Construindo Sua Blockchain

Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br

Resumo

- O que é?
- Conceitos Básicos
- Estrutura
- Funcionamento
- Aplicações

O que é Blockchain?

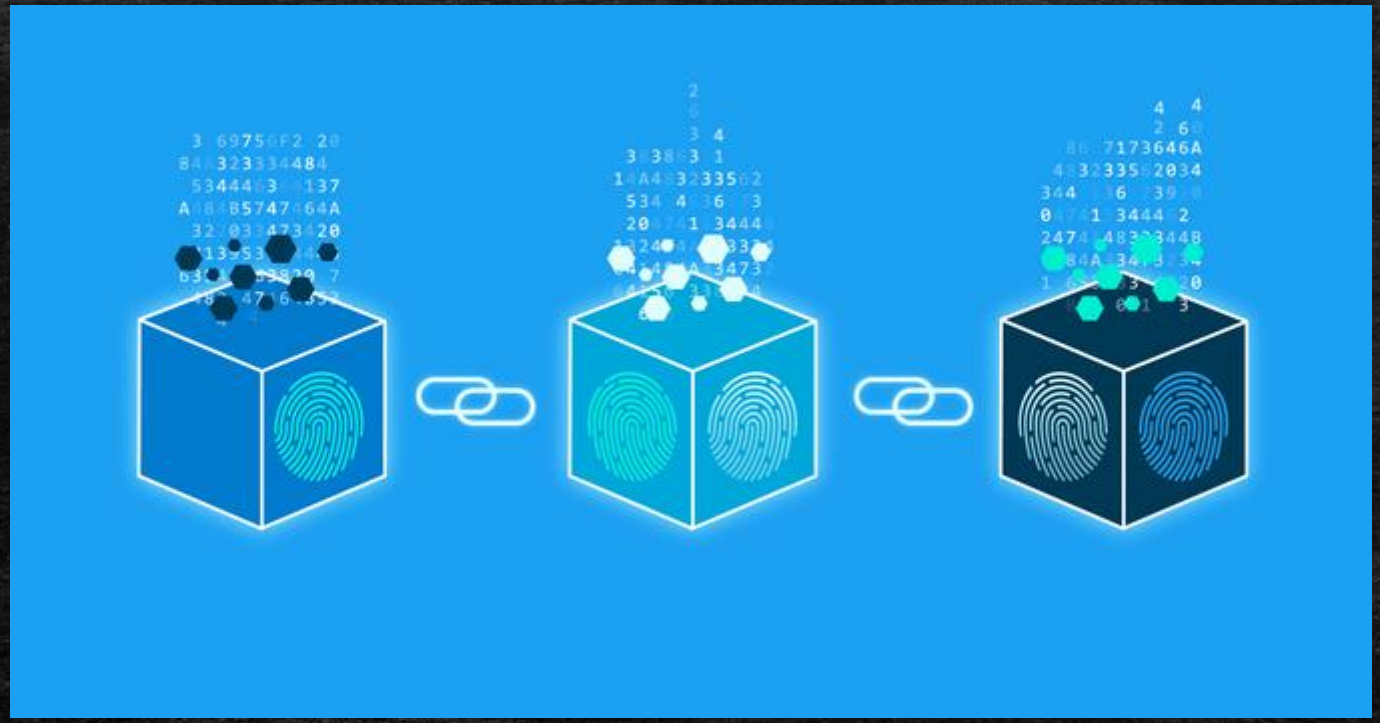
Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br

O que é blockchain?

- Livro de registros (Banco de Dados)
- Distribuído
- Imutabilidade
- Integridade

O que é blockchain?



Conceitos Básicos

Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br

Conceitos Básicos

- Funções de Hash
- Árvore de Merkle
- Criptografia Assimétrica

Funções de Hash

- Hash: bagunça, picadinho de carne, fricassê . . .
- Função como na matemática
- Entrada de tamanho arbitrário
- Saída de tamanho fixo

Funções de Hash

- Características:
- One Way (caminho único)
- Collision Proof (à prova de colisões artificiais)
- Descorrelação entre entrada e saída.

Funções de Hash

- Exemplo:
- SHA-1 (1995)
  - Saída de 160 bits (20 bytes)
- SHA-3 (2015)
  - Saídas de: 224, 256, 386 ou 512 bits

Funções de Hash

- Exemplo:

- http://www.sha1-online.com/

Funções de Hash

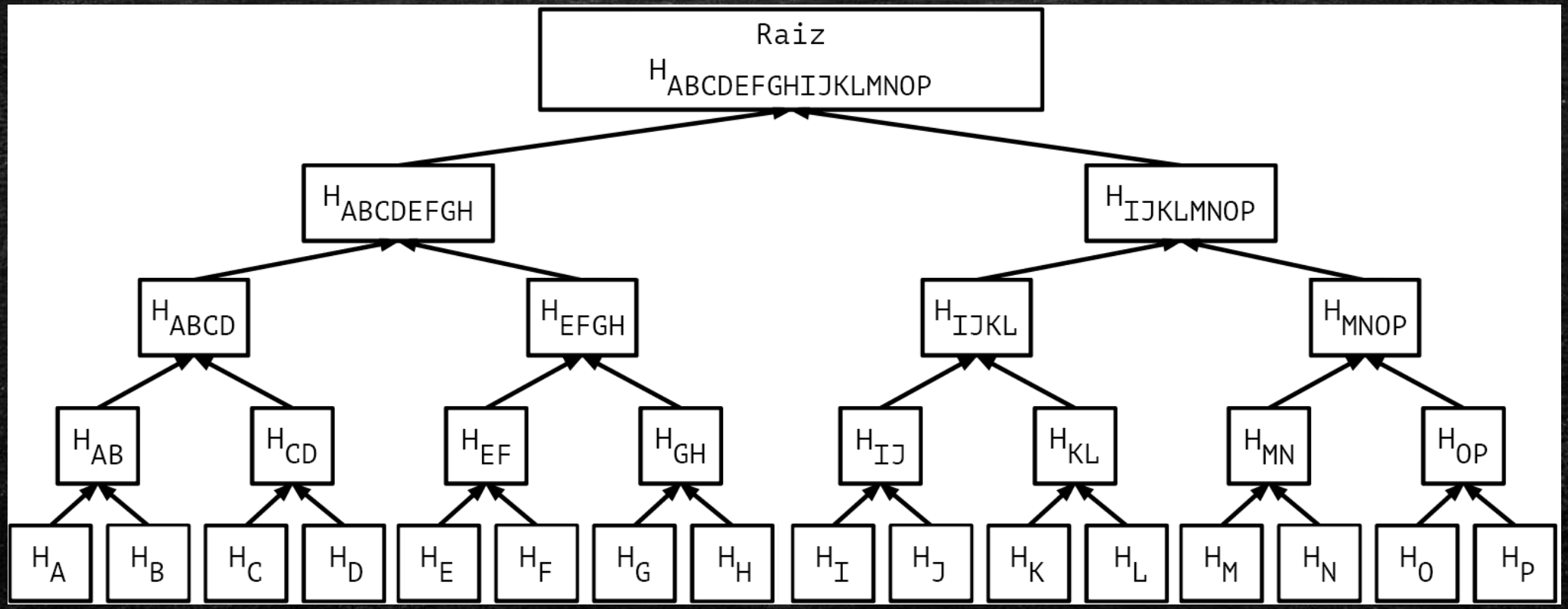
- Input: Teste123
- Output: 4d750439e3f39848345c6ef74ef3d719e34e7111

- Input: Teste122
- Output: 018d38f811fe61d0246498ac7099fda30d62ea0f

Árvore de Merkle

- Suponha que eu queira registrar dados no meu banco.
- De forma convencional cada entrada de dados ocupa uma linha da tabela do banco
- Essa entrada de dados chamaremos de registro

Árvore de Merkle



Criptografia Assimétrica

- Uma chave para criptografar
- Outra chave para descriptografar
- Garantir:
  - Confidencialidade
  - Autenticidade
  - Não-Repúdio

Criptografia Assimétrica

- Chave Pública
- Chave Privada

- Criptografar com a chave privada do emissor/remetente garante autenticidade.

Estrutura

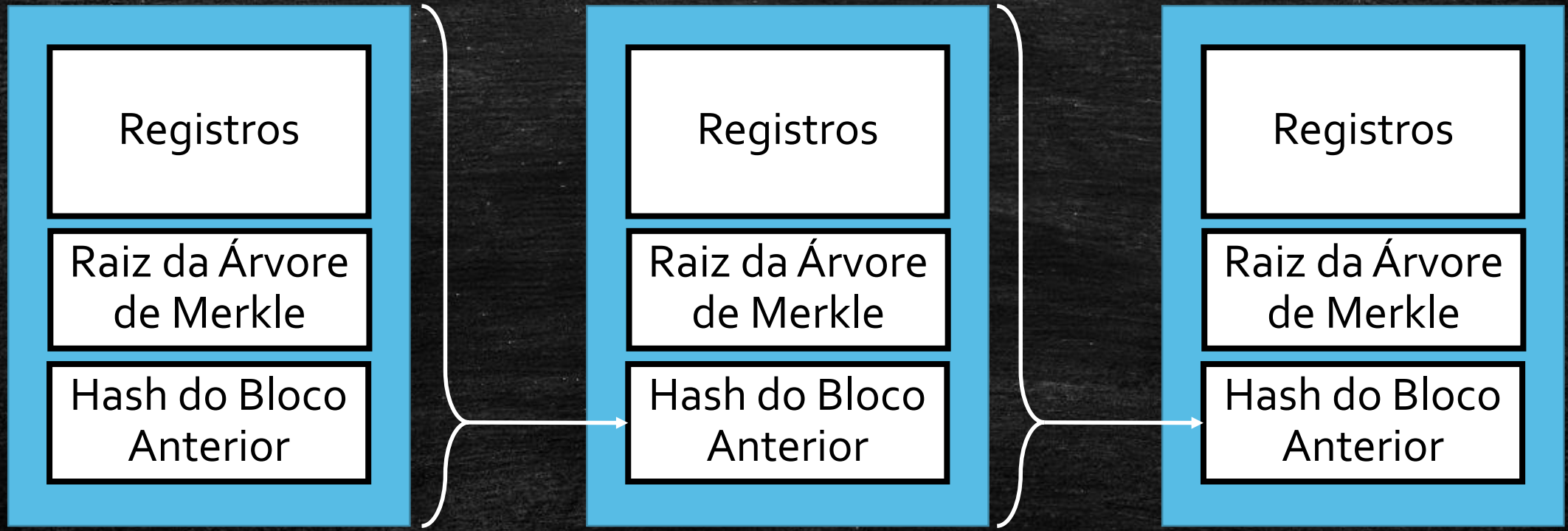
Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br

Estrutura

- Formada por conjuntos individuais de registros (Block)
- Cada bloco armazena o Hash do bloco anterior (Chain)

Estrutura


Registros
Raiz da Árvore de Merkle
Hash do Bloco Anterior
Registros
Raiz da Árvore de Merkle
Hash do Bloco Anterior
Registros
Raiz da Árvore de Merkle
Hash do Bloco Anterior

Funcionamento

Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br

Funcionamento

- Bloco armazena:
  - Registros
  - Hash Anterior
  - Raiz da Árvore de Merkle
  - Nonce

Funcionamento

- Bloco armazena:
  - Registros
  - Hash Anterior
  - Raiz da Árvore de Merkle
  - Nonce

Funcionamento

- Mecanismos de Consenso
  - Proof of Work (Cynthia Dwork & Moni Naor, 1993 → Markus Jacobsson & Ari Juels, 1999)
  - Proof of Steak
  - Proof of Authority

Funcionamento

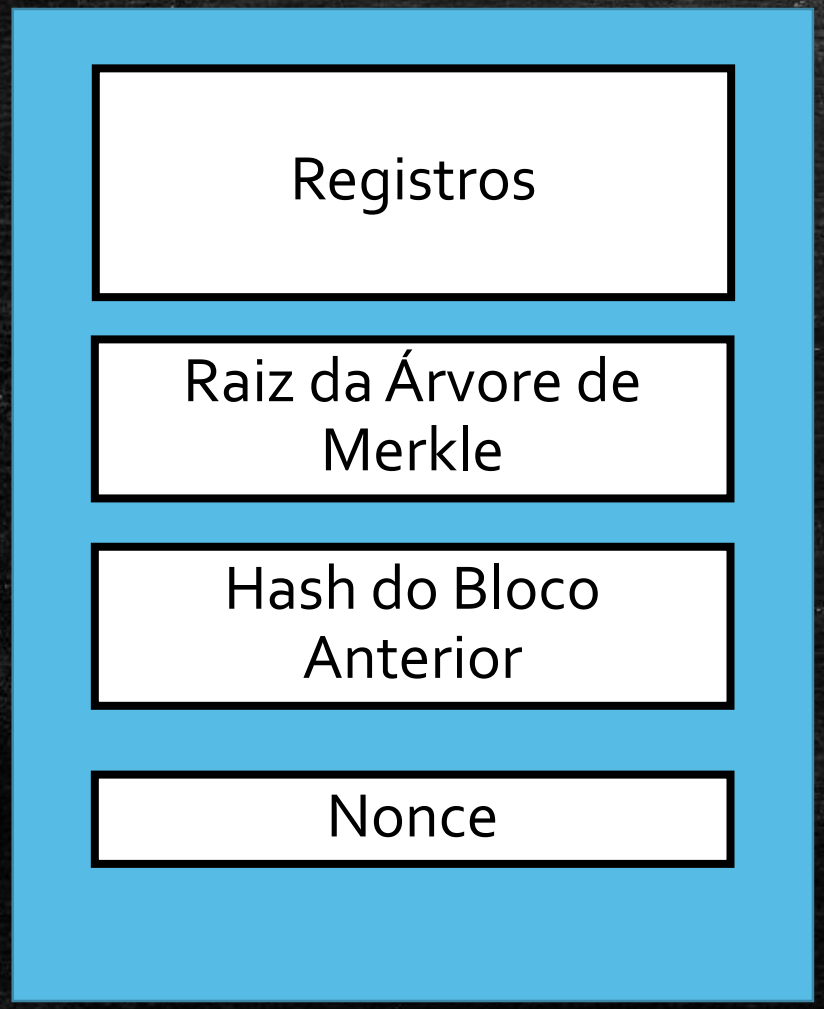
- Mecanismos de Consenso
  - Proof of Work (Cynthia Dwork & Moni Naor, 1993 → Markus Jacobsson & Ari Juels, 1999)
  - Proof of Steak
  - Proof of Authority

Funcionamento

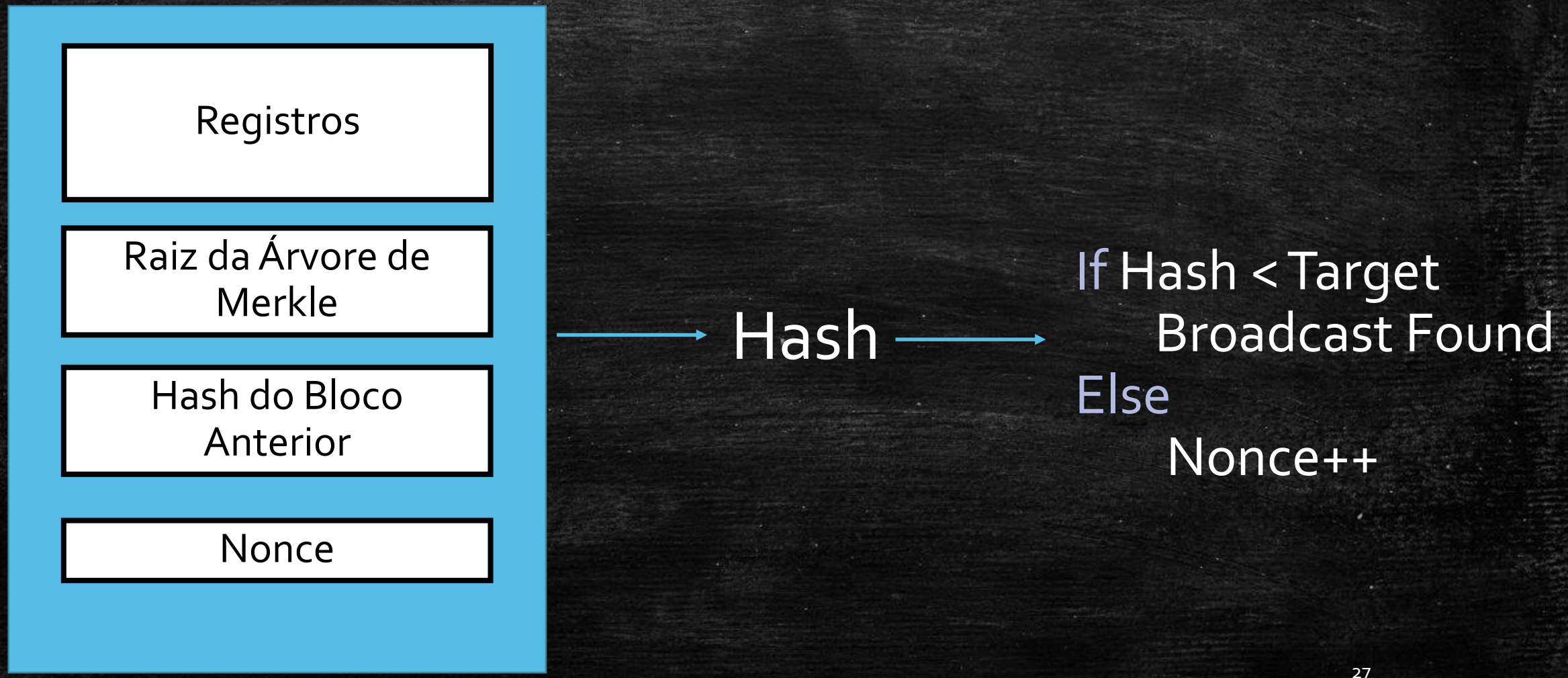
- Proof of Work

- Dado todas as informações do bloco exceto o nonce, encontre um número que concatenado ao bloco e feito o seu Hash o resultado é menor que um valor pré-determinado.

Funcionamento



Funcionamento



Aplicações

Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br

Aplicações

- Financeiras
  - Gerência de Ativos
  - Seguros
  - Pagamentos
  - Empréstimos com alienação fiduciária
- Propriedade Privada
  - Registro de bens
  - Smart Contracts
  - Registro de Propriedade Intelectual, Músicas, etc.

Aplicações

- Documentação
  - Passaporte
  - Certidões de Nascimento, Casamento e Óbito
  - Identificação Pessoal
  - Carteiras Profissionais
- Saúde
  - Prontuários Médicos
  - Histórico de Saúde
  - Rastreio de medicamentos controlados

Aplicações

- Redes
  - IoT
  - Smart Appliances
  - Redes de Sensores Encadeados
- Rastreamento de Encomendas

Mãos à Obra

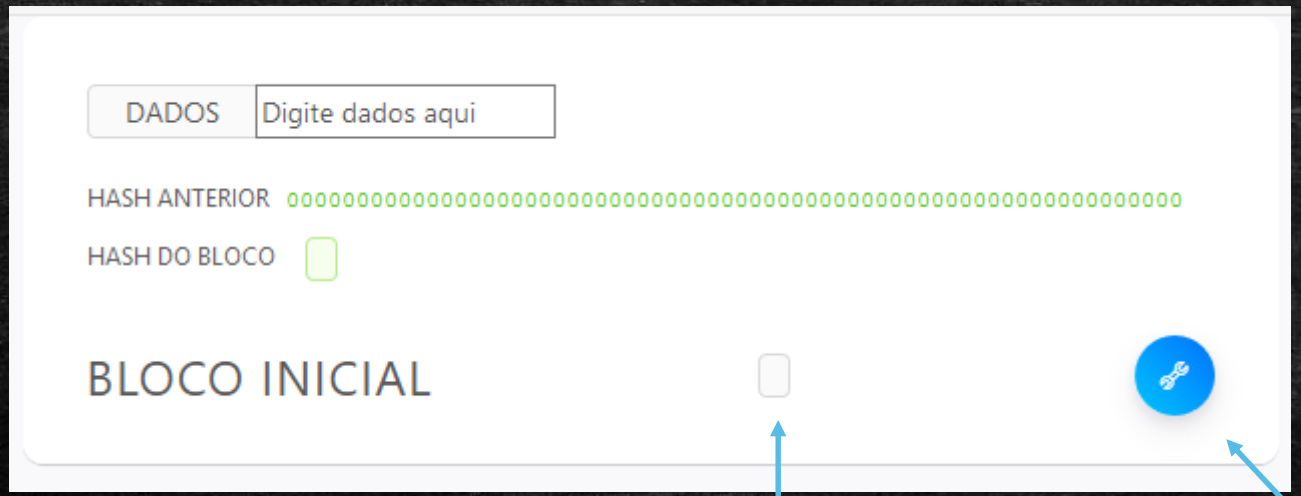
Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br

Funcionalidades

- Número de Blocos Fixos
- Alterar informações do Bloco
- Minerar (PoW)
- Dificuldade Constante

Interface



Nounce

Botão para Minerar o Bloco

GitHub

github.com/ldsampaio/blockchain-minicurso

Perguntas?

Lucas Dias Hiera Sampaio

ldsapaio@utfpr.edu.br