Insper

Ativos Digitais e Blockchain

Ricardo Rocha
Raul Ikeda

Agenda – Parte II

- Introdução Blockchain
- Blockchain Tecnicamente
- Bitcoin & Ethereum
- Outros Modelos
- Use Cases
- Programando Smart Contracts I
- Programando Smart Contracts II
- Programando Smart Contracts III
- Programando Smart Contracts IV
- Programando Smart Contracts V
- Projeto Final

Objetivo

- Introdução à tecnologia Blockchain

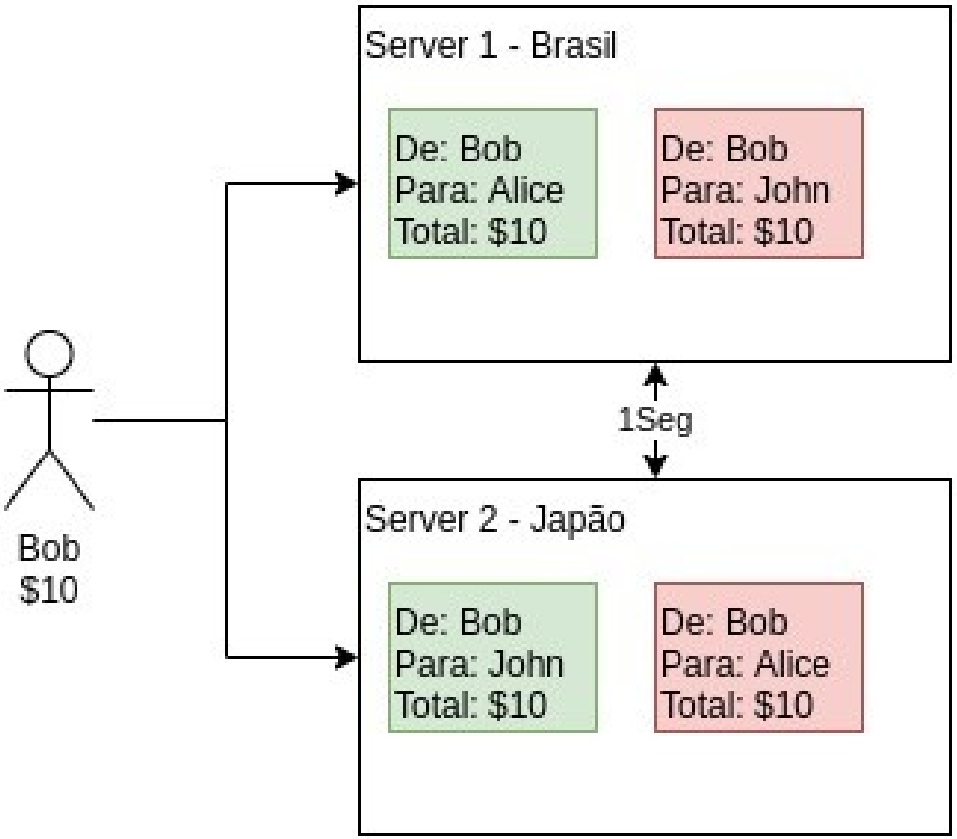
Por que a Blockchain foi criada?

- Transferir dinheiro de forma decentralizado evitando *double spending*

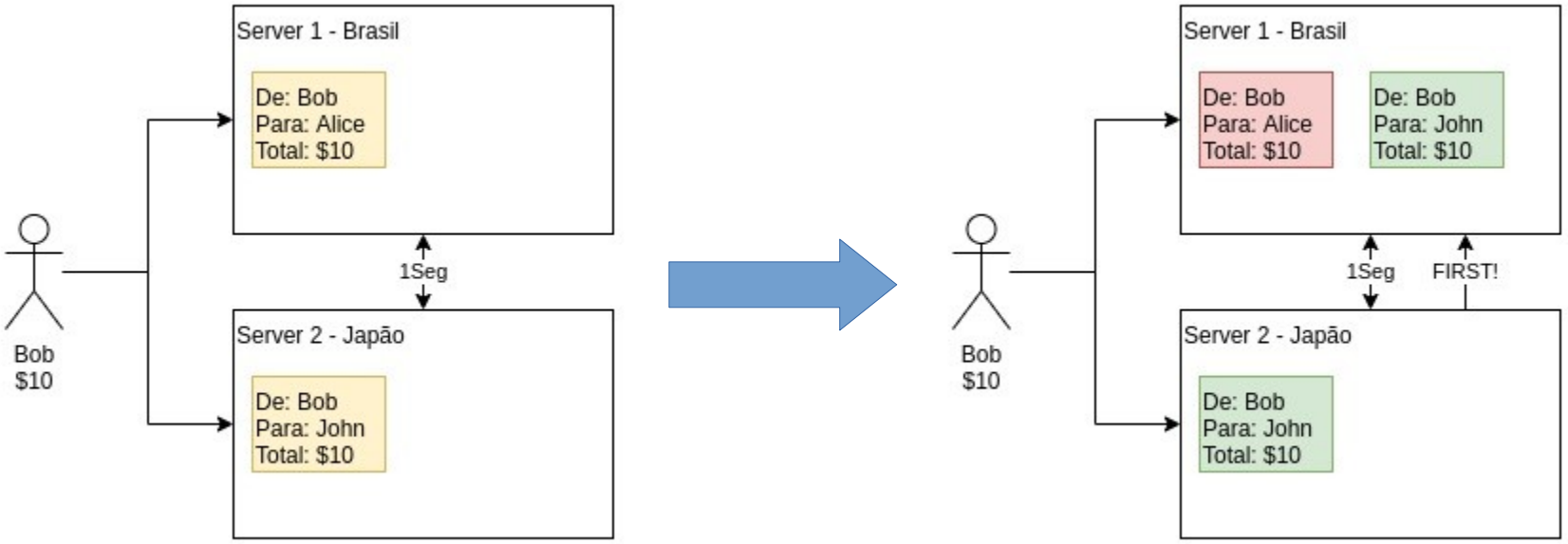
Decentralizado?

- Por que ser decentralizado?
- Qual a diferença entre centralizado e decentralizado?
- Qual a diferença entre decentralizado e distribuído?

O Problema do *Double Spending*



A solução


Server 1 - Brasil
De: Bob
Para: Alice
Total: $10
1Seg
Server 2 - Japão
De: Bob
Para: John
Total: $10
Bob
$10
Server 1 - Brasil
De: Bob
Para: Alice
Total: $10
De: Bob
Para: John
Total: $10
1Seg
FIRST!
Server 2 - Japão
De: Bob
Para: John
Total: $10
Bob
$10

Qual o pulo do gato?

- Uma transação é recebida e retransmitida mas não é registrada até que todos os nós concordem
- Para que todos registrem (e sincronizem os dados), eles jogam um jogo de adivinhação
- O jogo consiste em chutar números inteiros. Quem adivinhar primeiro um número correto ganha.
- Um número correto resolve um puzzle criptográfico.
- Quem conseguir bater grita para os outros o mais rápido possível
- Os chutes acontecem simultaneamente. Quem conseguir chutar mais números por segundo tem mais chances de ganhar.
- Esse jogo é a famosa MINERAÇÃO de moedas

Por que alguém joga esse jogo

- Um prêmio para quem bater primeiro
- Um percentual das transações registradas
- E quem não ganhar? Um abraço

E se alguém mentir?

- O número achado pelo vencedor precisa ser validado pelos demais
- Se um certo percentual da rede der ok, os dados são registrados para sempre (?!?)

- Quais os incentivos desse jogo?
- Ainda, quais os incentivos perversos de jogo?

E depois?

- Salvar os dados
- Bases sincronizadas
- Nova rodada!

Origens

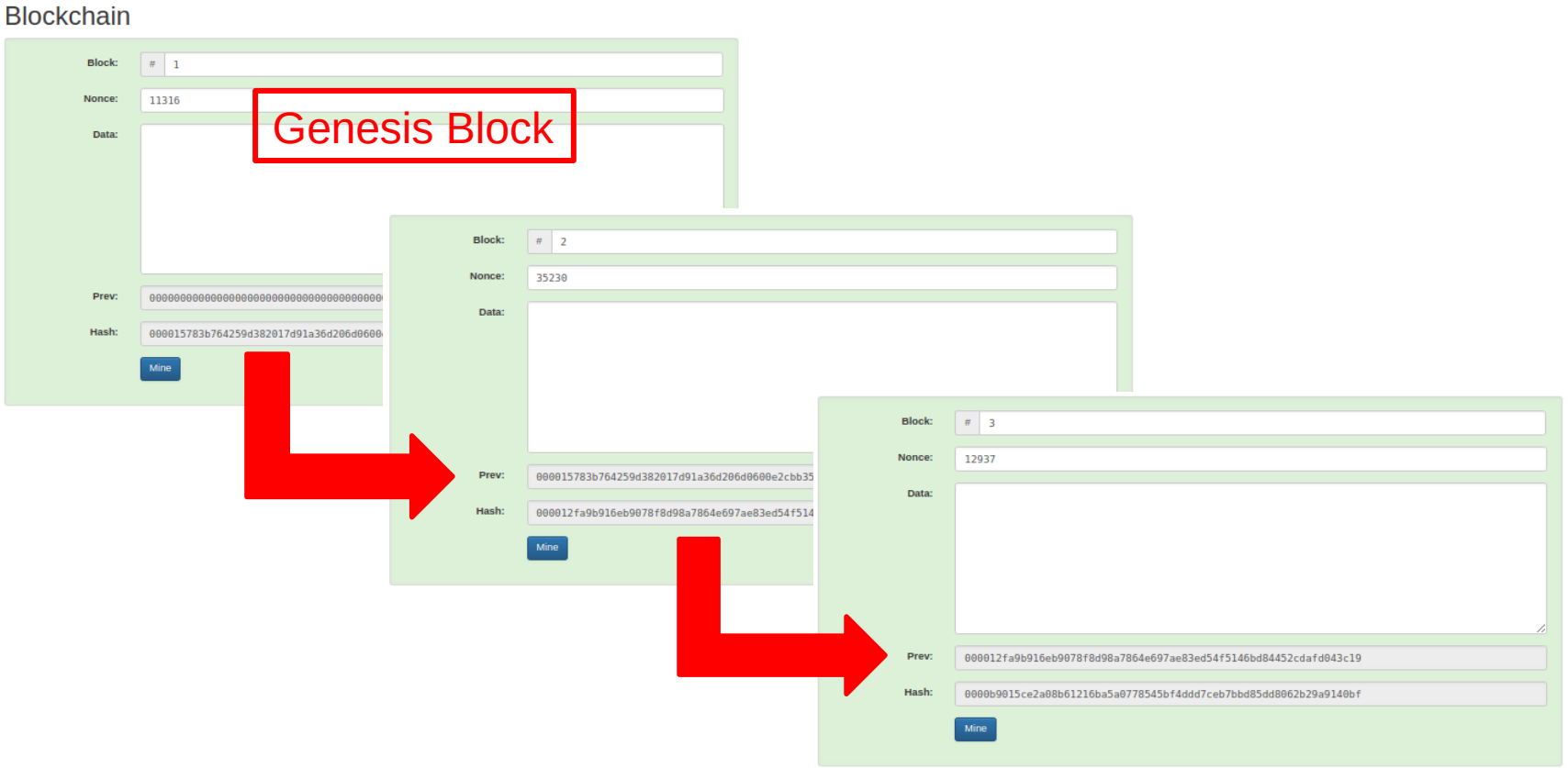
- Bitcoin: A Peer-to-Peer Electronic Cash System – Nakamoto S.

- Ideia: criar uma forma de transacionar valores eletronicamente e decentralizado que evitasse o *double spending*.
- Junção de várias técnicas já conhecidas: peer-to-peer, lista ligada, hash function, private/públic key, etc.
- Continuação do trabalhos:
  - "How to Time-Stamp a Digital Document", Haber & Stornetta, 1991.
  - "Pricing via Processing or Combatting Junk Mail", Dwork & Naor, 1993.
  - "Proofs of work and bread pudding protocols", Jakobsson & Juels, 1999.
  - "Reusable Proof-of-Work”, Finney(1956-2014).
  - "Hashcash - a denial of service counter-measure", Back, 2002.

Para demonstrar os conceitos, vamos usar a página: https://andersbrownworth.com/blockchain/hash

Blockchain: tecnicamente

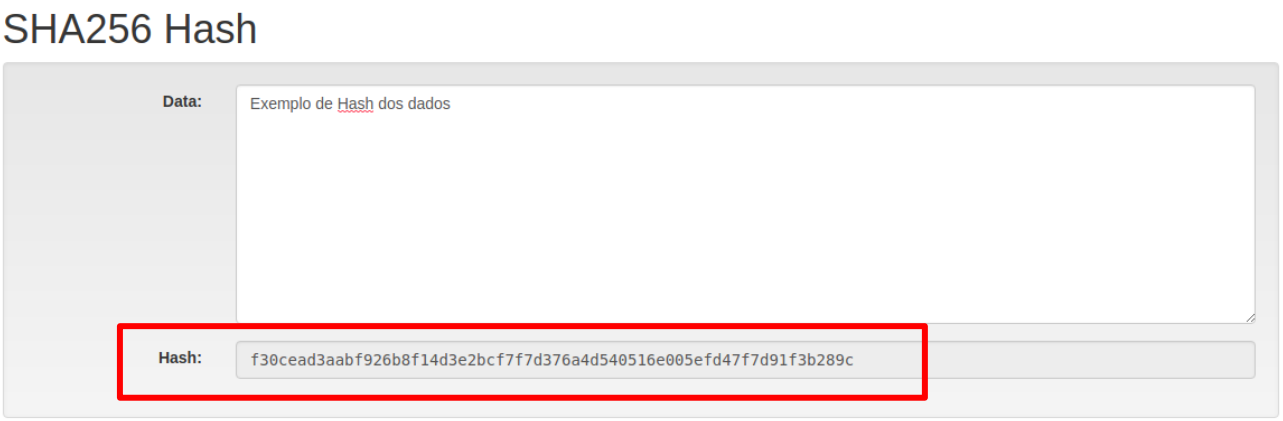
1. Lista ligada de blocos: O hash do bloco atual é formado pelo hash anterior + dados do bloco + nonce.



Função Hash

Hash Function: Exemplo SHA256

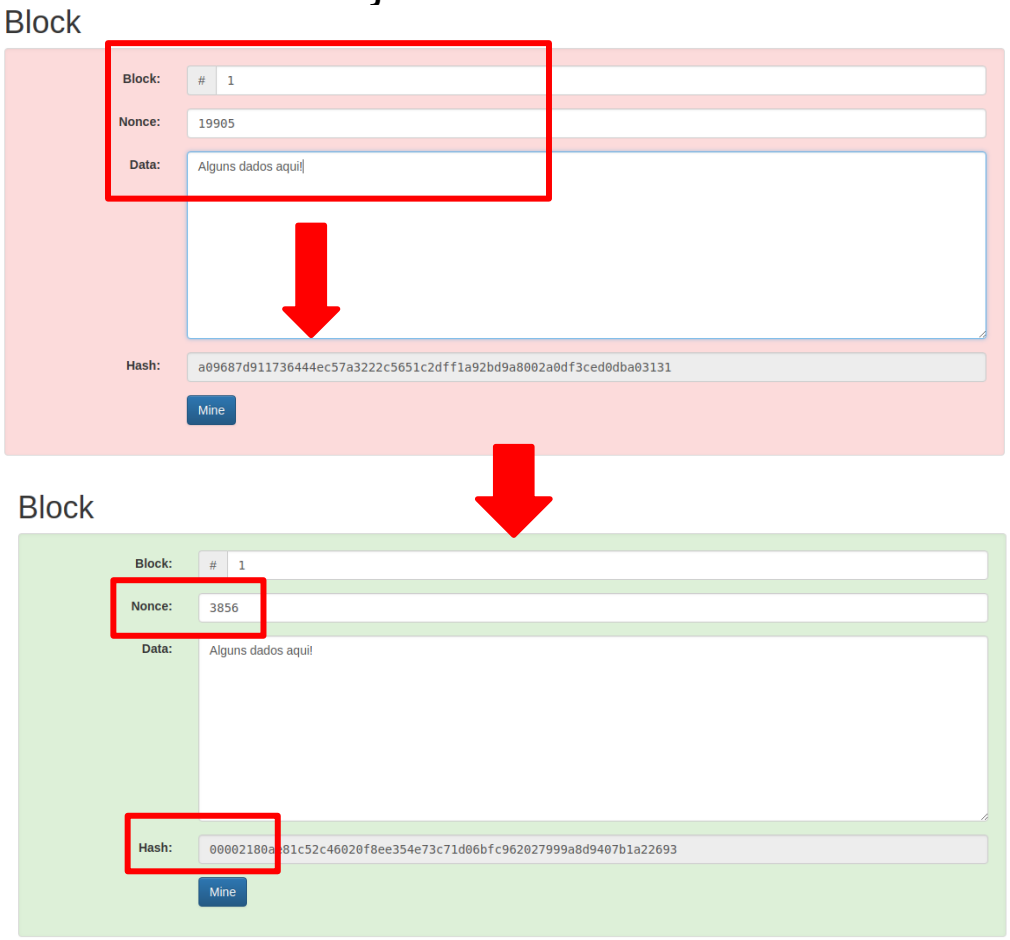
A função é NÃO inversível!



Mais detalhes: https://pt.wikipedia.org/wiki/SHA-2

O Jogo da Mineração

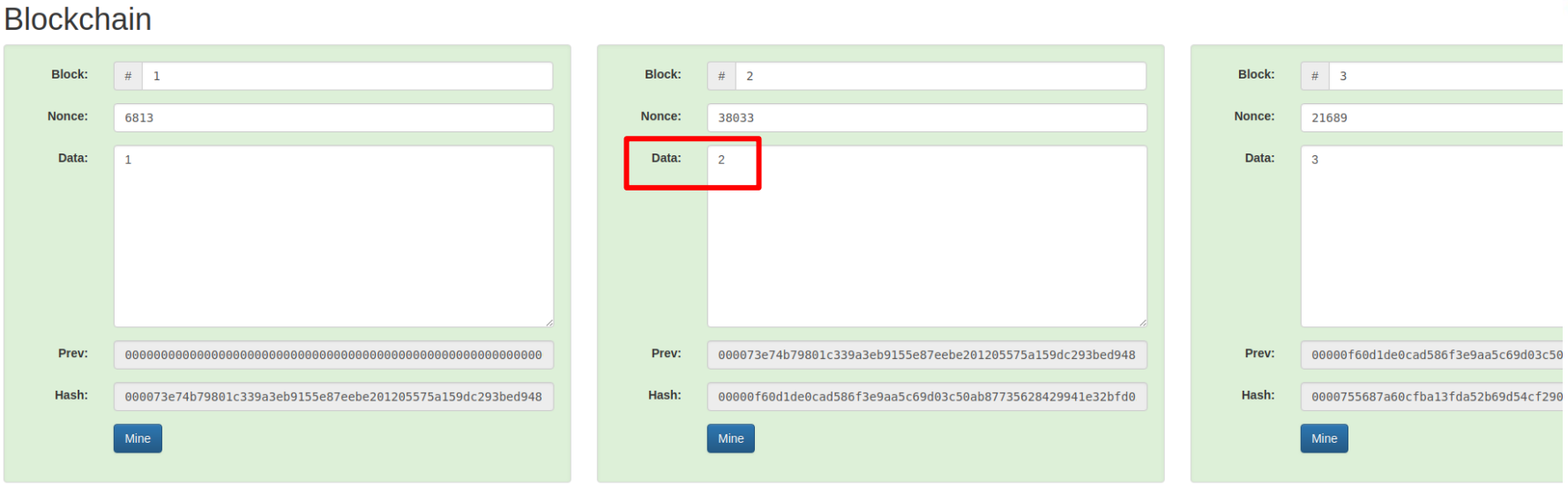
Calcular o **nonce** cujo o resultado do hash comece com n zeros.

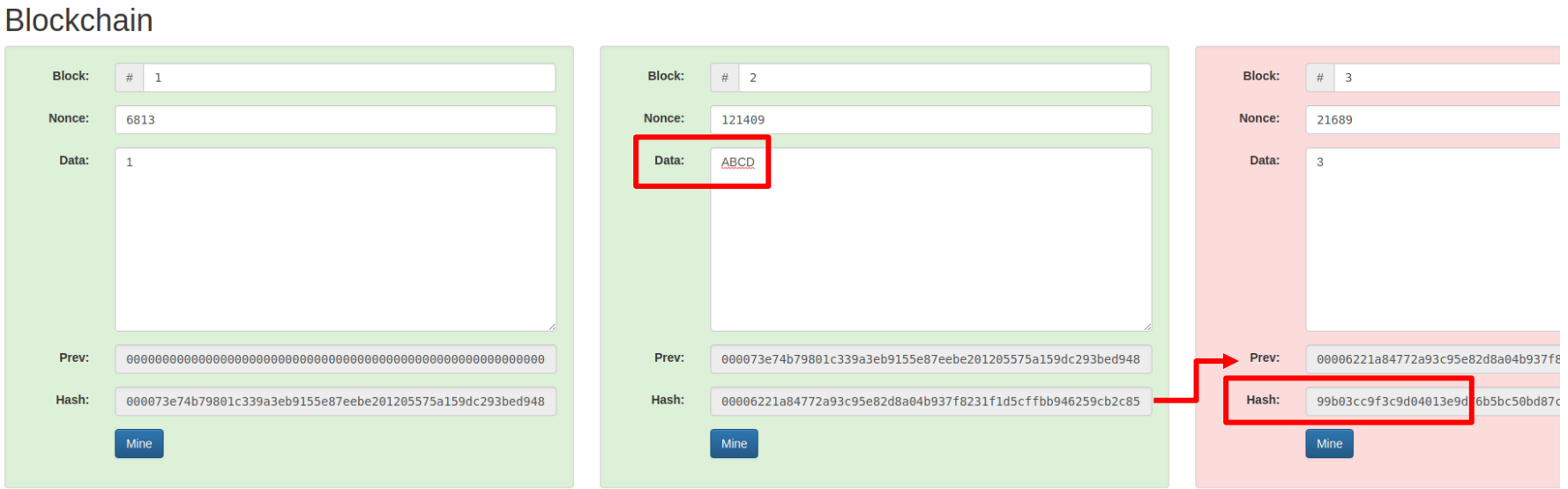


Dúvida: Existe apenas um nonce possível?

Insper

Imutabilidade: Se alterar algo em algum bloco, o seu hash seria alterado. Minerando novamente o bloco, dificilmente o hash se manteria o mesmo. Logo a lista se tornaria inconsistente.

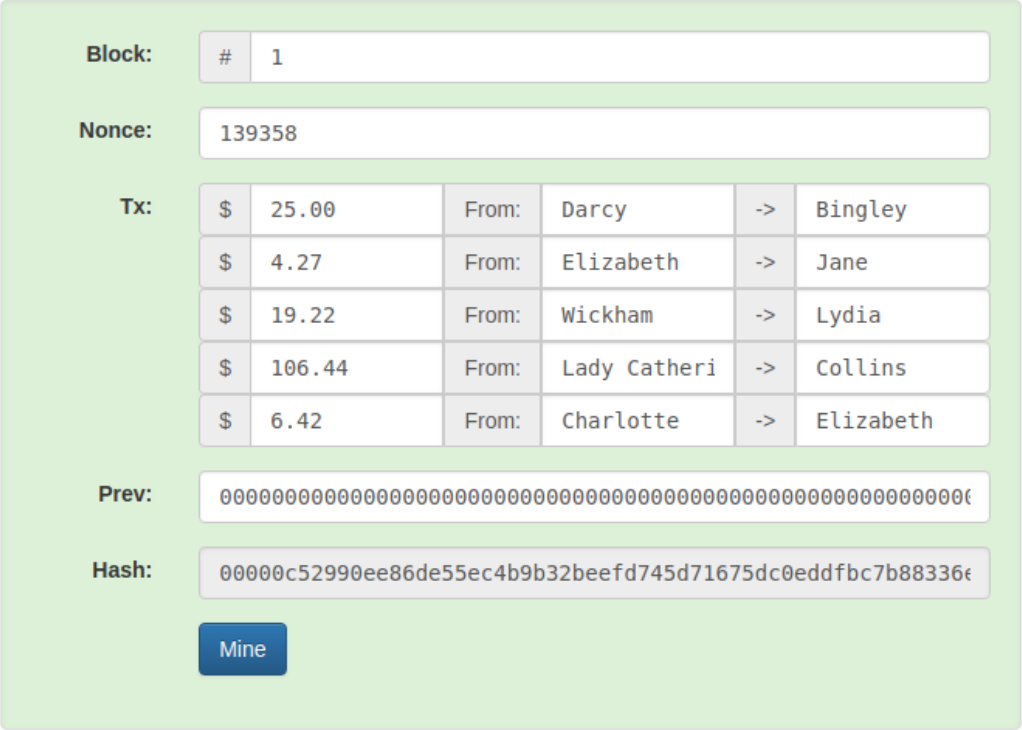




Insper

Transações

E se os dados contidos no bloco representassem transações financeiras entre duas partes:

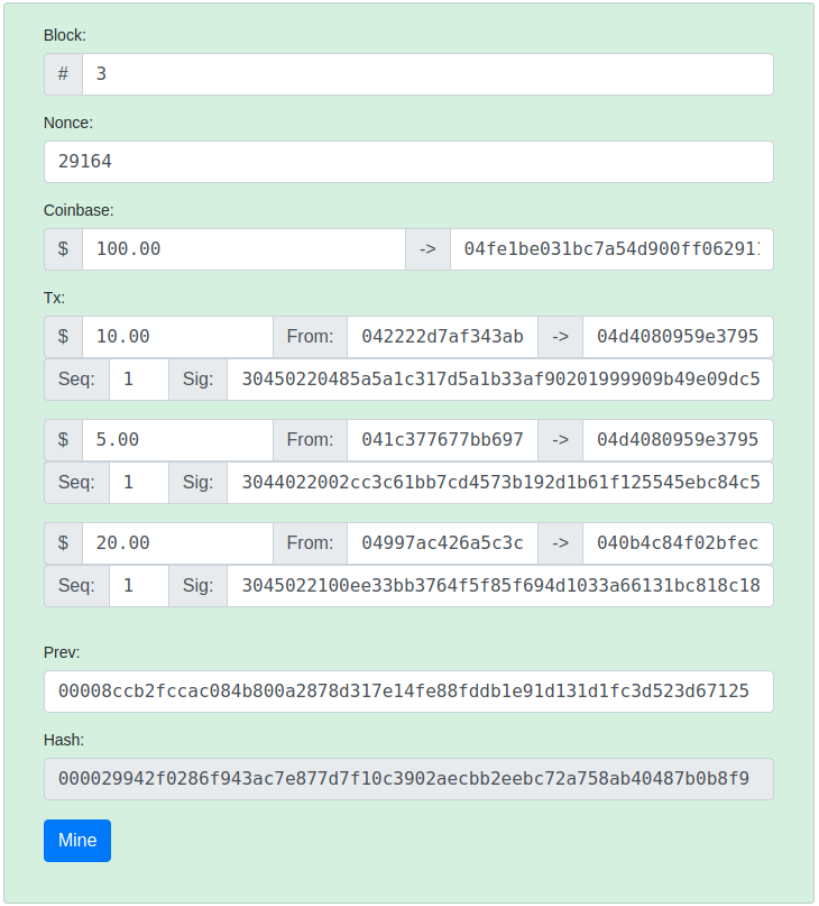


Como garantir que a transação realmente partiu da conta origem?

Transações

Assinatura: Chave pública e privada.

A origem e destino não precisa necessariamente ser identificado nominalmente:



Insper

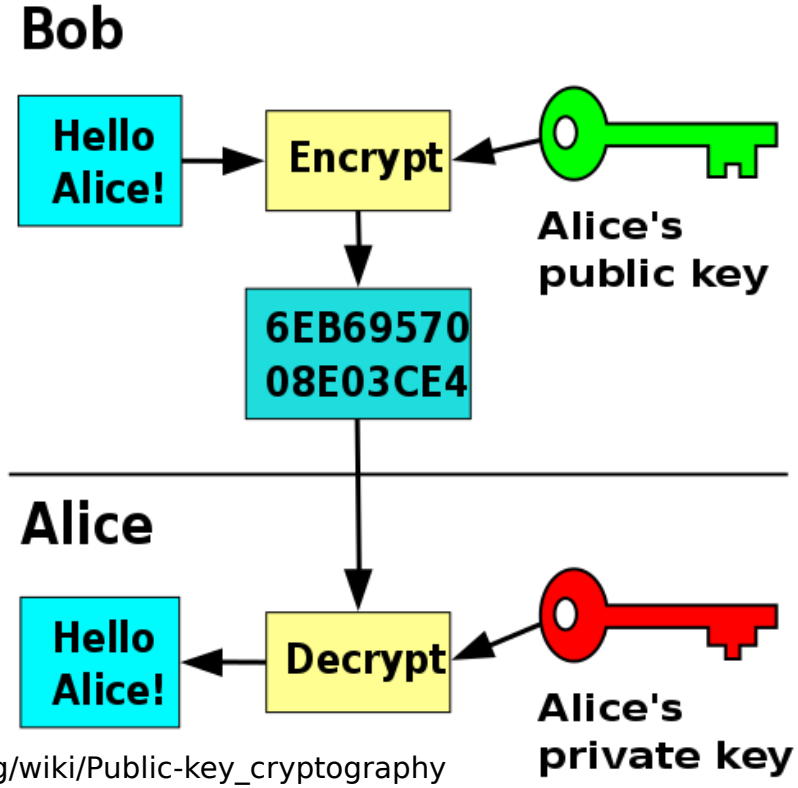
Chave Pública e Chave Privada

- Public-key Cryptography é um modelo que utiliza as duas chaves assimétricas para criptografar e descriptografar uma informação.
- Uma informação criptografada com a chave pública só pode ser recuperada com a chave privada e vice-versa.
- É possível combinar as duas chaves para criar um canal seguro de comunicação com garantia de origem.
- A chave pública pode e deve ser divulgado para todo mundo.
- A chave privada não deve ser divulgada para ninguém.

Mais detalhes: Tecnologias Hacker (7º COMP).

Caso 1:

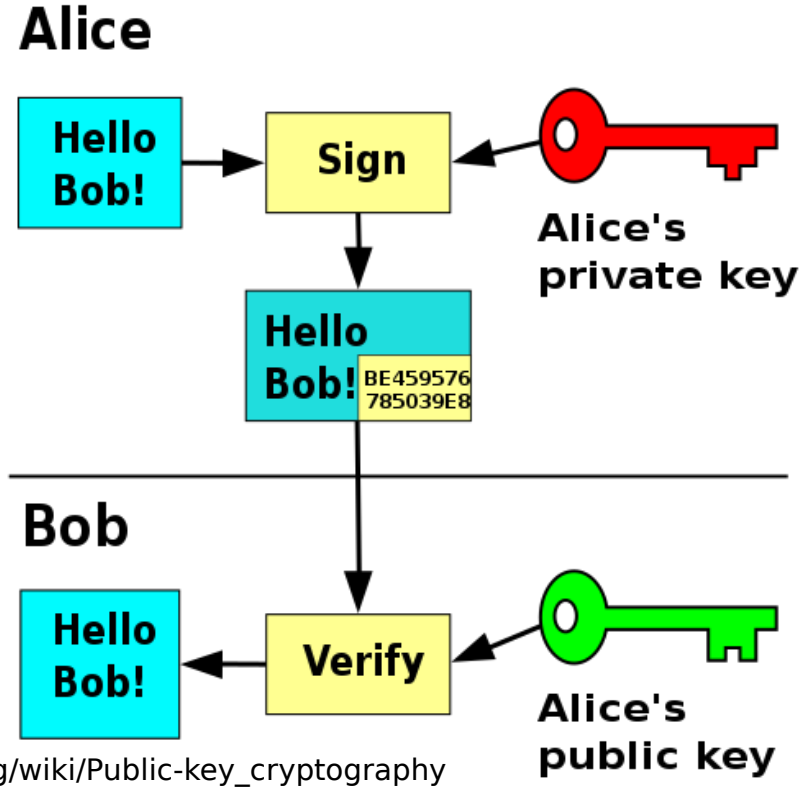
- Bob deseja mandar uma mensagem que só Alice pode ver.
- Bob criptografa a mensagem com a chave pública da Alice. Lembrando que a chave pública é divulgada para todo mundo.
- A mensagem só pode ser descriptografada com a chave privada. Apenas Alice tem a chave a privada.



Fonte: https://en.wikipedia.org/wiki/Public-key_cryptography

Caso 2:

- Alice deseja mandar uma mensagem assinada, onde todos tem a garantia de que foi ela quem mandou a mensagem.
- Alice criptografa a mensagem com a chave privada.
- Qualquer um pode descriptografar a mensagem com a chave pública da Alice, garantindo a origem da mensagem.



Fonte: https://en.wikipedia.org/wiki/Public-key_cryptography

Consenso e Votação

- Para evitar fraudes, cria-se uma rede *peer-to-peer*, onde cada nó possui uma cópia do Blockchain.
- Quando um novo nó é minerado, envia-se os dados do bloco a todos os nós da rede.
- Cada nó declara se aceita ou rejeita o bloco em questão. Caso um certo número de nós aceite o bloco, ele é incorporado ao Blockchain e começa-se a minerar um novo bloco.
- Durante a análise do bloco, os nós também avaliam a validade dos dados, e no caso de transações financeiras, se haveria saldo suficiente para efetuar cada transação.
- Caso o nó enviado seja inválido, se o minerador insistir em incorporar o bloco, ele irá divergir do resto da rede (fork).

Coinbase

- Equilíbrio do jogo: Qual o incentivo dos nós para minerar e manter uma cópia dos dados? Isso custa dinheiro.
- Ideia do Bitcoin: cada bloco minerado atribui um certo valor para a conta do minerador. Ainda, cada transação registrada paga um valor para o minerador do bloco.

- Dúvida: É possível haver um Blockchain sem uma moeda atrelada?

Concluindo!

- O que é Blockchain?
  - Em poucas palavras: um grande banco de dados descentralizado.

- Vantagens:
  - Auditável
  - Imutável
  - Robusto
  - "Democrático"

- Desvantagens:
  - Baixa performance
  - "Hackeável" (e de várias formas)

- Video Explicativo: https://youtu.be/SSo_EIwHSd4

Recapitulando

- Introdução ao Blockchain (Cadeia de Blocos ligados por hashes)
- O Jogo da Mineração (adivinhar o nonce)
- Função Hash (não inversível)
- Chave pública e Privada (assinatura de transações)
- Consenso (Proof of Work)

Próxima aula

- Redes
- Wallets
- Exchanges
- Cryptomoedas