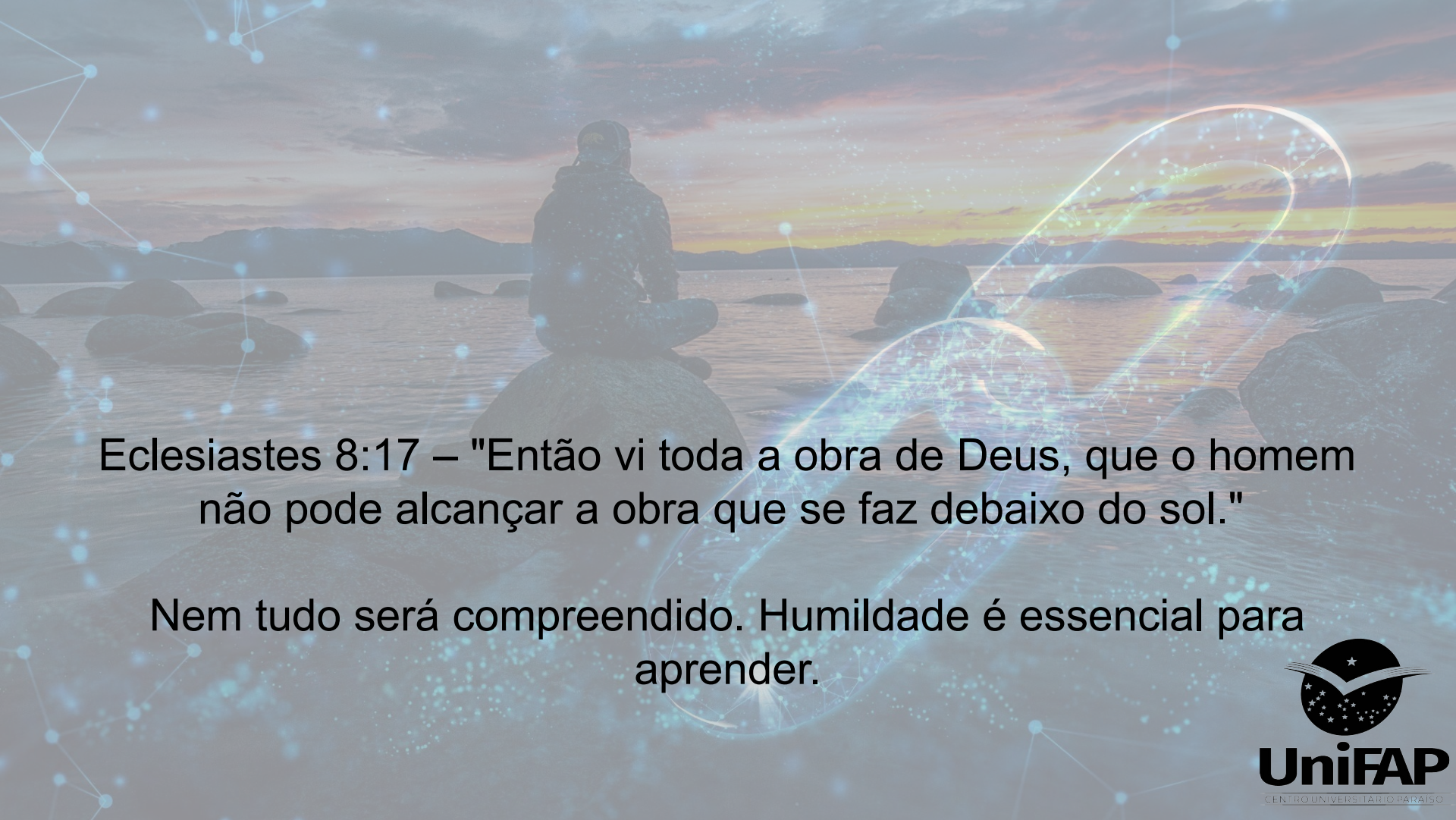


Bibliografia

LYRA, João Guilherme. Blockchain e organizações descentralizadas. 1. ed. Rio de Janeiro: Brasport, 2019. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/169379 . Acesso em: 09 maio 2025.




🤭
Perguntas?!



Eclesiastes 8:17 – "Então vi toda a obra de Deus, que o homem não pode alcançar a obra que se faz debaixo do sol."

Nem tudo será compreendido. Humildade é essencial para aprender.

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO



Obrigado!

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO