



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

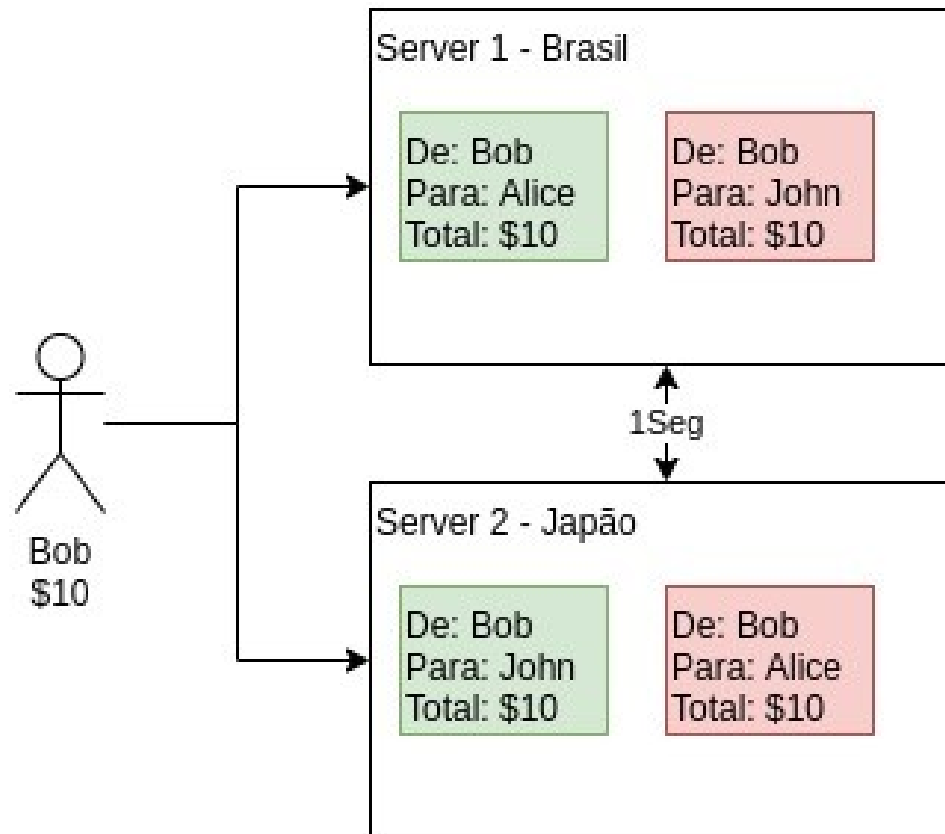
Por que a Blockchain foi criada?

- Transferir dinheiro de forma descentralizado evitando *double spending*

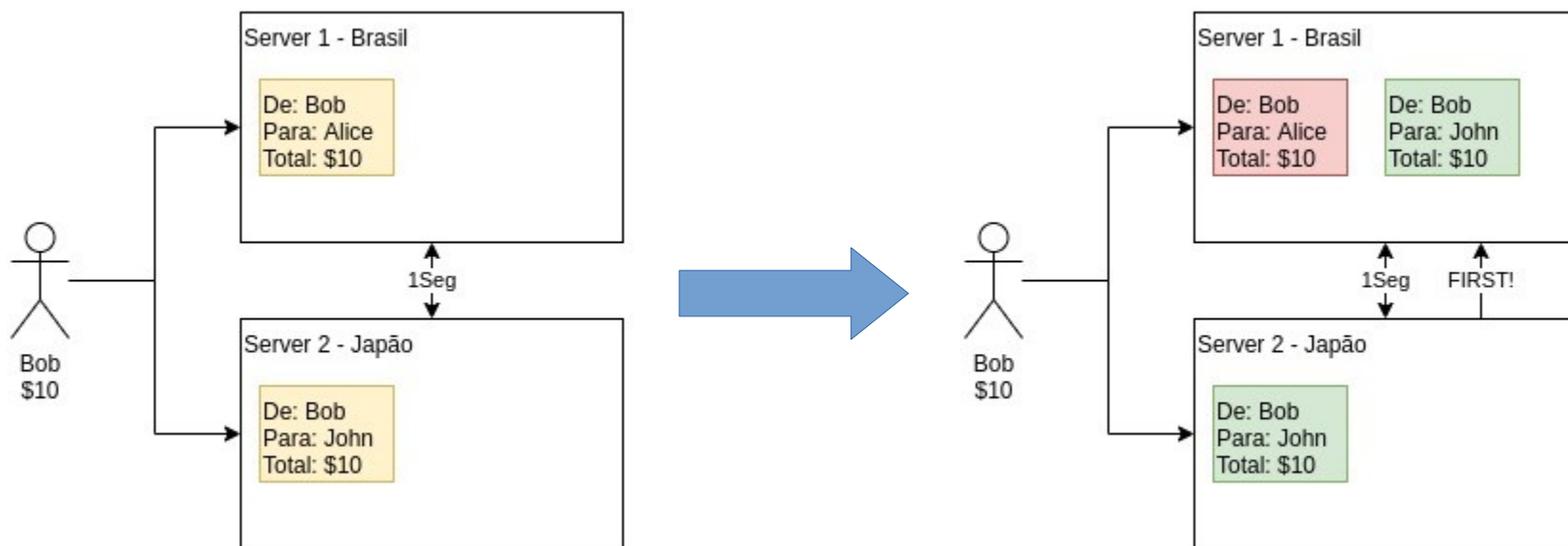
Decentralizado?

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

O Problema do *Double Spending*



A solução



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?

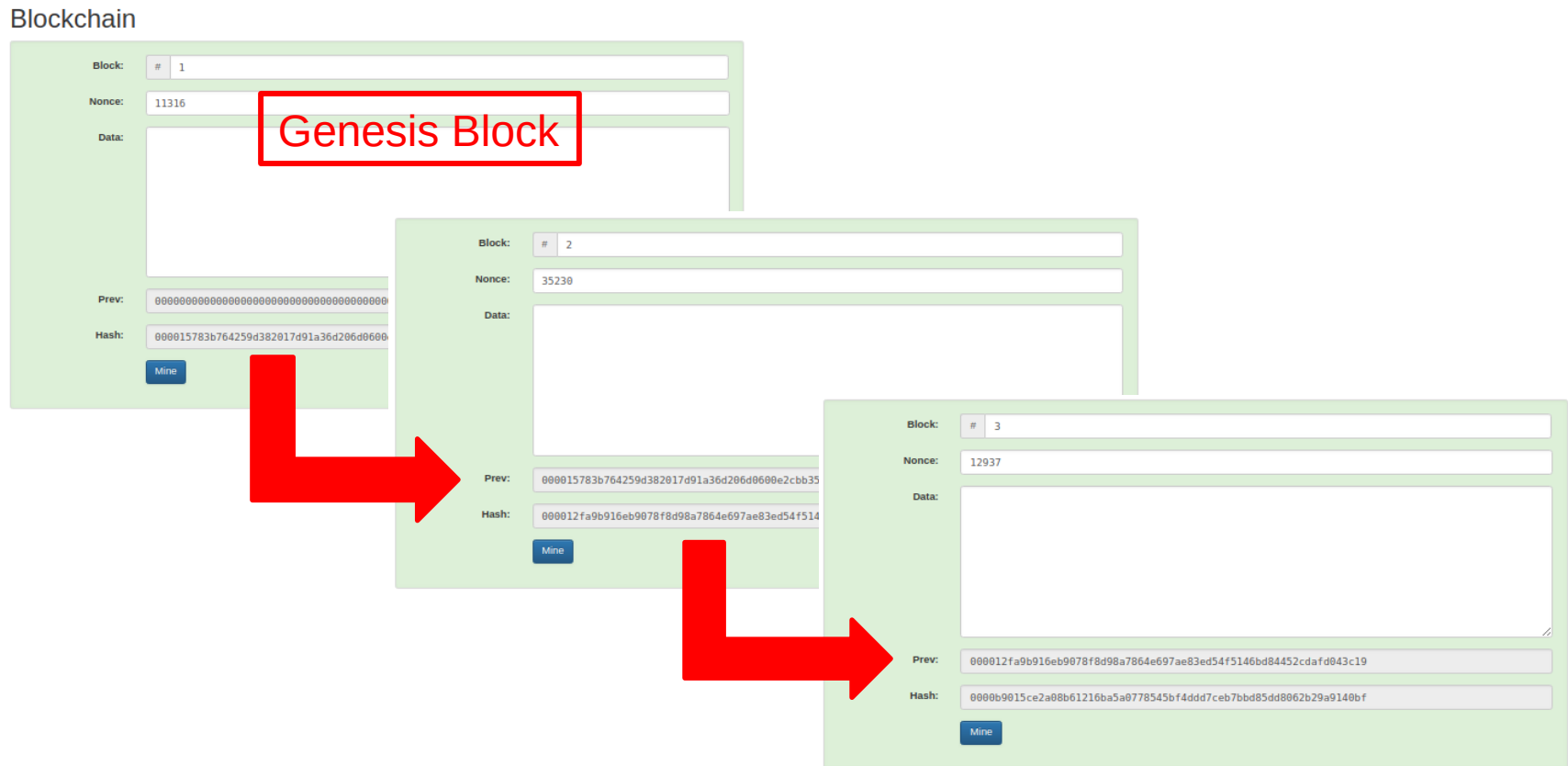
- Salvar os dados
- Bases sincronizadas
- Nova rodada!

Origens

- Bitcoin: A Peer-to-Peer Electronic Cash System – Nakamoto S.
- Ideia: criar uma forma de transacionar valores eletronicamente e descentralizado 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.

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!

SHA256 Hash



The image shows a web-based SHA256 hash calculator interface. It consists of a light gray container with two main input fields. The top field is labeled 'Data:' and contains the text 'Exemplo de Hash dos dados'. The bottom field is labeled 'Hash:' and contains a long alphanumeric string: 'f30cead3aabf926b8f14d3e2bcf7f7d376a4d540516e005efd47f7d91f3b289c'. This bottom field is highlighted with a red rectangular border. There is a small icon in the bottom right corner of the input area.

Label	Value
Data:	Exemplo de Hash dos dados
Hash:	f30cead3aabf926b8f14d3e2bcf7f7d376a4d540516e005efd47f7d91f3b289c

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.

Block

Block: # 1

Nonce: 19905

Data: Alguns dados aqui

Hash: a09687d911736444ec57a3222c5651c2dff1a92bd9a8002a0df3ced0dba03131

Mine

Block

Block: # 1

Nonce: 3856

Data: Alguns dados aqui

Hash: 00002180b81c52c46020f8ee354e73c71d06bfc962027999a8d9407b1a22693

Mine

Dúvida: Existe apenas um nonce possível?

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.

Blockchain

Block: #	Nonce	Data	Prev	Hash
1	6813	1	00	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948
2	38033	2	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948	0000f60d1de0cad586f3e9aa5c69d03c50ab87735628429941e32bfd0
3	21689	3	0000f60d1de0cad586f3e9aa5c69d03c50ab87735628429941e32bfd0	0000755687a60cfba13fda52b69d54cf290

Blockchain

Block: #	Nonce	Data	Prev	Hash
1	6813	1	00	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948
2	121409	ABCD	000073e74b79801c339a3eb9155e87eebe201205575a159dc293bed948	00006221a84772a93c95e82d8a04b937f8231f1d5cfffbb946259cb2c85
3	21689	3	00006221a84772a93c95e82d8a04b937f8231f1d5cfffbb946259cb2c85	99b03cc9f3c9d04013e9d06b5bc50bd87c

Transações

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

[illegible]

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:

Block:

3

Nonce:

29164

Coinbase:

\$ 100.00 -> 04fe1be031bc7a54d900ff06291

Tx:

\$ 10.00 From: 04222d7af343ab -> 04d4080959e3795

Seq: 1 Sig: 30450220485a5a1c317d5a1b33af90201999909b49e09dc5

\$ 5.00 From: 041c377677bb697 -> 04d4080959e3795

Seq: 1 Sig: 3044022002cc3c61bb7cd4573b192d1b61f125545ebc84c5

\$ 20.00 From: 04997ac426a5c3c -> 040b4c84f02bfec

Seq: 1 Sig: 3045022100ee33bb3764f5f85f694d1033a66131bc818c18

Prev:

00008ccb2fccac084b800a2878d317e14fe88fddb1e91d131d1fc3d523d67125

Hash:

000029942f0286f943ac7e877d7f10c3902aecbb2eebc72a758ab40487b0b8f9

Mine

Insper

Chave Pública e Chave Privada

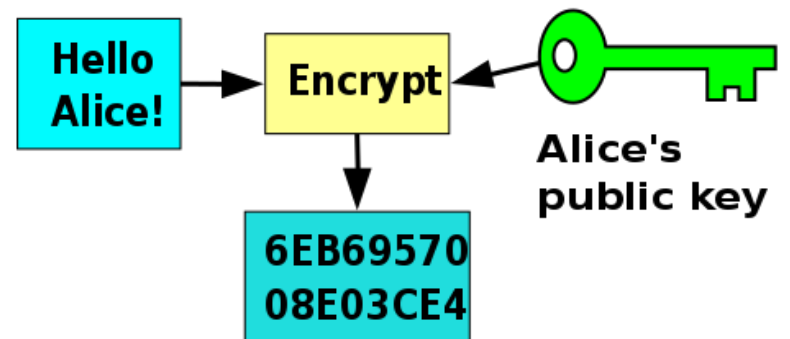
- Public-key Cryptography é um modelo que utiliza as duas chaves assimétricas para criptografar e descriptografar uma informação.
- Uma informação criptografada com a chave pública só pode ser recuperada com a chave privada e vice-versa.
- É possível combinar as duas chaves para criar um canal seguro 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).

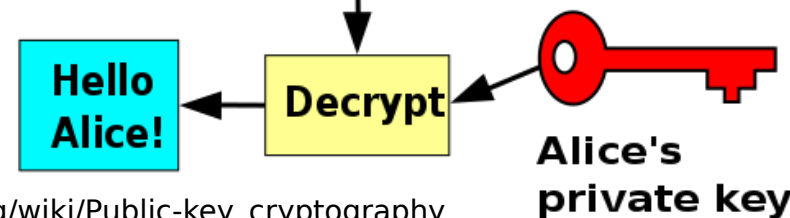
Caso 1:

- 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.

Bob



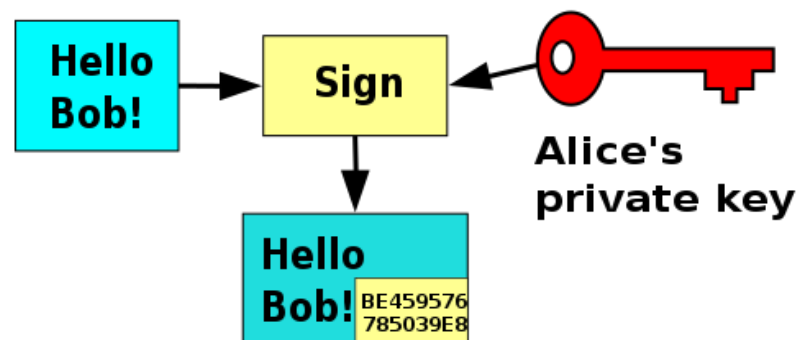
Alice



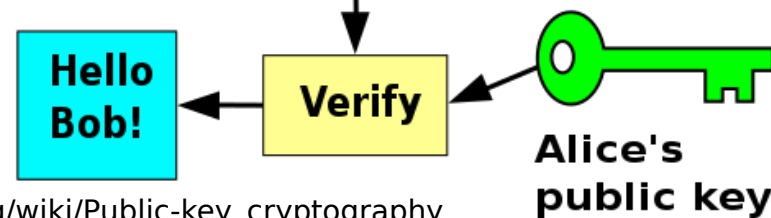
Caso 2:

- 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.

Alice



Bob



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_ElwHSd4

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