GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Blockchain:
Das Criptomoedas à Internet do Futuro

Gabriel Antonio F. Rebello

Semana de Eletrônica UFRJ 2019

Grupo de Teleinformática e Automação – GTA/UFRJ
Programa de Engenharia Elétrica - PEE/COPPE/UFRJ
Universidade Federal do Rio de Janeiro

COPPE UFRJ

Apresentador

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- **Gabriel Antonio Fontes Rebello**
  - Graduação em Eng. de Computação e Informação (UFRJ)
  - Mestrado em curso (PEE/COPPE/UFRJ)
  - Atua em
    correntes de blocos (blockchain),
    segurança em redes de computadores,
    virtualização e inteligência computacional
  - Pesquisa blockchains no GTA desde 2017

COPPE 50 UFRJ

Cronograma

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- **Parte I – Conceitos básicos e Bitcoin**
  - Motivação
  - O problema do gasto duplo
  - Funções hash, criptografia e replicação
  - Estrutura de uma blockchain
  - Prova de trabalho (Proof-of Work - PoW)
  - Bitcoin
  - Revisão

COPPE UFRJ

Cronograma

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- **Parte II – Alternativas ao Bitcoin**
  - Desafios da prova de trabalho
  - Blockchains públicas/privadas
  - Algoritmos alternativos de consenso
  - Hyperledger Fabric
- **Parte III – Aula prática**
  - Hyperledger Composer
  - Criação de uma blockchain para leilões de objetos
- **Parte IV – Conclusão e Perspectivas Futuras**

COPPE UFRJ

Parte I
Conceitos básicos e Bitcoin

Blockchains: Motivação

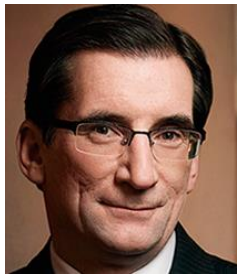
Blockchains: Motivação

“O futuro dos negócios são as moedas digitais.”
Bill Gates

Blockchains: Motivação

“O futuro dos negócios são as moedas digitais.”
Bill Gates

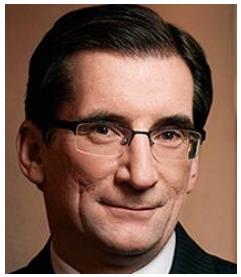
“Blockchain é a maior oportunidade de negócios que teremos na próxima década.”
Bob Grifeld, CEO NASDAQ



Blockchains: Motivação

“O futuro dos negócios são as moedas digitais.”
Bill Gates

“Blockchain é a maior oportunidade de negócios que teremos na próxima década.”
Bob Grifeld, CEO NASDAQ

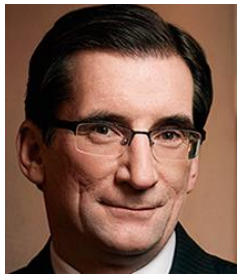


“A blockchain será o TCP/IP das transações financeiras no futuro.”
Paul Bucheit, criador do GMail

Blockchains: Motivação

“O futuro dos negócios são as moedas digitais.”
Bill Gates

“Blockchain é a maior oportunidade de negócios que teremos na próxima década.”
Bob Grifeld, CEO NASDAQ



“A blockchain será o TCP/IP das transações financeiras no futuro.”
Paul Bucheit, criador do GMail

“Blockchain está na moda e eu quero uma tese disso!”
Meu orientador

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Emerging Technology Trends 2018

Democratized AI

- AI PaaS
- Artificial general intelligence
- Autonomous driving Level 4
- Autonomous driving Level 5
- Autonomous mobile robots
- Conversational AI platform
- Deep neural nets
- Flying autonomous vehicles
- Smart robots
- Virtual assistants

Digitalized Ecosystems

- Blockchain
- Blockchain for data security
- Digital twin
- IoT platform
- Knowledge graphs

Do-It-Yourself Biohacking

- Biochips
- Biotech — cultured or artificial tissue
- Brain-computer interface
- Exoskeletons
- Augmented reality
- Mixed reality
- Smart fabrics

Transparently Immersive Experiences

- 4D printing
- Connected home
- Edge AI
- Self-healing system technology
- Silicon anode batteries
- Smart dust
- Smart workspace
- Volumetric displays

Ubiquitous Infrastructure

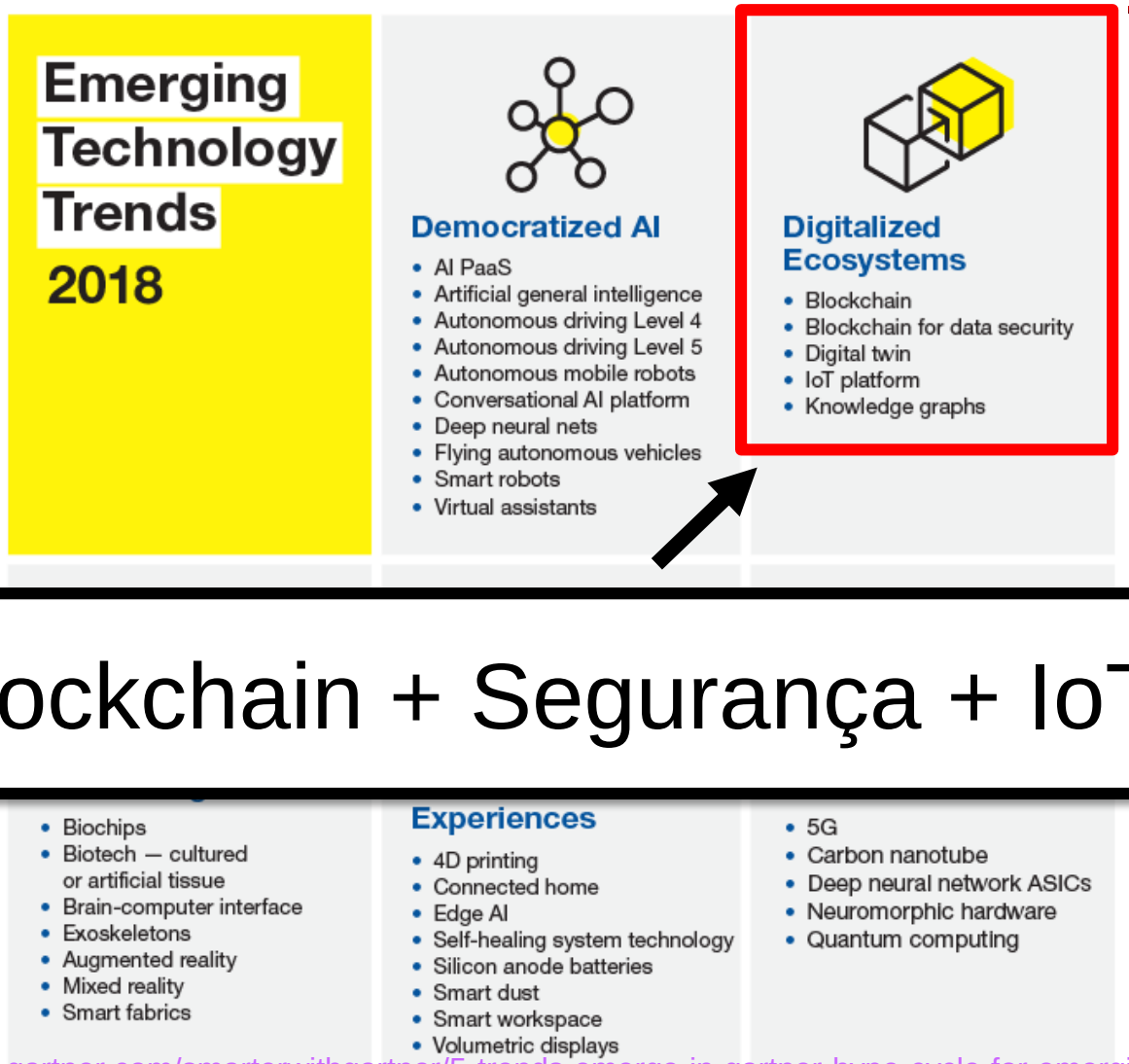
- 5G
- Carbon nanotube
- Deep neural network ASICs
- Neuromorphic hardware
- Quantum computing

COPPE UFRJ

Fonte: Gartner. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO



Blockchain + Segurança + IoT

COPPE UFRJ

Fonte: Gartner. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Troca online de itens com **valor**
  - Podemos construir uma **Internet de Valores?**

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Por que blockchain é uma tecnologia tão revolucionária?

COPPE UFRJ

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Por que blockchain é uma tecnologia tão revolucionária?
- Porque **elimina** a necessidade de **intermediários**

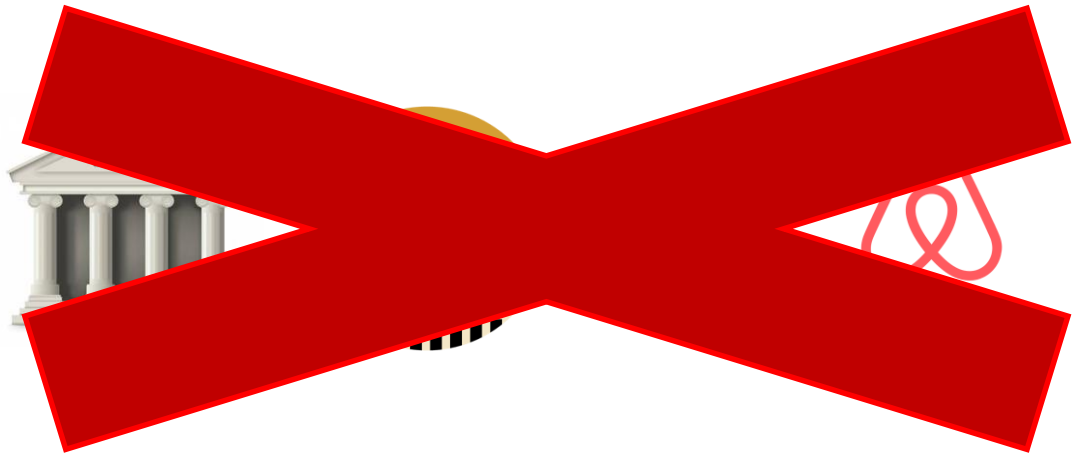
COPPE UFRJ

Blockchains: Motivação

- Por que blockchain é uma tecnologia tão revolucionária?
- Porque **elimina** a necessidade de **intermediários**
  - **Bancos, governos, Uber, AirBnB, etc.**

Blockchains: Motivação

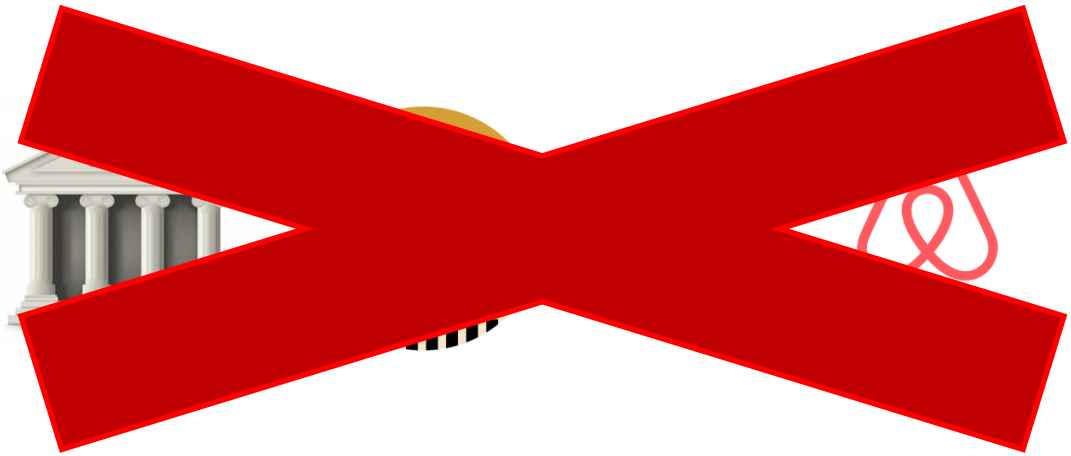
- Por que blockchain é uma tecnologia tão revolucionária?
- Porque **elimina** a necessidade de **intermediários**
  - **Bancos, governos, Uber, AirBnB, etc.**



Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Por que blockchain é uma tecnologia tão revolucionária?
- Porque **elimina** a necessidade de **intermediários**
  - **Bancos, governos, Uber, AirBnB, etc.**



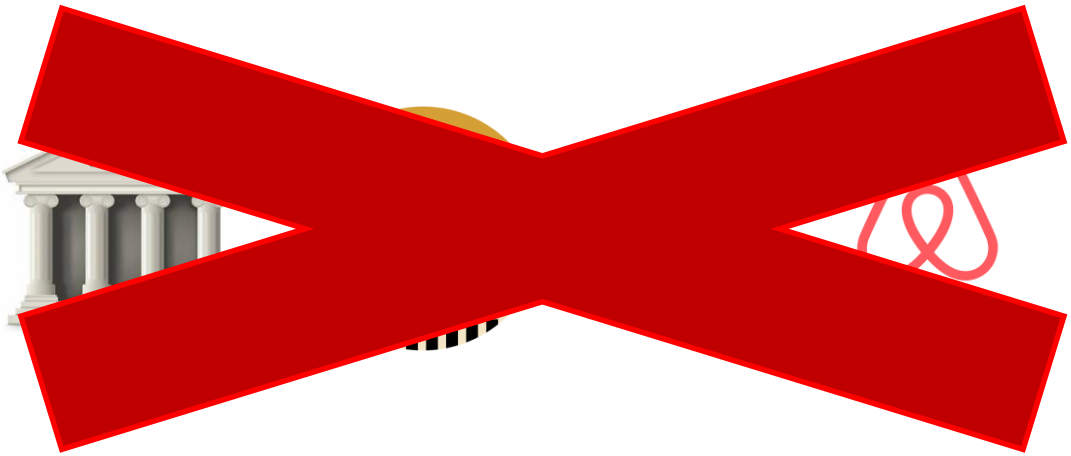
tinder

COPPE UFRJ

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Por que blockchain é uma tecnologia tão revolucionária?
- Porque **elimina** a necessidade de **intermediários**
  - **Bancos, governos, Uber, AirBnB, etc.**



tinder

Tecnologia mais **disruptiva** desde a **Internet**

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- A corrente de blocos foi proposta

COPPE UFRJ

Blockchains: Motivação

- A corrente de blocos foi proposta

Blockchain

Blockchains: Motivação

- A corrente de blocos foi proposta

Blockchain

Blockchain

Blockchains: Motivação

- A corrente de blocos foi proposta

Blockchain

Blockchain

Blockchain

Blockchains: Motivação

- A corrente de blocos foi proposta

Blockchain

Blockchain

Blockchain

Blockchain

Blockchains: Motivação

- A corrente de blocos foi proposta

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchains: Motivação

- A corrente de blocos foi proposta

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchains: Motivação

- A corrente de blocos foi proposta

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Transferência de valores sem taxas

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

Blockchain

COPPE UFRJ

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Transferência de valores sem taxas

Transferência imediata de valores

Blockchain

Blockchain

Blockchain

Blockchain

COPPE UFRJ

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Transferência de valores sem taxas

Transferência imediata de valores

Eliminação de intermediários

Blockchain

Blockchain

COPPE UFRJ

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Transferência de valores sem taxas

Transferência imediata de valores

Eliminação de intermediários

FIM dos bancos e instituições financeiras

Blockchains: Motivação

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Transferência de valores sem taxas

OK, mas o que é uma blockchain?
Como **funciona**?

FIM dos bancos e instituições financeiras

Transferência de Ativos

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Ativo: um recurso **único** que possui um **valor** e pertence a um **dono**

COPPE UFRJ

Transferência de Ativos

- Ativo: um recurso **único** que possui um **valor** e pertence a um **dono**

146.164.69.202

Transferência de Ativos

- Ativo: um recurso **único** que possui um **valor** e pertence a um **dono**

146.164.69.202

- Transferência física de ativos: enviar ou receber o ativo

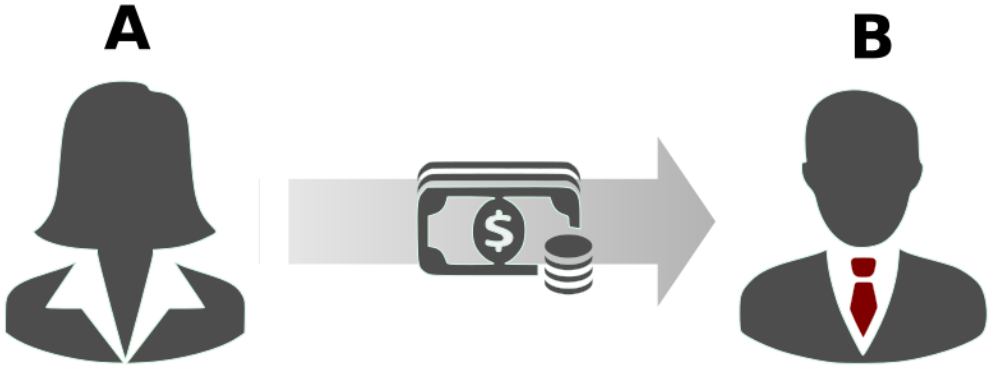
Transferência de Ativos

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Ativo: um recurso **único** que possui um **valor** e pertence a um **dono**

146.164.69.202

- Transferência física de ativos: enviar ou receber o ativo



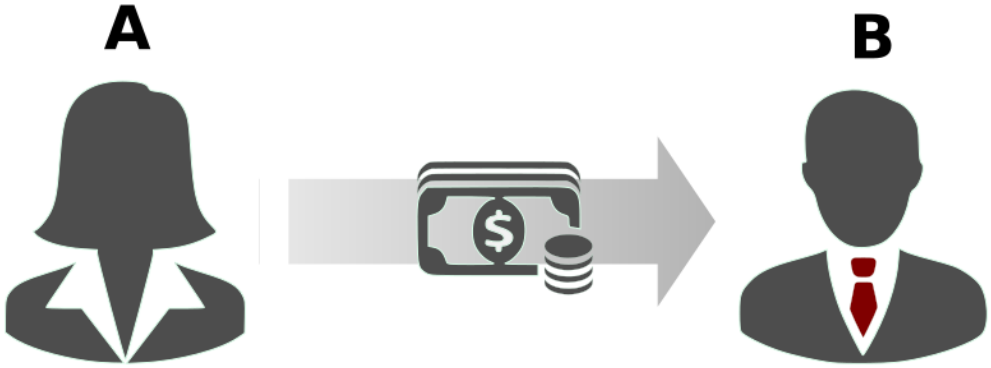
COPPE UFRJ

Transferência de Ativos

- Ativo: um recurso **único** que possui um **valor** e pertence a um **dono**


146.164.69.202

- Transferência física de ativos: enviar ou receber o ativo
  - Desvantagem → alcance ou tempo de transferência



O Problema do Gasto Duplo

O Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

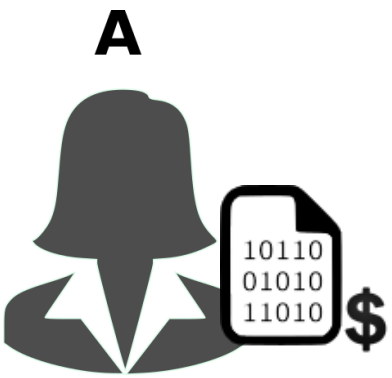
- Possibilidade de **gasto duplo** do mesmo ativo

COPPE UFRJ

O Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Possibilidade de **gasto duplo** do mesmo ativo

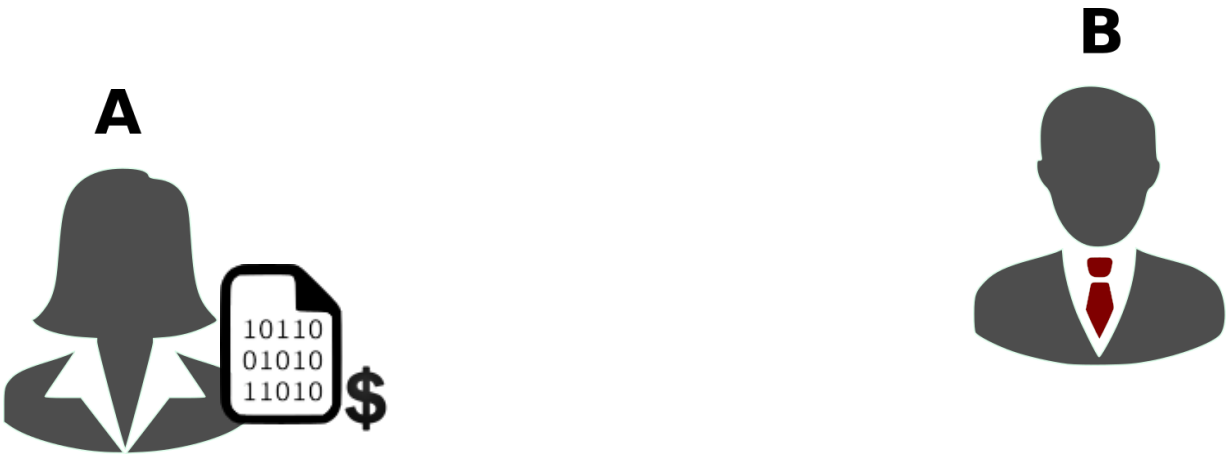


COPPE UFRJ

O Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Possibilidade de **gasto duplo** do mesmo ativo



COPPE UFRJ

O Problema do Gasto Duplo

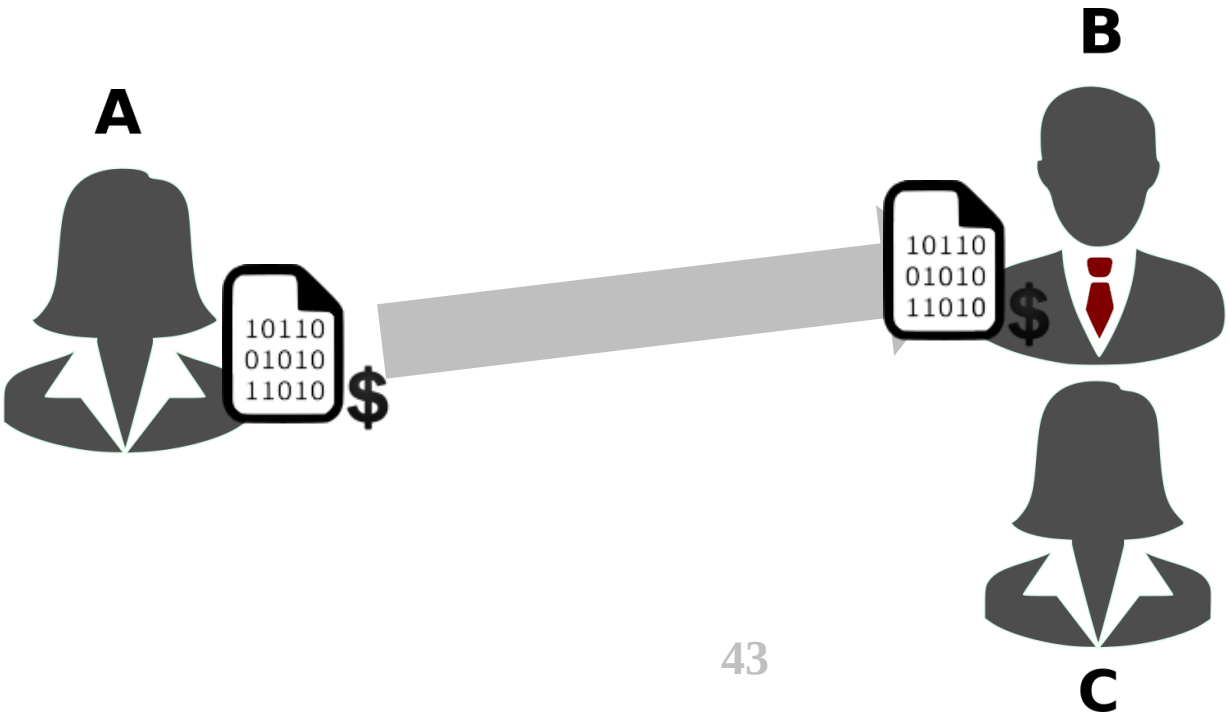
GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Possibilidade de **gasto duplo** do mesmo ativo

COPPE UFRJ

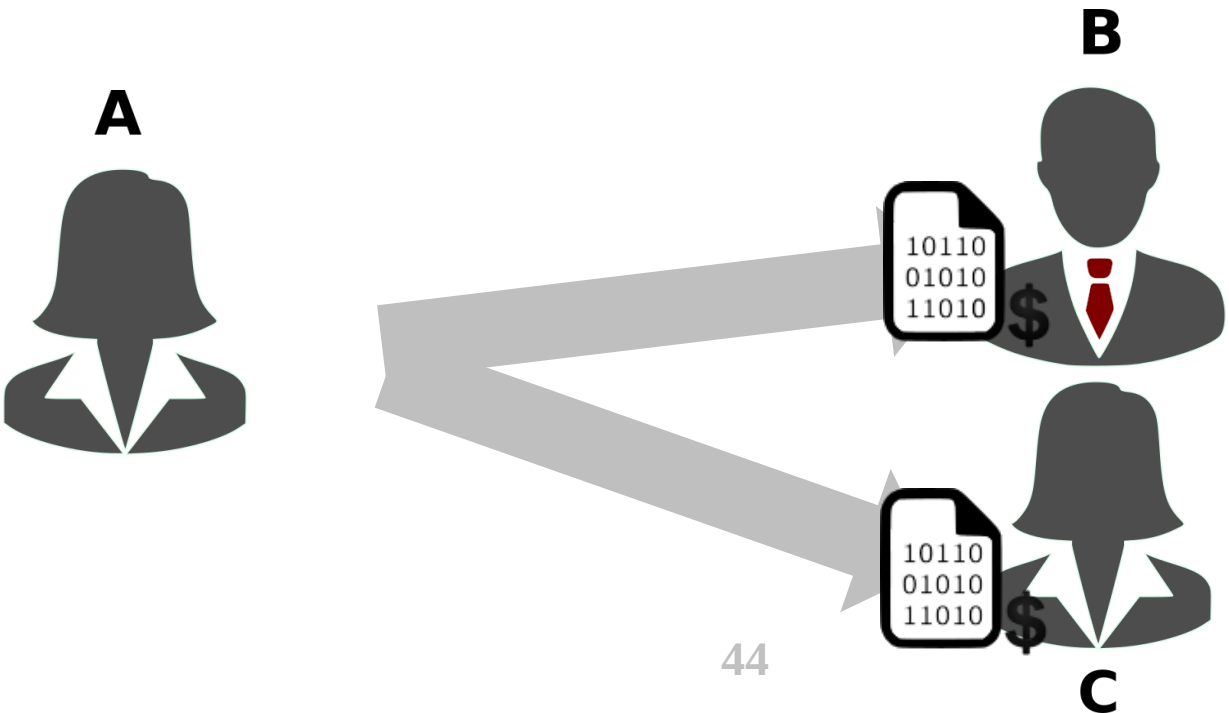
O Problema do Gasto Duplo

- Possibilidade de **gasto duplo** do mesmo ativo



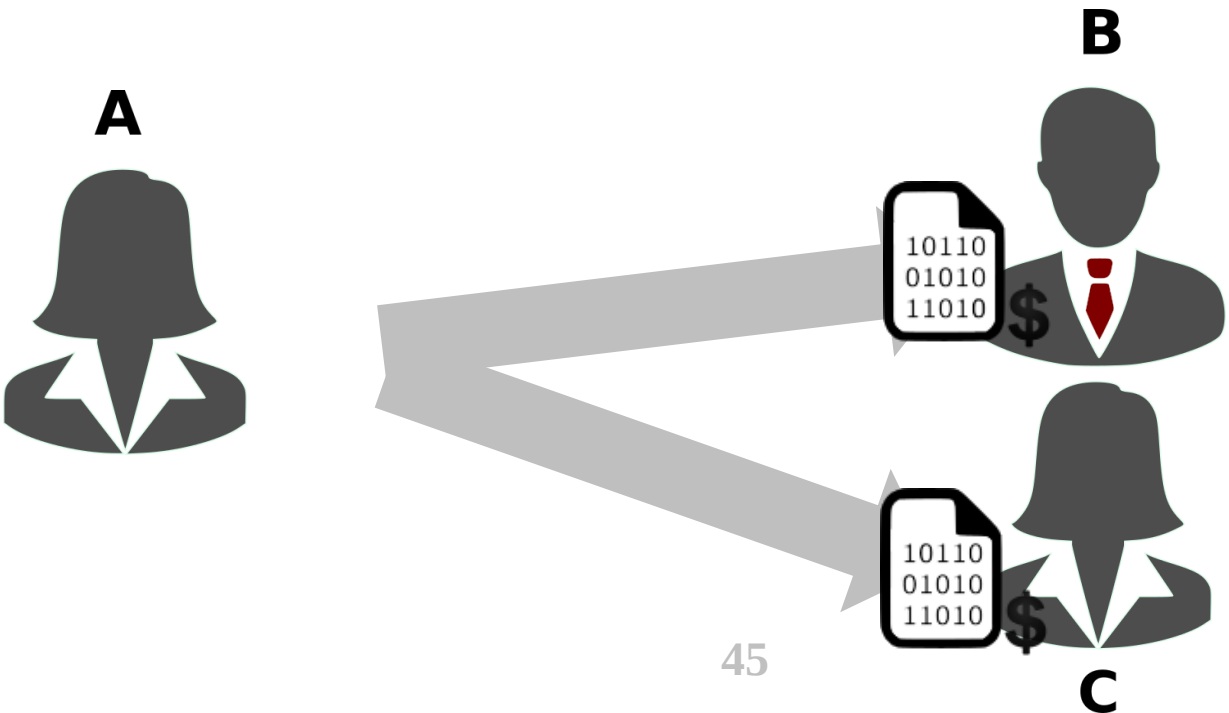
O Problema do Gasto Duplo

- Possibilidade de **gasto duplo** do mesmo ativo



O Problema do Gasto Duplo

- Possibilidade de **gasto duplo** do mesmo ativo
- Alta probabilidade de **comportamento malicioso**

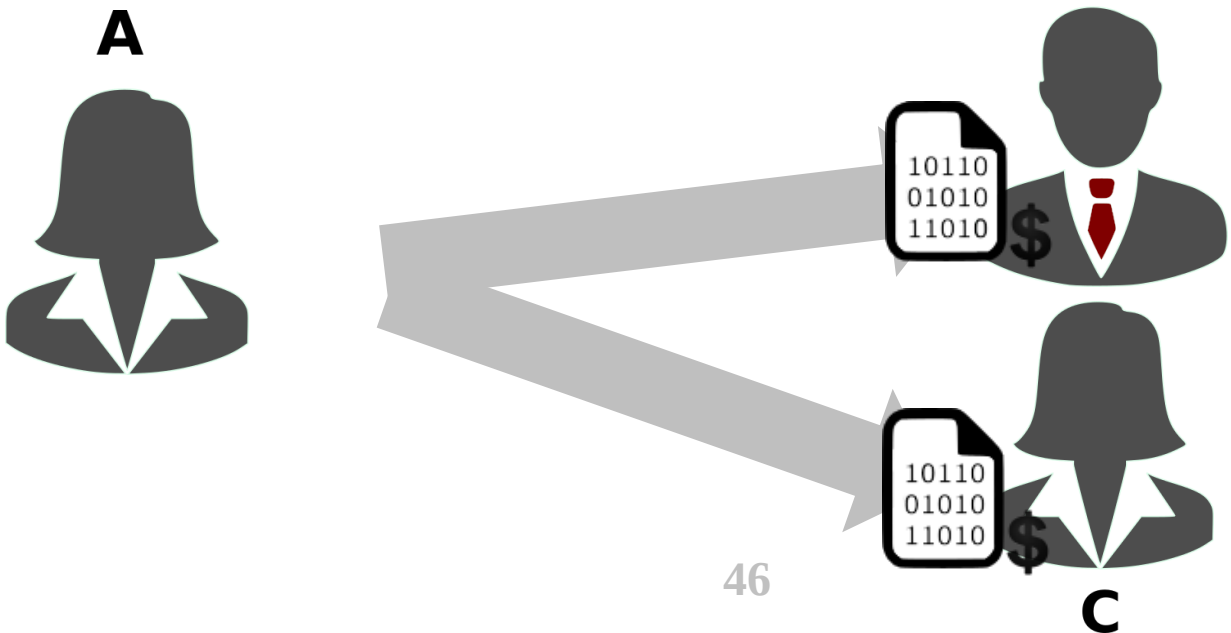


O Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Possibilidade de **gasto duplo** do mesmo ativo

Entidades pares não possuem **confiança mútua**



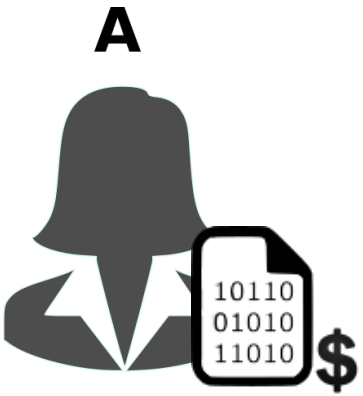
COPPE UFRJ

Solução Tradicional (Intermediação)

- Transferência de ativos online → **intermediários**

Solução Tradicional (Intermediação)

- Transferência de ativos online → **intermediários**



Solução Tradicional (Intermediação)

- Transferência de ativos online → **intermediários**

Solução Tradicional (Intermediação)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Transferência de ativos online → **intermediários**

COPPE UFRJ

Solução Tradicional (Intermediação)

- Transferência de ativos online → **intermediários**

Solução Tradicional (Intermediação)

- Transferência de ativos online → **intermediários**

Solução Tradicional (Intermediação)

- Transferência de ativos online → **intermediários**

- Desvantagens
  - **Confiança** em uma autoridade centralizada
  - Encargos de serviço
  - Comprometimento da **privacidade** e **anonimidade**
  - Ponto único de falha

Solução Tradicional (Intermediação)

- Transferência de ativos online → **intermediários**

Como transferir ativos online **sem um intermediário**?

  - Ponto único de falha

Solução Descentralizada (Blockchain)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Mais de 30 anos depois...

COPPE UFRJ

Solução Descentralizada (Blockchain)

- Mais de 30 anos depois...

- Em novembro de 2008, Satoshi Nakamoto envia uma resposta em uma lista de e-mails com a solução do problema do gasto duplo usando técnicas criptográficas simples e conhecidas

Bitcoin: A Peer-to-Peer Electronic Cash System

Resolvendo o Problema do Gasto Duplo

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:

Resolvendo o Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:
  - Toda transação é **autêntica** →

COPPE UFRJ

Resolvendo o Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:
  - Toda transação é **autêntica** →
  - O **histórico completo** de transações está disponível para **todos os participantes da rede** →

COPPE UFRJ

Resolvendo o Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:
  - Toda transação é **autêntica** →
  - O **histórico completo** de transações está disponível para **todos os participantes da rede** →
  - Transações passadas **não podem ser alteradas**

COPPE UFRJ

Resolvendo o Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:
  - Toda transação é **autêntica** → **asssinatura** pelo emissor (criptografia de chaves assimétricas)
  - O **histórico completo** de transações está disponível para **todos os participantes da rede** →
  - Transações passadas **não podem ser alteradas**

COPPE UFRJ

Resolvendo o Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:
  - Toda transação é **autêntica** → **asssinatura** pelo emissor (criptografia de chaves assimétricas)
  - O **histórico completo** de transações está disponível para **todos os participantes da rede** → **replicação**
  - Transações passadas **não podem ser alteradas**

COPPE UFRJ

Resolvendo o Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:
  - Toda transação é **autêntica** → **asssinatura** pelo emissor (criptografia de chaves assimétricas)
  - O **histórico completo** de transações está disponível para **todos os participantes da rede** → **replicação**
  - Transações passadas **não podem ser alteradas** → integridade baseada em **funções resumo** (*hash*)

COPPE UFRJ

Resolvendo o Problema do Gasto Duplo

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Para resolver o problema do gasto duplo de maneira **descentralizada**, é necessário garantir que:

A corrente de blocos **reúne** conceitos **simples** para resolver o problema do gasto duplo

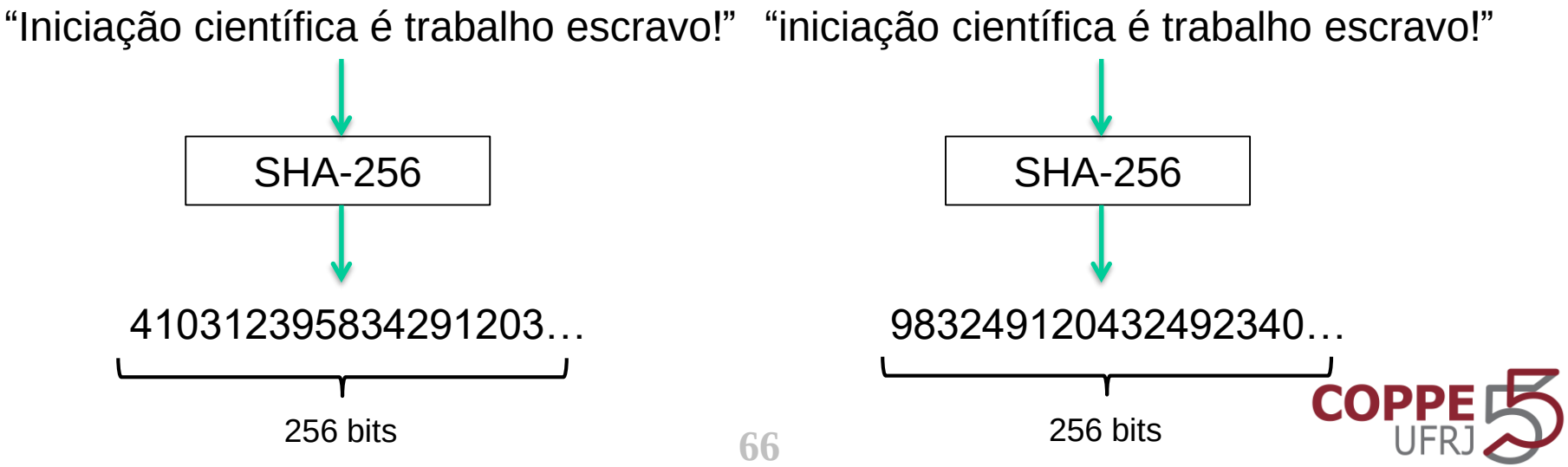
integridade baseada em **funções resumo** (*hash*)

COPPE UFRJ

Revisão de Fundamentos de Criptografia e Replicação

Funções Resumo

- Uma função resumo (hash) recebe um conjunto de dados de **qualquer tamanho** e produz uma saída aleatória de **tamanho fixo**
- Qualquer alteração no conjunto de entrada gera uma nova saída aleatória → garante a **integridade** dos dados



Colisões de Hash

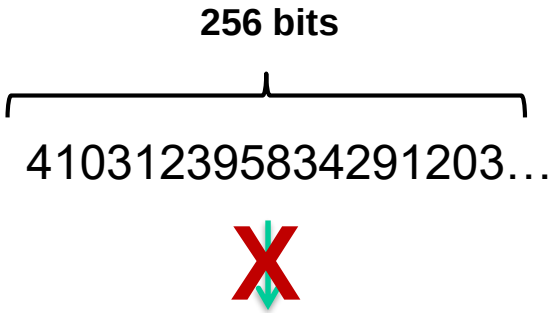
GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Mensagens de N bits geram resumos de 256 bits
- É possível achar duas (ou mais) entradas que são mapeadas no mesmo resumo?
  - Problema do aniversário

COPPE UFRJ

Reversão de Hash

- Porém, se temos apenas o resumo...
  - É necessário testar todas as possibilidades de mensagens → **força bruta**
  - Praticamente impossível recriar a mensagem original

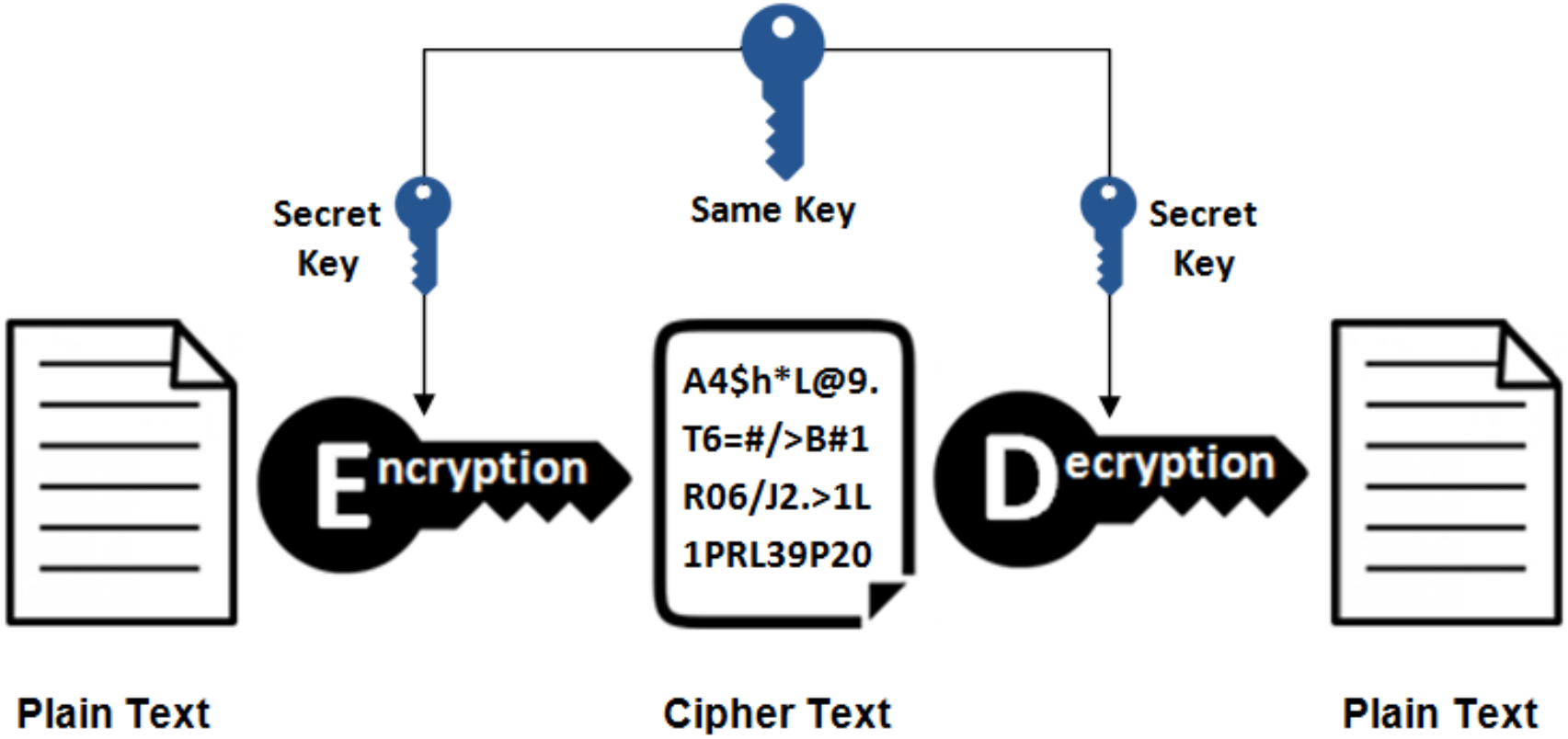


"Iniciação científica é trabalho escravo!"

Criptografia Simétrica

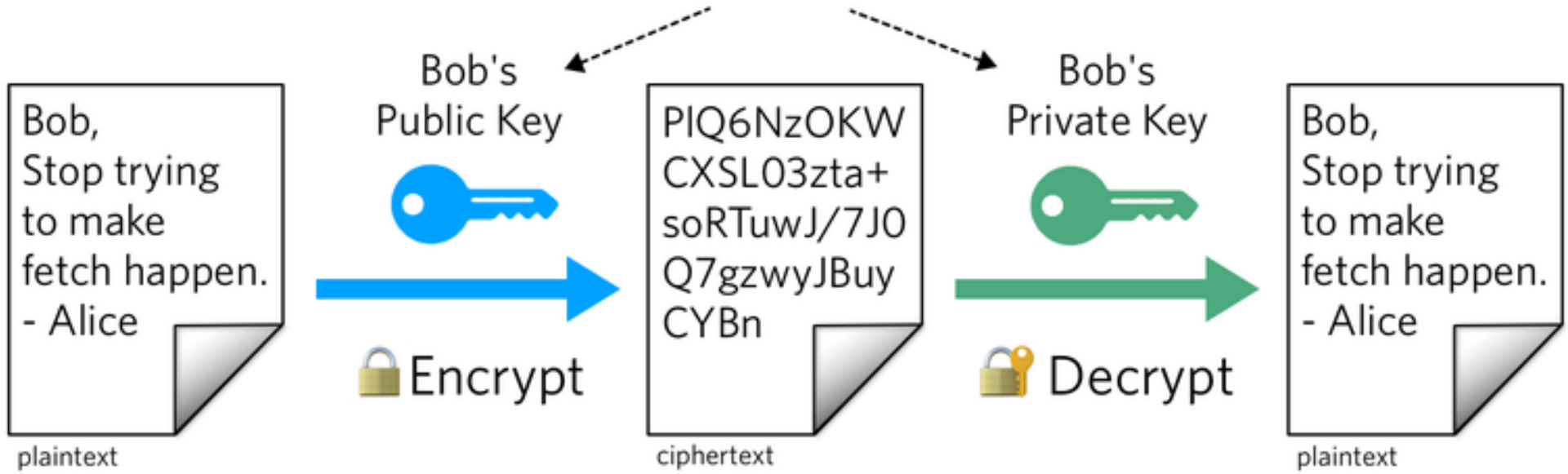
GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Chaves iguais para os dois interlocutores
  - **Chave simétrica**



Criptografia Assimétrica

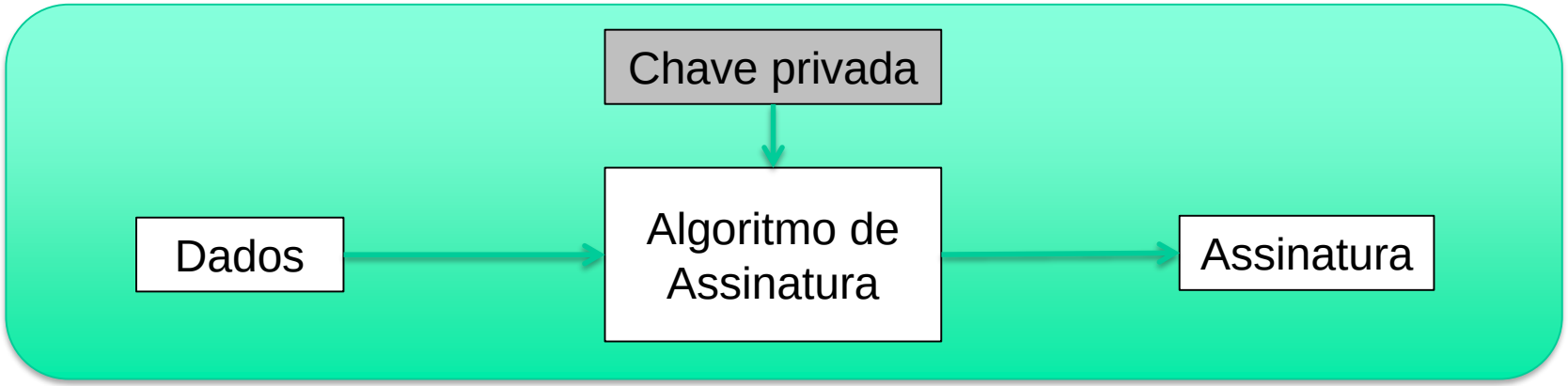
- Chaves são diferentes, mas estão **associadas**
  - **Chave pública** e **chave privada**

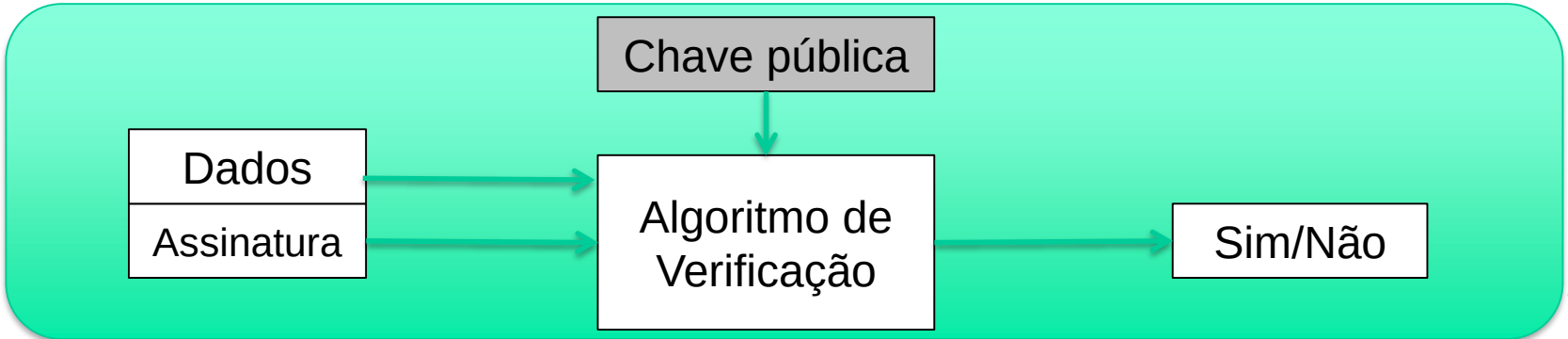


Assinaturas Digitais

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Par de chaves assimétricas	
Chave pública	454F4D3E1..
Chave privada	56F23F2D..



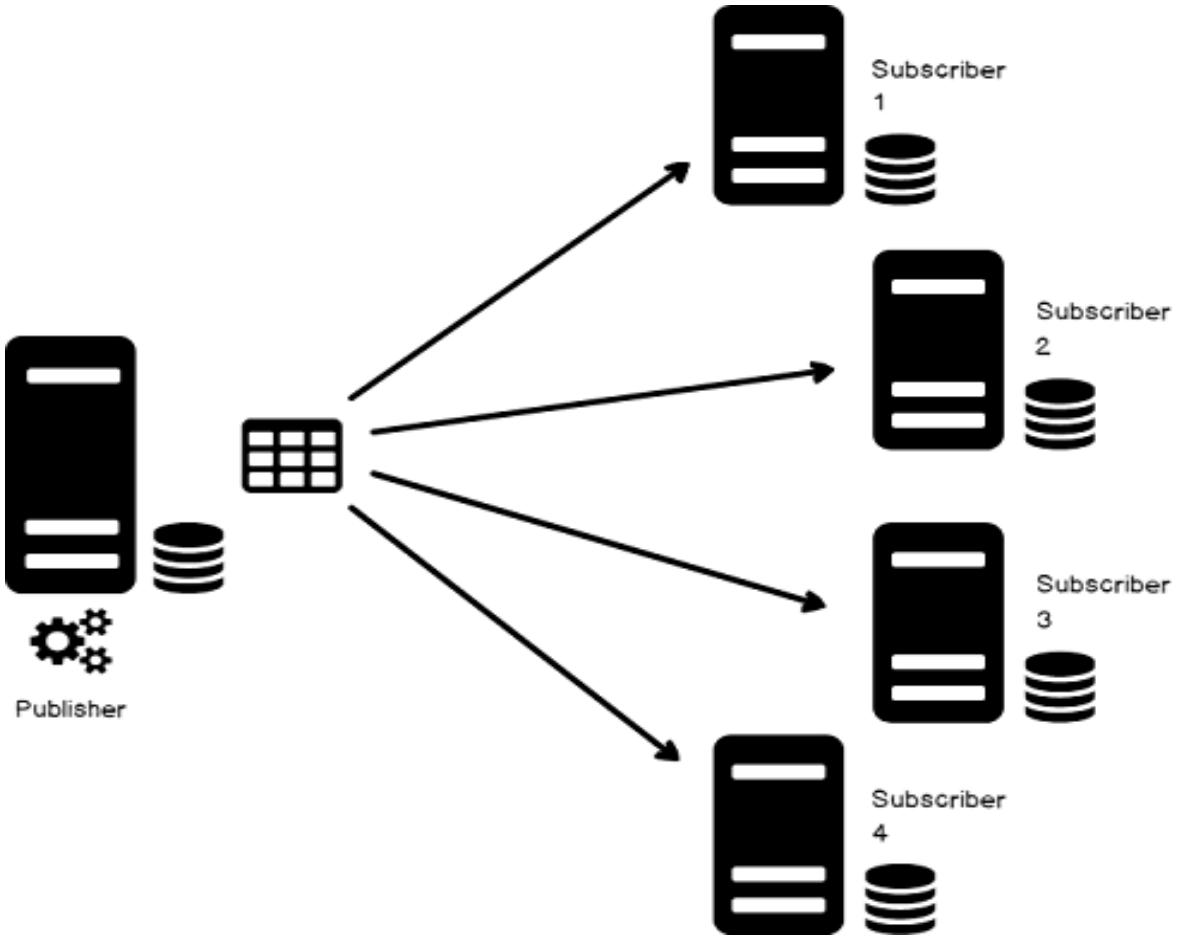


Replicação de Dados

Replicação de Dados

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- **Tolerância a falhas e auditabilidade** dos dados



COPPE UFRJ

Voltando para o problema do gasto duplo...

Corrente de Blocos (Blockchain)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

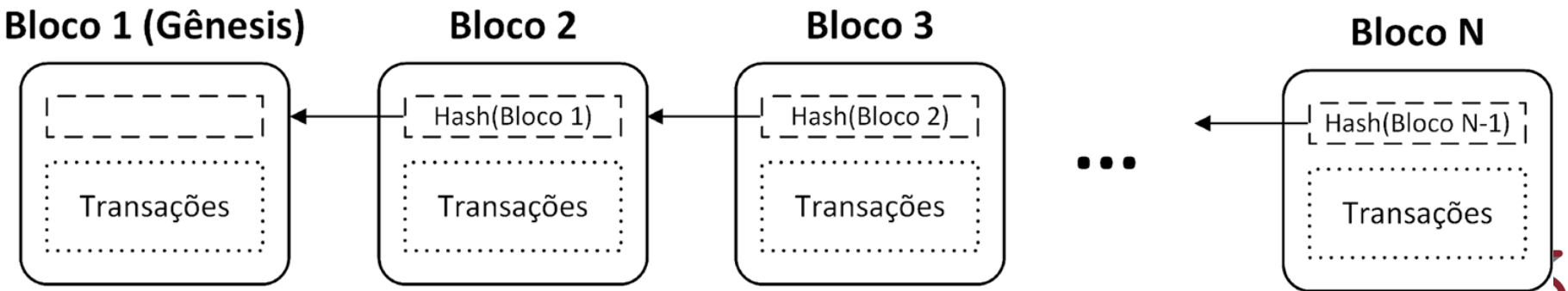
- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior

COPPE UFRJ

Corrente de Blocos (Blockchain)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

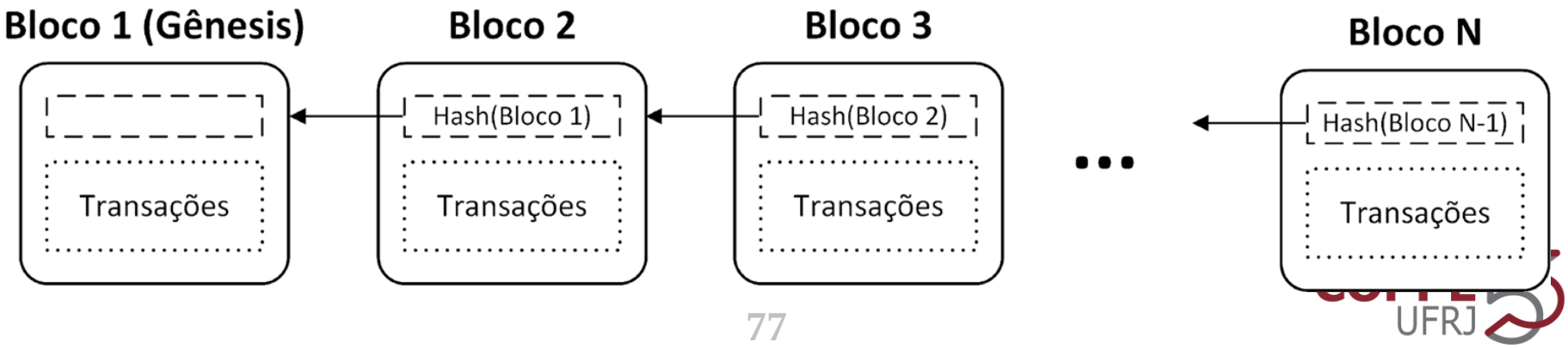
- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior



Corrente de Blocos (Blockchain)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

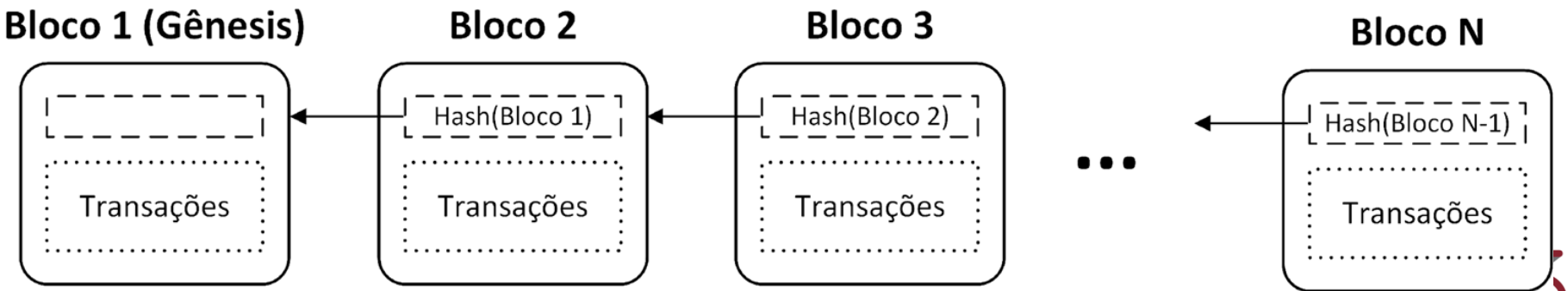
- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior
  - Cada participante possui uma **réplica** da blockchain



Corrente de Blocos (Blockchain)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

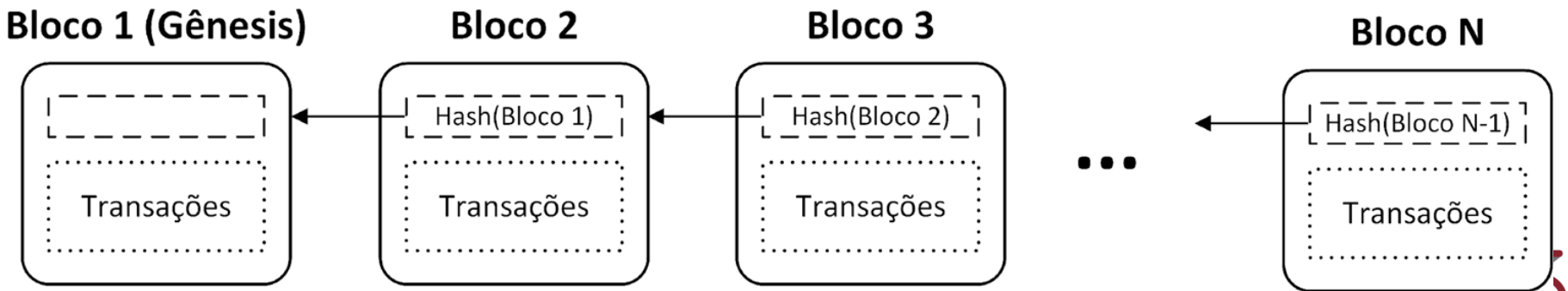
- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior
  - Cada participante possui uma **réplica** da blockchain
  - Transações são **assinadas** por seus emissores



Corrente de Blocos (Blockchain)

- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior
  - Cada participante possui uma **réplica** da blockchain
  - Transações são **assinadas** por seus emissores

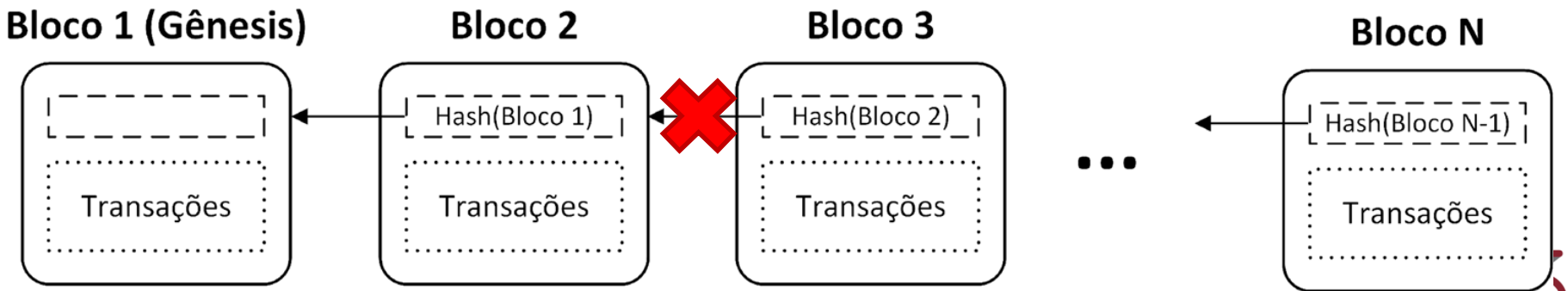
O que acontece se um atacante altera um bloco passado?



Corrente de Blocos (Blockchain)

- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior
  - Cada participante possui uma **réplica** da blockchain
  - Transações são **assinadas** por seus emissores

O que acontece se um atacante altera um bloco passado?

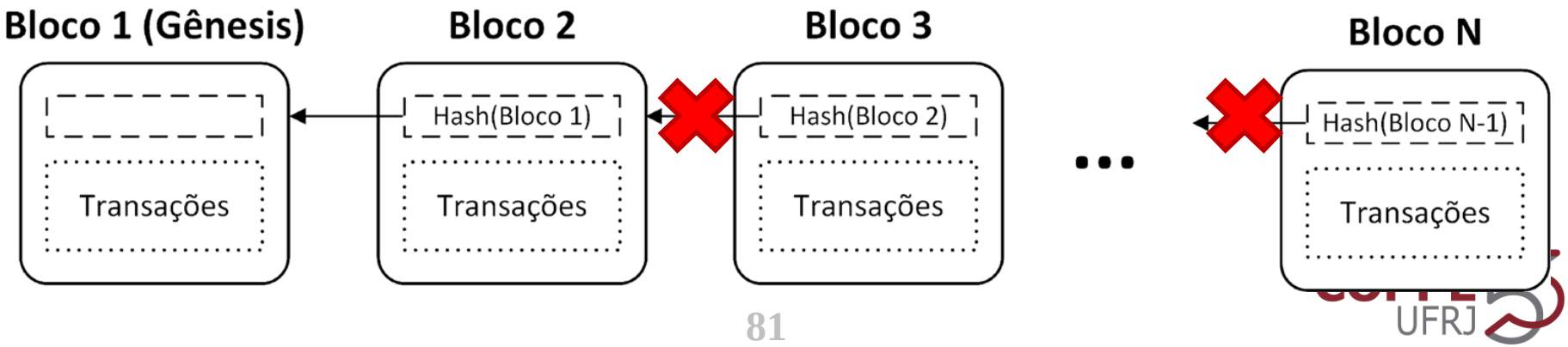


Corrente de Blocos (Blockchain)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

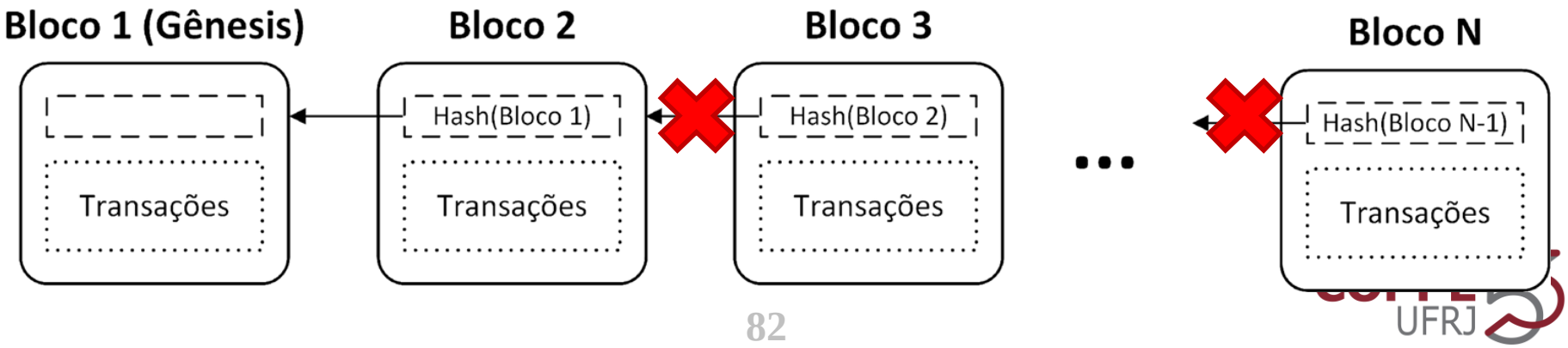
- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior
  - Cada participante possui uma **réplica** da blockchain
  - Transações são **assinadas** por seus emissores

O que acontece se um atacante altera um bloco passado?



Corrente de Blocos (Blockchain)

- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior
  - Cada participante possui uma **réplica** da blockchain
  - Transações são **assinadas** por seus emissores

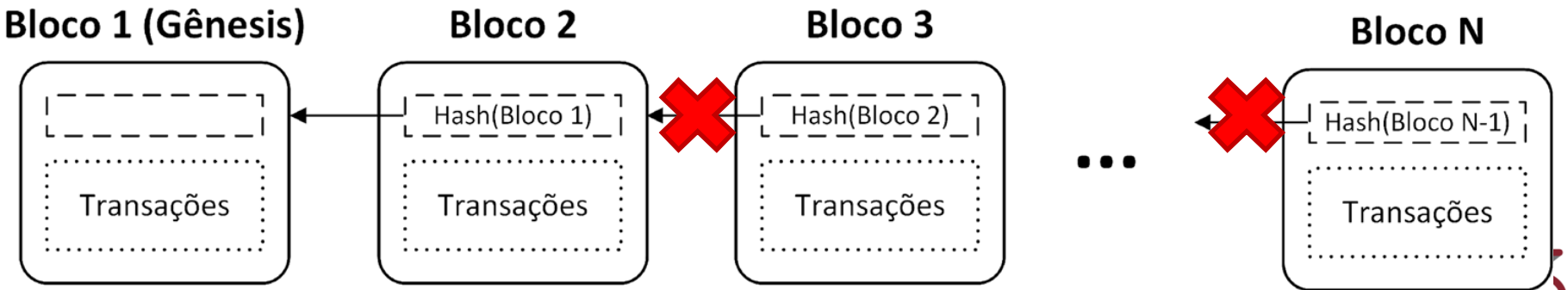


Corrente de Blocos (Blockchain)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Livro-razão **distribuído** e **público** organizado em **blocos**
  - Cada bloco contém o ***hash*** do bloco anterior
  - Cada participante possui uma **réplica** da blockchain
  - Transações são **assinadas** por seus emissores

- A replicação e integridade garantem **imutabilidade** e **não-repúdio** das transações



Transações no Bitcoin

Transações no Bitcoin

- **Anonimidade** → Identificador de um participante é sua chave pública (pseudonimidade)

Transações no Bitcoin

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- **Anonimidade** → Identificador de um participante é sua chave pública (pseudonimidade)
- **Autenticidade e Integridade** → Verificação da assinatura através da chave pública

COPPE UFRJ

Transações no Bitcoin

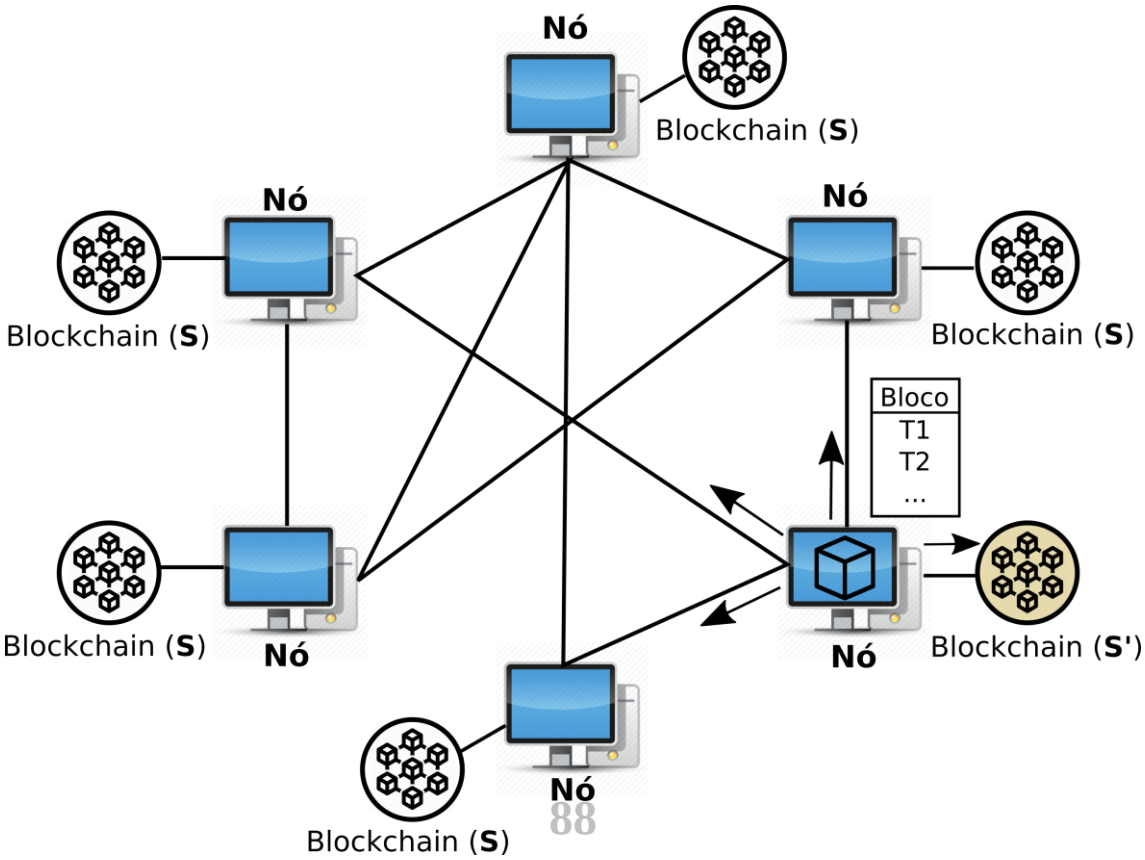
- **Anonimidade** → Identificador de um participante é sua chave pública (pseudonimidade)
- **Autenticidade e Integridade** → Verificação da assinatura através da chave pública

Transação #8423	
De	Ch_Pública1
Para	Ch_Pública2
Quantidade	50 BTC
Assinatura	345349354

Consenso em Correntes de Blocos

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- A corrente de blocos é um **sistema distribuído**
  - Os nós da rede devem concordar sobre o estado global

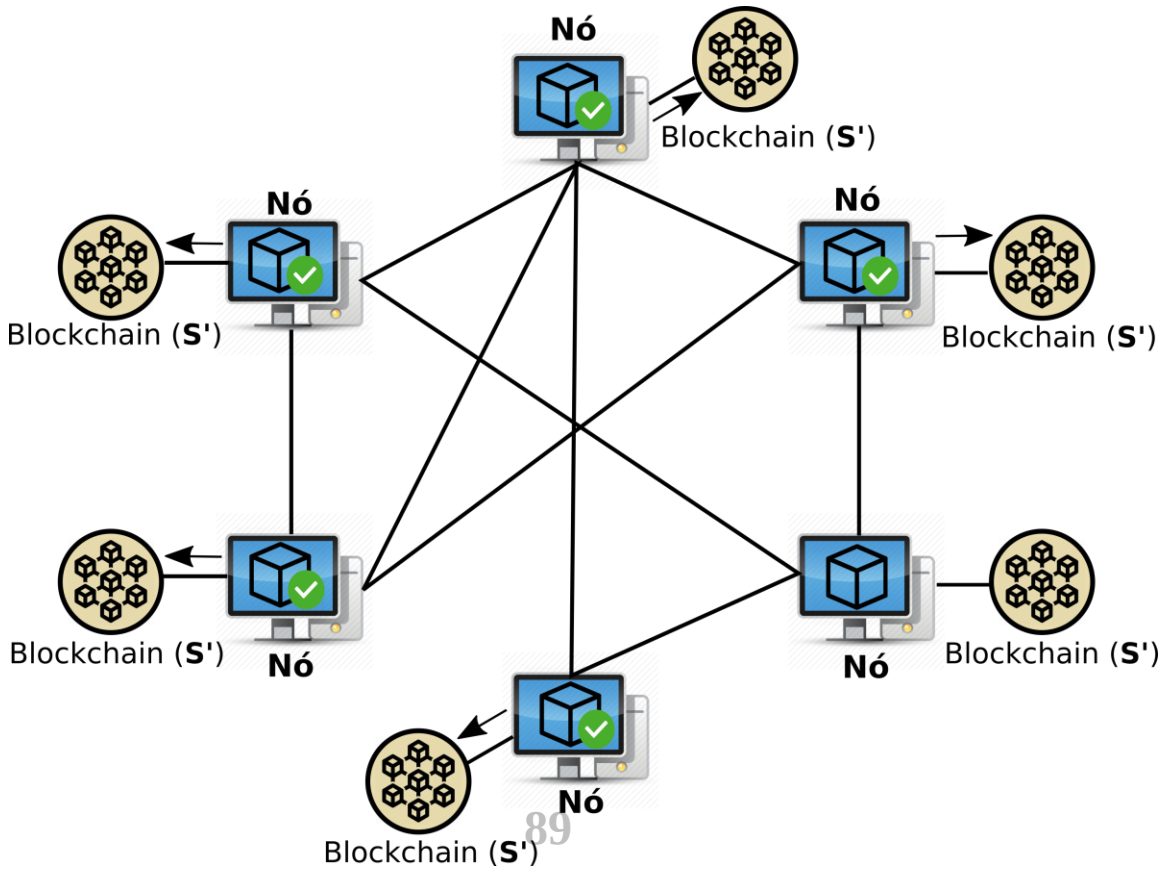


COPPE UFRJ

Consenso em Correntes de Blocos

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- A corrente de blocos é um **sistema distribuído**
  - Os nós da rede devem concordar sobre o estado global

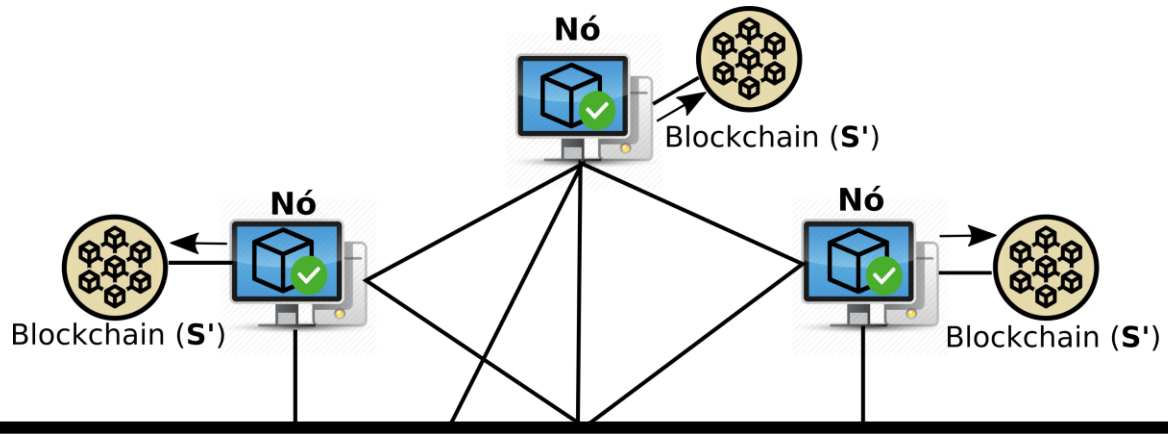


COPPE UFRJ

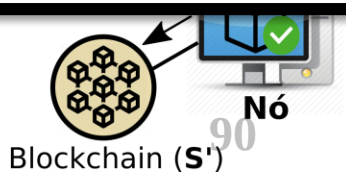
Consenso em Correntes de Blocos

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- A corrente de blocos é um **sistema distribuído**
  - Os nós da rede devem concordar sobre o estado global



Desafio: como garantir sincronia do estado global?
Como definir quem propõe um novo bloco?



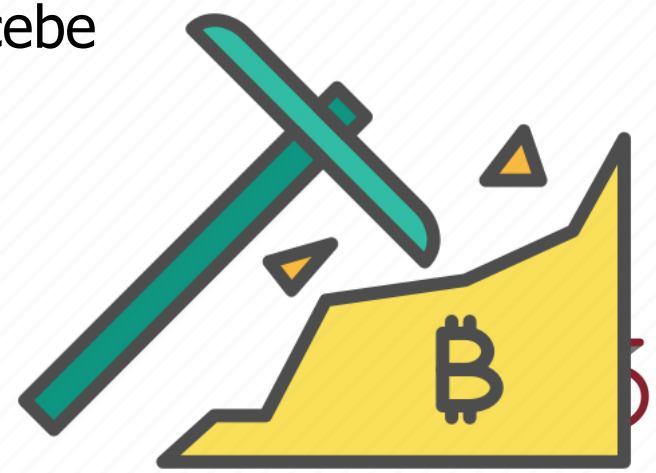
COPPE UFRJ

Prova de Trabalho (Proof of Work – PoW)

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Proposta por Nakamoto no artigo original do Bitcoin

- Algoritmo de consenso baseado em competição
  - Lança-se um desafio computacional na rede
  - Nós gastam processamento para resolver o desafio
  - O primeiro que resolver o desafio divulga a solução
  - Se a solução for aceita, o vencedor recebe uma recompensa em Bitcoins



Prova de Trabalho

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Função resumo é unívoca
  - Obter o conjunto de entrada → **força bruta**
  - Verificar uma resposta → basta aplicar a função
- Encontrar um conjunto de N zeros no início da entrada requer 2^N operações
- Se aplicarmos a função a um "nonce" incremental, podemos calcular saídas com N zeros:

in 3e-05 seconds, nonce = 0 yielded 0 zeros. value = 4c8f1205f49e70248939df9c7b704ace62c2f…
in 0.000138 seconds, nonce = 12 yielded 1 zeros. value = **0**5017256be77ad2985b36e75e486af9s…
in 0.000482 seconds, nonce = 112 yielded 2 zeros. value = **00**ae7e0956382f55567d0ed9311cfd41…
in 0.014505 seconds, nonce = 3728 yielded 3 zeros. value = **000**b5a6cfc0f076cd81ed3a60682063…
in 0.595024 seconds, nonce = 181747 yielded 4 zeros. value = **0000**af058b74703b55e27437b89b…
in 3.491151 seconds, nonce = 1037701 yielded 5 zeros. value = **00000**e55bd0d2027f3024c378e…
in 32.006105 seconds, nonce = 9913520 yielded 6 zeros. value = **00000**77a77854ee39dc0dc97…
in 590.89462 seconds, nonce = 186867248 yielded 7 zeros. value = **0000000**225060b16117b23d…
in 4686.171007 seconds, nonce = 1424462909 yielded 8 zeros. value = **00000000**2dd7437246…

COPPE UFRJ

Dificuldade da Prova de Trabalho

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Função resumo produz saída aleatória → encontrar N zeros é o mesmo que jogar uma moeda e obter N coroas em seguida
- Para N zeros, na média, deve-se tentar $2^N/2$ nonces
  - N = 1 … Tente 1 nonce
  - N = 16 … Tente 32768 nonces
  - N = 32 … Tente 2 billion nonces

COPPE UFRJ

Dificuldade da Prova de Trabalho

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Função resumo produz saída aleatória → encontrar N zeros é o mesmo que jogar uma moeda e obter N coroas em seguida
- Para N zeros, na média, deve-se tentar $2^N/2$ nonces
  - N = 1 … Tente 1 nonce
  - N = 16 … Tente 32768 nonces
  - N = 32 … Tente 2 billion nonces

Vencer a rodada **prova** que o participante **trabalhou**!

COPPE UFRJ

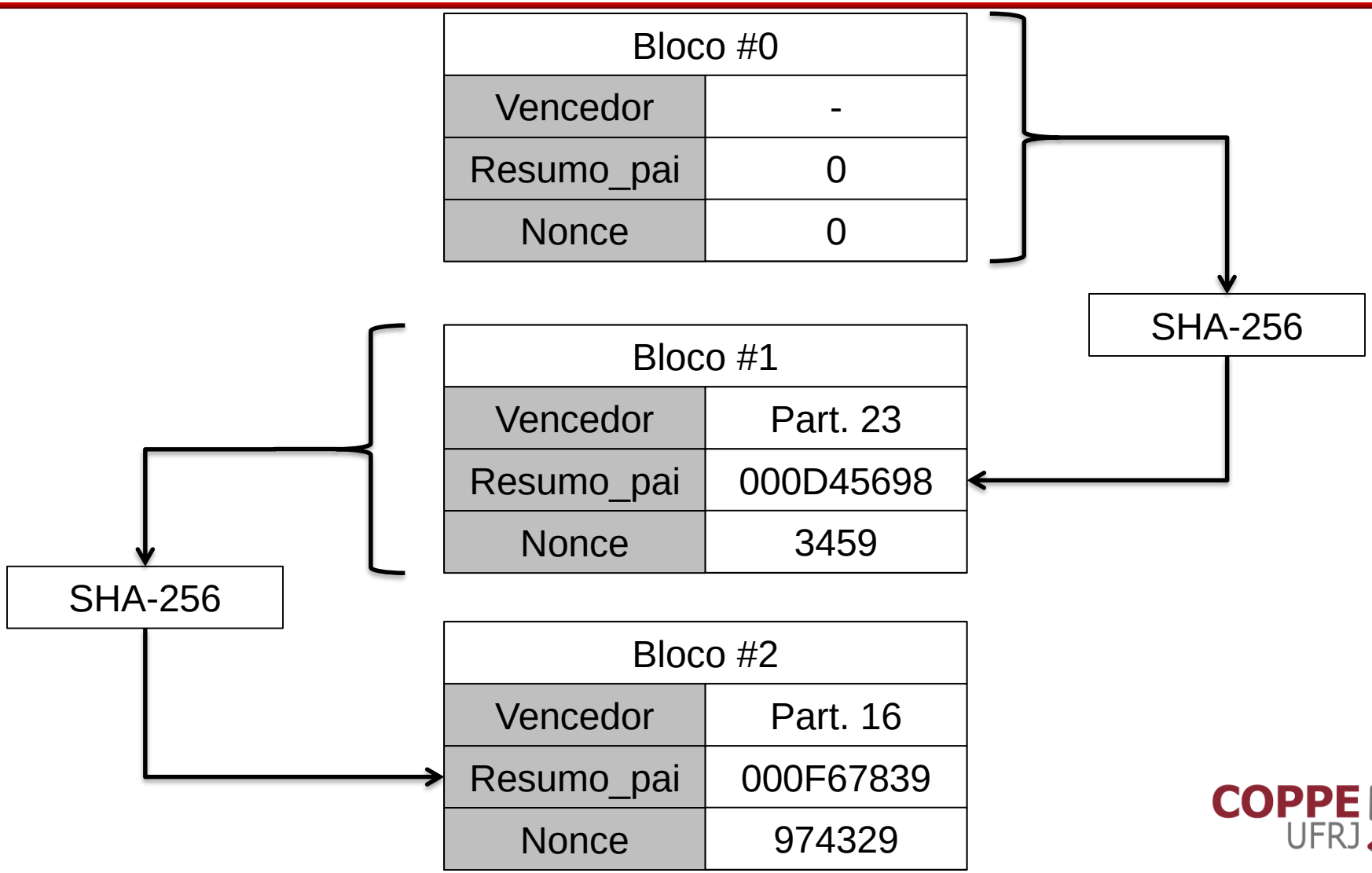
Prova de Trabalho

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- A prova de trabalho é como um **jogo** de criar blocos
- Cada participante possui uma lista dos blocos anteriores
- Um parâmetro N define o número alvo de zeros
- Participantes **acumulam pontos** ao criar um novo bloco
  - Aplicar a função resumo ao último bloco
  - Encontrar um hash do novo bloco iniciado por pelo menos N zeros usando um nonce
  - Transmitir o novo bloco a todos os participantes

COPPE UFRJ

Corrente de Blocos



Bifurcações na Corrente

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

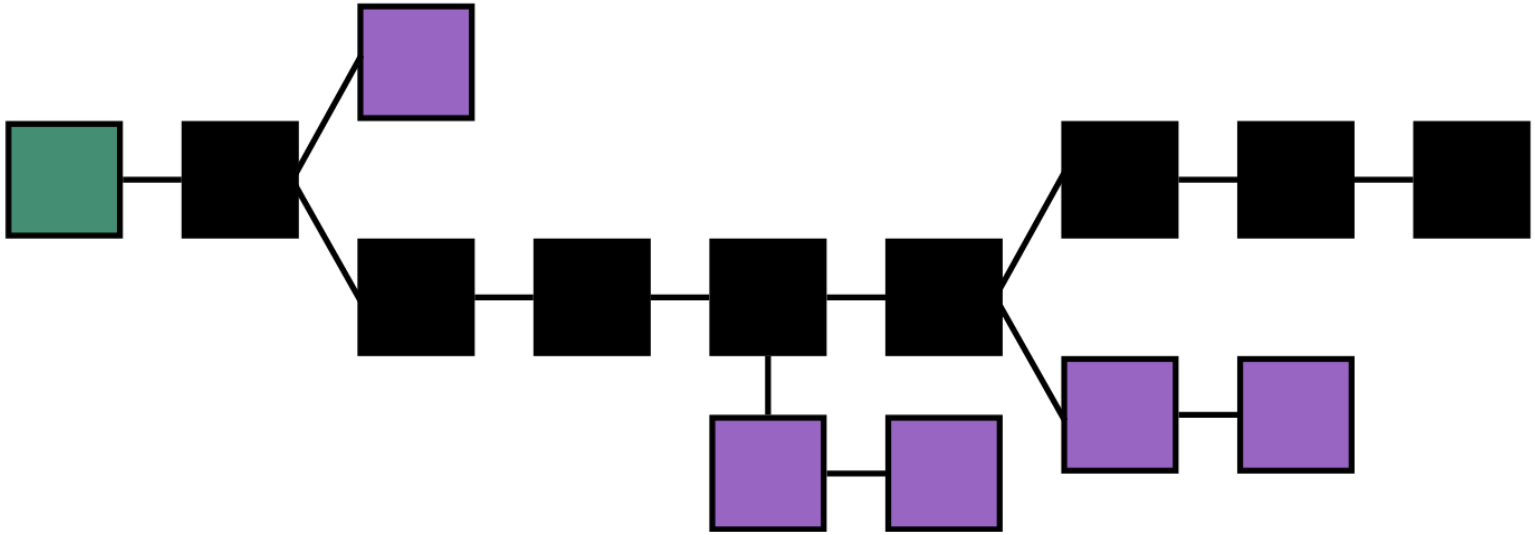
- E se dois participantes vencem ao mesmo tempo?

COPPE UFRJ

Bifurcações na Corrente

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- E se dois participantes vencem ao mesmo tempo?
- Regra da cadeia mais longa: maior gasto computacional
  - Cada participante considera o bloco que chega primeiro
  - Após outra rodada, escolhe-se a **corrente mais longa**
  - Blocos podem ser **abandonados**
  - Um bloco só é confirmado após 6 rodadas (estimativa)

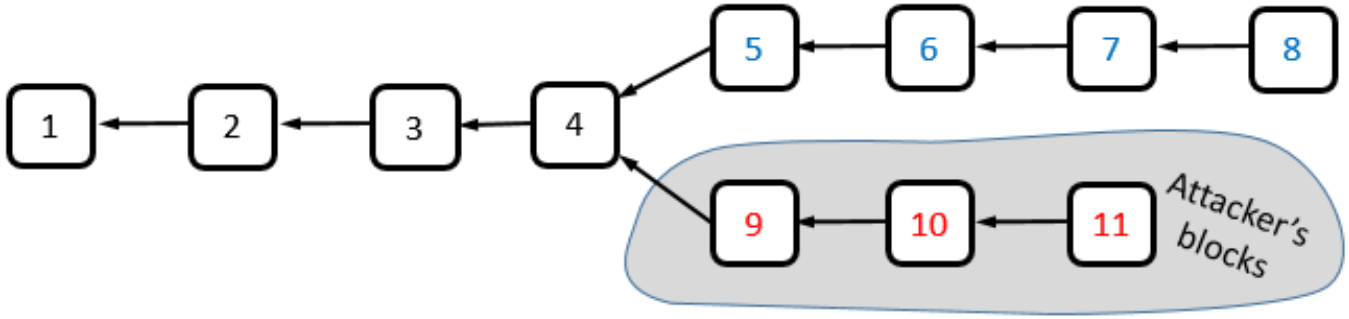


Fraudes na Prova de Trabalho

- Prova de Trabalho → baseado no poder computacional
- **Assume-se** que nenhum participante é capaz de vencer a maior parte das rodadas
- O que acontece se uma pessoa detém a maior parte do poder computacional da rede?

Fraudes na Prova de Trabalho

- Prova de Trabalho → baseado no poder computacional
- **Assume-se** que nenhum participante é capaz de vencer a maior parte das rodadas
- O que acontece se uma pessoa detém a maior parte do poder computacional da rede?
  - Ataque dos 51% → atacante detém a maior cadeia
    - Permite transações com **gasto duplo**
    - Rede não é mais **confiável**

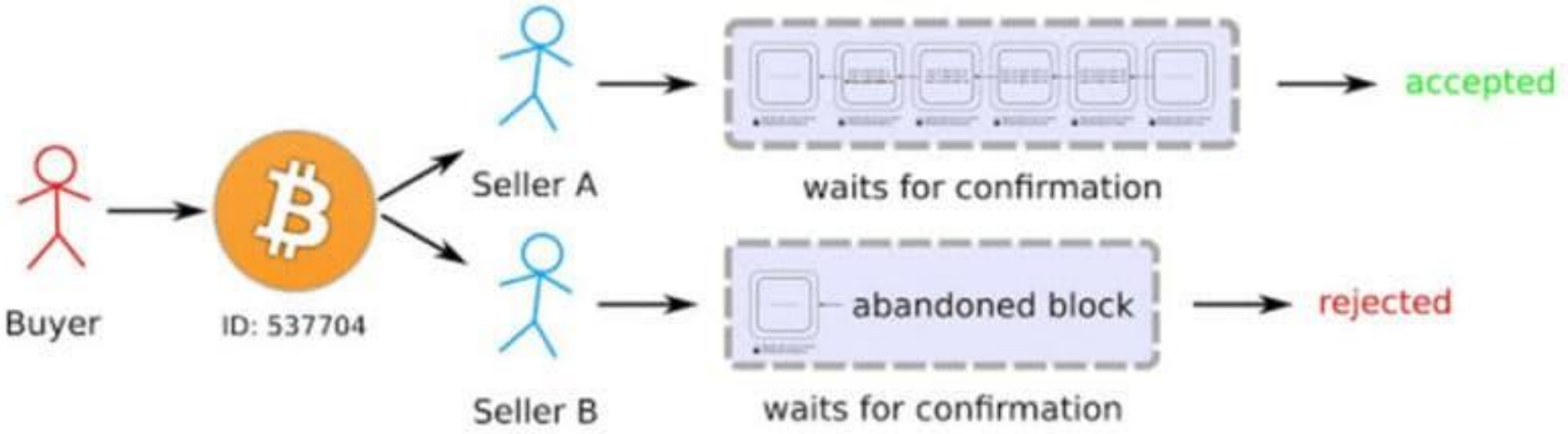


Bitcoin

- Participantes = mineradores, pontos = bitcoins
- Transações enviam valores através de chaves públicas

Bitcoin

- Participantes = mineradores, pontos = bitcoins
- Transações enviam valores através de chaves públicas
- O **consenso** por **prova de trabalho** previne o gasto duplo sem necessidade de uma autoridade central



Bitcoin

- Recompensa por um bloco minerado
  - 12.5 BTC (2018) ~ US$ 106k
  - Inicialmente 50 BTC, a recompensa é reduzida pela metade a cada 210k blocos (~4 anos) para prevenir inflação
- Tempo de mineração: ~10min
  - A dificuldade é ajustada a cada duas semanas de acordo com o poder computacional da rede
- Vazão: ~7 transações/s
- Poder computacional: mais de 1 exahash/s (10^18)

Distribuição de Poder Computacional no Bitcoin

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

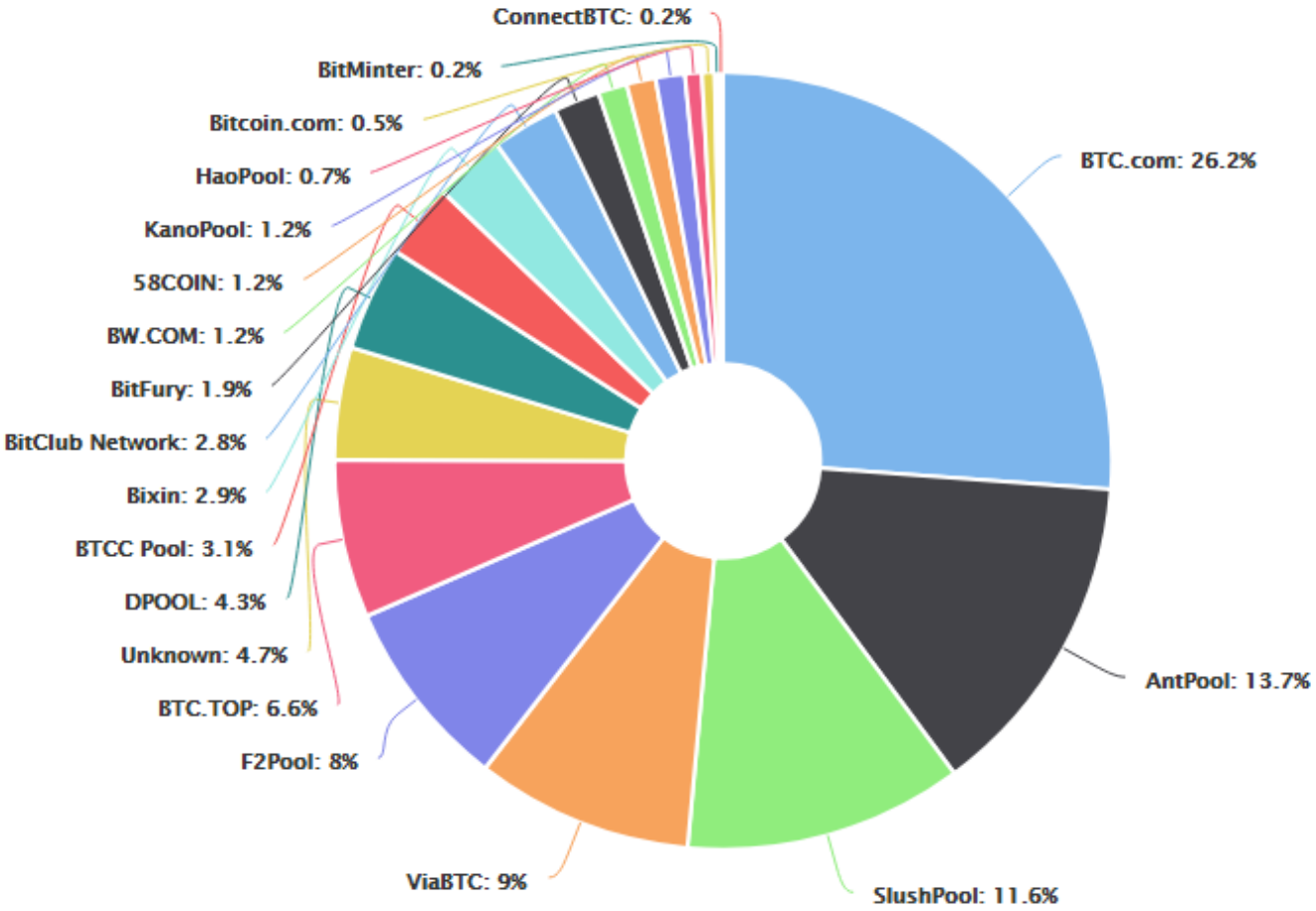
- Fonte: http://blockchain.info

COPPE UFRJ

Distribuição de Poder Computacional no Bitcoin

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Fonte: http://blockchain.info



COPPE UFRJ

Bitcoin na Prática

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- 1 petahash/s (10^15 hash/s)

PPE UFRJ

Revisão

O que é corrente de blocos?

O que é corrente de blocos?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Corrente de blocos é uma tecnologia disruptiva baseada em **criptografia, comunicação fim-a-fim, replicação de máquina de estados, consenso e teoria dos jogos** que permite prover uma **camada de confiança** e, com isto, permitir a **transferência segura de ativos**

COPPE UFRJ

O que é corrente de blocos?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Corrente de blocos é uma tecnologia disruptiva baseada em **criptografia, comunicação fim-a-fim, replicação de máquina de estados, consenso e teoria dos jogos** que permite prover uma **camada de confiança** e, com isto, permitir a **transferência segura de ativos**

A corrente de blocos em si é uma estrutura de dados encadeada e **imutável** pelo uso de funções *hash* criptográficas. A corrente de blocos só cresce.

COPPE UFRJ

O que é corrente de blocos?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Corrente de blocos é uma tecnologia disruptiva baseada em **criptografia, comunicação fim-a-fim, replicação de máquina de estados, consenso e teoria dos jogos** que permite prover uma **camada de confiança** e, com isto, permitir a **transferência segura de ativos**

A corrente de blocos em si é uma estrutura de dados encadeada e **imutável** pelo uso de funções *hash* criptográficas. A corrente de blocos só cresce.

Para que um bloco seja acrescido na corrente de blocos tem existir **consenso** entre os participantes

COPPE UFRJ

O que é corrente de blocos?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Corrente de blocos é uma tecnologia disruptiva baseada em **criptografia, comunicação fim-a-fim, replicação de máquina de estados, consenso e teoria dos jogos** que permite prover uma **camada de confiança** e, com isto, permitir a **transferência segura de ativos**

A corrente de blocos em si é uma estrutura de dados encadeada e **imutável** pelo uso de funções *hash* criptográficas. A corrente de blocos só cresce.

Para que um bloco seja acrescido na corrente de blocos tem existir **consenso** entre os participantes

A corrente de blocos é **disponível** em todos os nós participantes.

COPPE UFRJ

Qual a dificuldade de se transferir valores online?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

COPPE UFRJ 50

Qual a dificuldade de se transferir valores online?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

O maior problema é transferir ativos (moedas, valores, etc.) entre pessoas que **não possuem confiança mútua**

COPPE UFRJ

Qual a dificuldade de se transferir valores online?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

O maior problema é transferir ativos (moedas, valores, etc.) entre pessoas que **não possuem confiança mútua**

A autenticação criptográfica garante o conhecimento da origem e do destino, mas não garante a validade da operação

COPPE UFRJ

Qual a dificuldade de se transferir valores online?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

O maior problema é transferir ativos (moedas, valores, etc.) entre pessoas que **não possuem confiança mútua**

A autenticação criptográfica garante o conhecimento da origem e do destino, mas não garante a validade da operação

Por que eu não posso transferir o que eu não tenho? Que tal verificar através de prova o que a origem possui? Que tal esperar que o destino comprove que recebeu?

COPPE UFRJ

Qual a dificuldade de se transferir valores online?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

O maior problema é transferir ativos (moedas, valores, etc.) entre pessoas que **não possuem confiança mútua**

A autenticação criptográfica garante o conhecimento da origem e do destino, mas não garante a validade da operação

Por que eu não posso transferir o que eu não tenho? Que tal verificar através de prova o que a origem possui? Que tal esperar que o destino comprove que recebeu?

Esperar a realização da transferência não garante a validade pois, neste meio tempo, a origem pode gastar o mesmo recurso várias vezes

COPPE UFRJ

Qual foi a proposta inovadora genial de Satoshi Nakamoto ao propor o Bitcoin?

Qual foi a proposta inovadora genial de Satoshi Nakamoto ao propor o Bitcoin?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Resolveu o problema do gasto duplo sem intermediários com tecnologias simples já existentes

O consenso é estudado há mais de 30 anos e sempre foi um enorme desafio. Com o Bitcoin, Satoshi Nakamoto resolveu o problema do consenso de forma probabilística propondo o consenso de Prova de Trabalho (Proof of Work – PoW)

COPPE UFRJ

Em que consiste o consenso por prova de trabalho?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Satoshi Nakamoto propõe o consenso probabilístico através da prova de trabalho que consiste em **resolver um desafio** para que um novo bloco seja acrescido na corrente de blocos

A solução do desafio requer o uso de muito processamento e com isto um gasto energético muito grande

Para compensar o custo do gasto energético os ganhadores dos desafios são **incentivados** com uma **remuneração**

COPPE UFRJ

Por que o consenso PoW é probabilístico?

Por que o consenso PoW é probabilístico?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Por que pode acontecer bifurcações (*forks*) quando mais de um minerador resolve o desafio ao mesmo tempo!

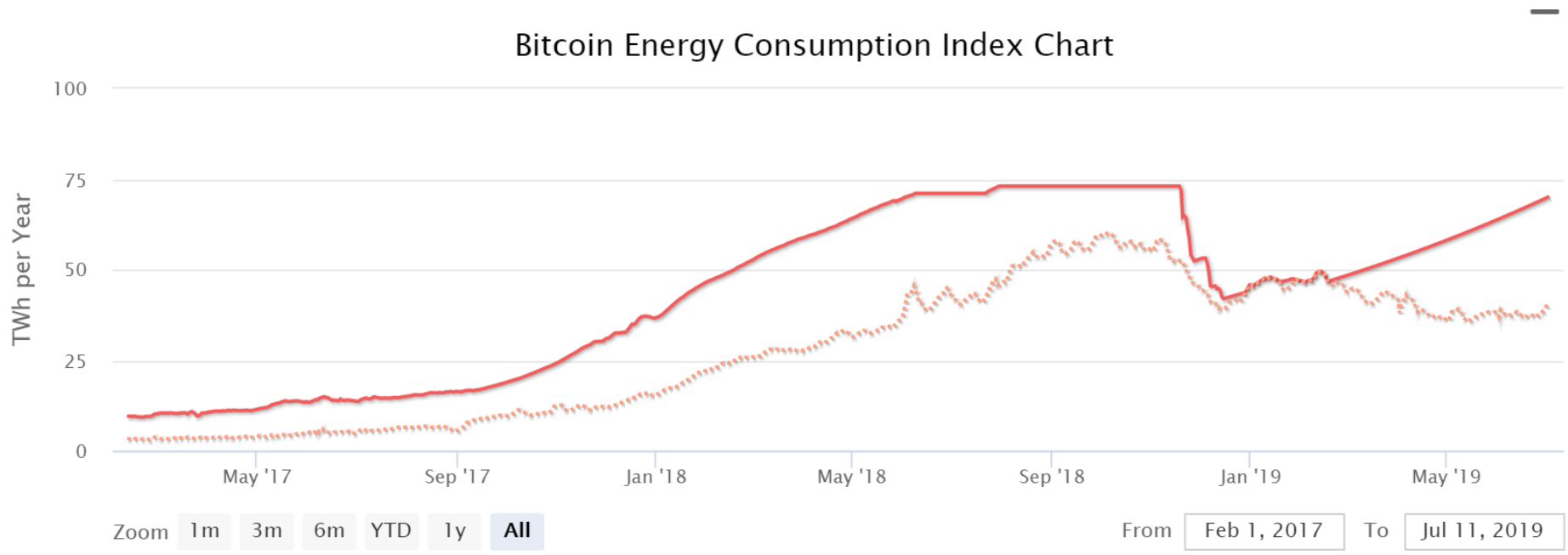
COPPE UFRJ

Parte II
Alternativas ao Bitcoin

Prova de Trabalho – Consumo Energético Bitcoin

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Consumo energético = **70 TWh** (2019)
  - Angra 1 + Angra 2 = 15,6 TWh (2014)
  - Itaipu: 96,5 TWh (2018)
  - Mais energia do que **160 países**!



Fonte: https://digiconomist.net/bitcoin-energy-consumption (Acessado em 4/7/2019)

Prova de Trabalho – Centralização

- Centralização em ASICs com alto poder computacional

Fonte: https://www.blockchain.com/pt/pools (Acessado em 4/7/2019)

Prova de Trabalho – Centralização

- Centralização em ASICs com alto poder computacional

Fonte: https://www.blockchain.com/pt/pools (Acessado em 4/7/2019)

Prova de Trabalho – Centralização

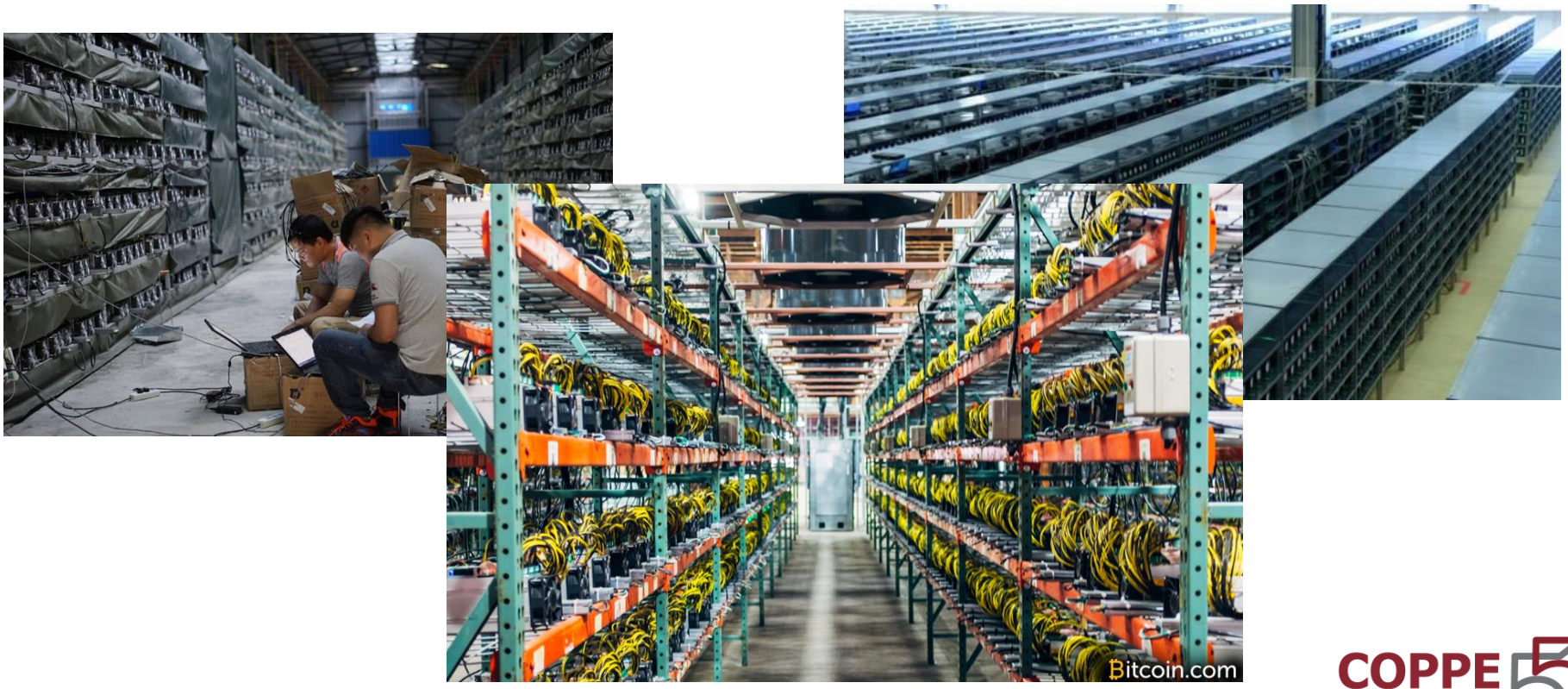
- Centralização em ASICs com alto poder computacional

Fonte: https://www.blockchain.com/pt/pools (Acessado em 4/7/2019)

Prova de Trabalho – Centralização

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Centralização em ASICs com alto poder computacional



Fonte: https://www.blockchain.com/pt/pools (Acessado em 4/7/2019)

COPPE UFRJ

Prova de Trabalho – Centralização

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Centralização em ASICs com alto poder computacional

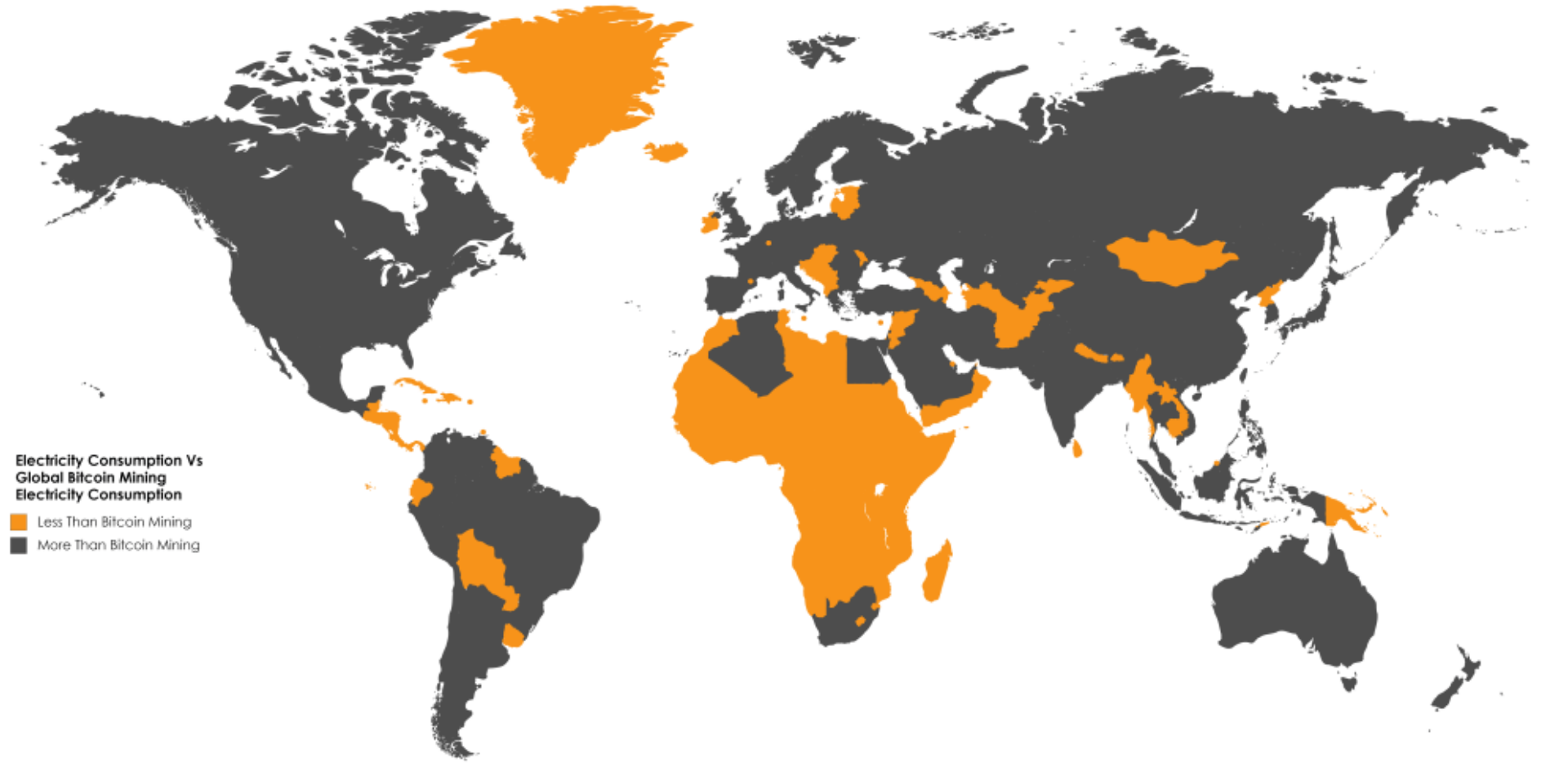
Países onde os equipamentos são mais baratos são beneficiados (e.g. China)

Fonte: https://www.blockchain.com/pt/pools (Acessado em 4/7/2019)

COPPE UFRJ

Prova de Trabalho – Consumo Energético Bitcoin

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO



Source: https://powercompare.co.uk/bitcoin/

Prova de Trabalho – Consumo Energético

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Custo médio por transação (Bitcoin): 472 kWh
  - Consumo residencial médio no Brasil: 159,8 kWh/mês (2017)

Tabela 3.53 Consumo médio residencial por região e UF (kWh/mês)

Average residential consumption by region and state (kWh/month)

	2012	2013	2014	2015	2016	Δ% (2016/2015)
Brasil	**158,9**	**163,0**	**167,2**	**161,5**	**159,8**	**-1,0**

Fonte: Anuário Estatístico de Energia Elétrica 2017. Ministério de Minas e Energia. Disponível em http://epe.gov.br/sites-pt/publicacoes-dados-abertos/publicacoes/PublicacoesArquivos/publicacao-160/topico-168/Anuario2017vf.pdf (Acessado em 4/7/2019)

COPPE UFRJ

Prova de Trabalho – Consumo Energético

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Custo médio por transação (Bitcoin): 472 kWh
  - Consumo residencial médio no Brasil: 159,8 kWh/mês (2017)

Tabela 3.53 Consumo médio residencial por região e UF (kWh/mês)

Average residential consumption by region and state (kWh/month)

	2012	2013	2014	2015	2016	Δ% (2016/2015)
Brasil	**158,9**	**163,0**	**167,2**	**161,5**	**159,8**	**-1,0**

A energia gasta em **uma transação** de Bitcoin sustentaria uma residência brasileira por **3 meses**!

COPPE UFRJ

Prova de Trabalho – Consumo Energético

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Custo de minerar 1 Bitcoin por país (em USD)

Fonte: https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/ (Acessado em 4/7/2019)

Prova de Trabalho – Consumo Energético

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

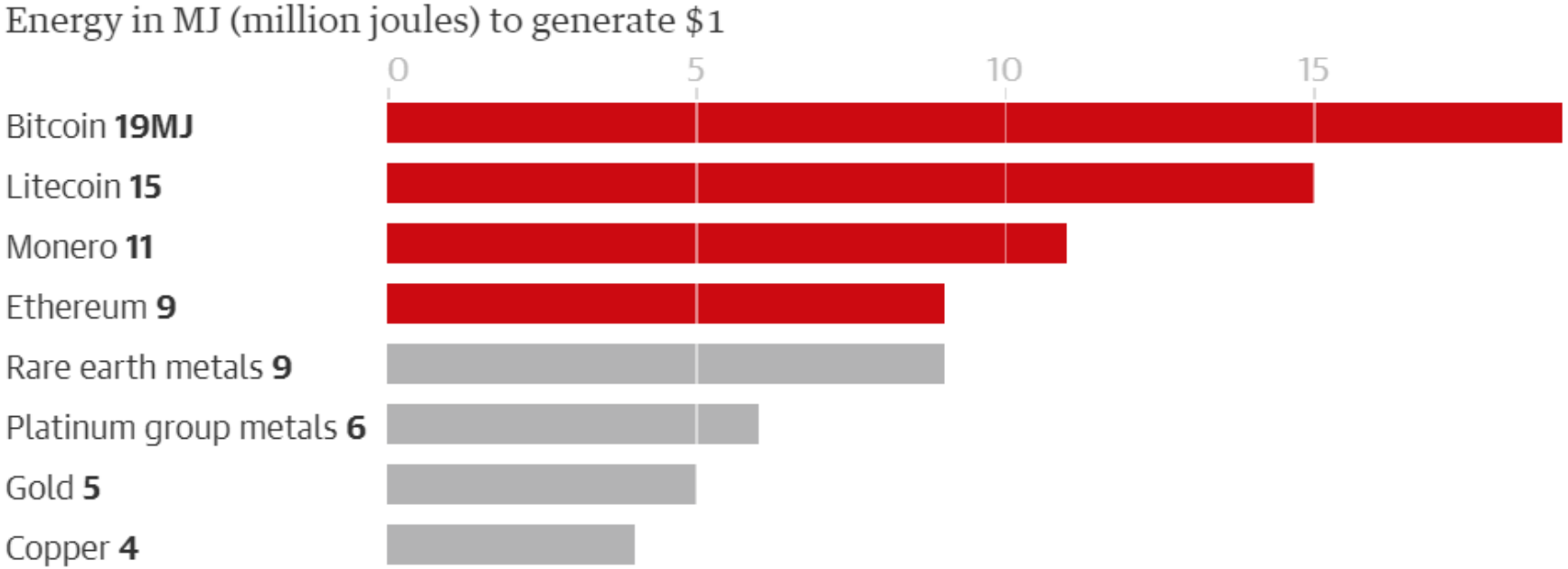
- Custo de minerar 1 Bitcoin por país (em USD)

Fonte: https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/ (Acessado em 4/7/2019)

Prova de Trabalho – Centralização

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Minerar Bitcoin é energeticamente **menos eficiente** do que minerar **ouro**



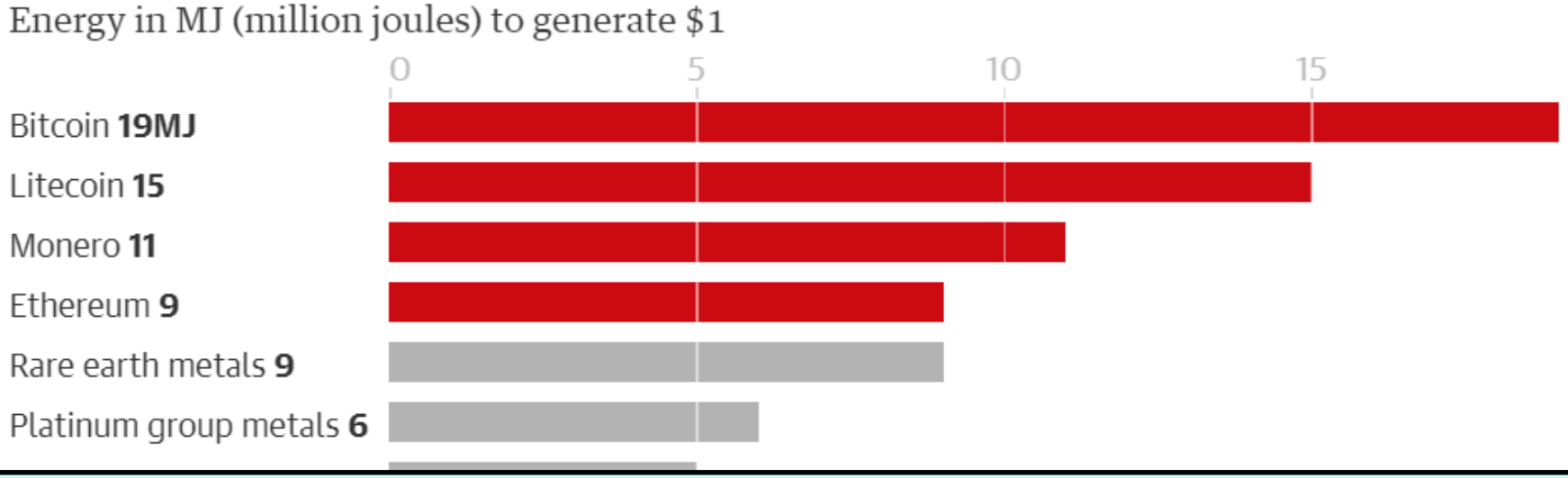
Fonte: https://www.theguardian.com/technology/2018/nov/05/energy-cost-of-mining-bitcoin-more-than-twice-that-of-copper-or-gold (Acessado em 4/7/2019)

COPPE UFRJ

Prova de Trabalho – Centralização

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Minerar Bitcoin é energeticamente **menos eficiente** do que minerar **ouro**



É necessário criar blockchains mais **eficientes**...

COPPE UFRJ

Alternativas ao Bitcoin

- Princípios da blockchain do Bitcoin
  - Qualquer um pode virar minerador e escrever na blockchain
    - Consequência: gasto energético com a prova de trabalho
  - Qualquer um pode ler a blockchain
    - Consequência: falta de privacidade
  - Tipo de ativo: moeda digital
  - Protocolo de consenso: prova de trabalho

- É possível construir blockchains com outras características? Talvez uma blockchain privada em que controlamos as permissões, protocolos, ativos, etc.?

A Iniciativa Hyperledger

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

"O Hyperledger é um esforço colaborativo "open source" criado para promover as tecnologias de blockchain em vários setores. Éuma colaboração global, hospedada pela "The Linux Foundation", incluindo líderes em finanças, Internet das Coisas, cadeias de suprimento, saúde, manufatura e tecnologia. "

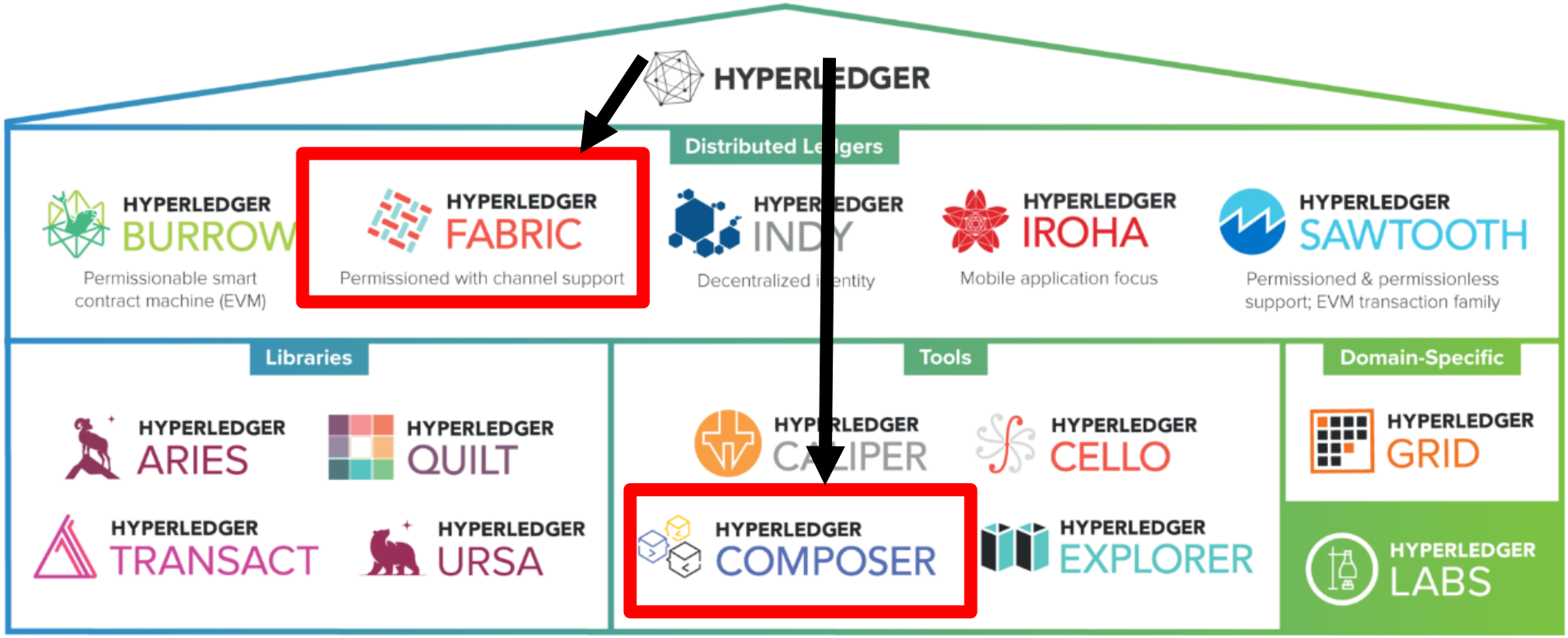
- Fonte: hyperledger.org

COPPE UFRJ

Objetivos do Hyperledger

- Criar estruturas e bases de código de nível corporativo, **código-fonte aberto** e suporte a transações comerciais;
- Fornecer infraestrutura neutra, aberta e orientada pela comunidade, apoiada pela governança técnica e de negócios;
- Construir comunidades técnicas para desenvolver projetos em blockchain e "ledger" compartilhado, casos de uso e implantações;
- Educar o público sobre as oportunidades de mercado para a tecnologia blockchain;
- Promover a comunidade em comunidades que adotam uma abordagem de kit de ferramentas com muitas plataformas e frameworks.

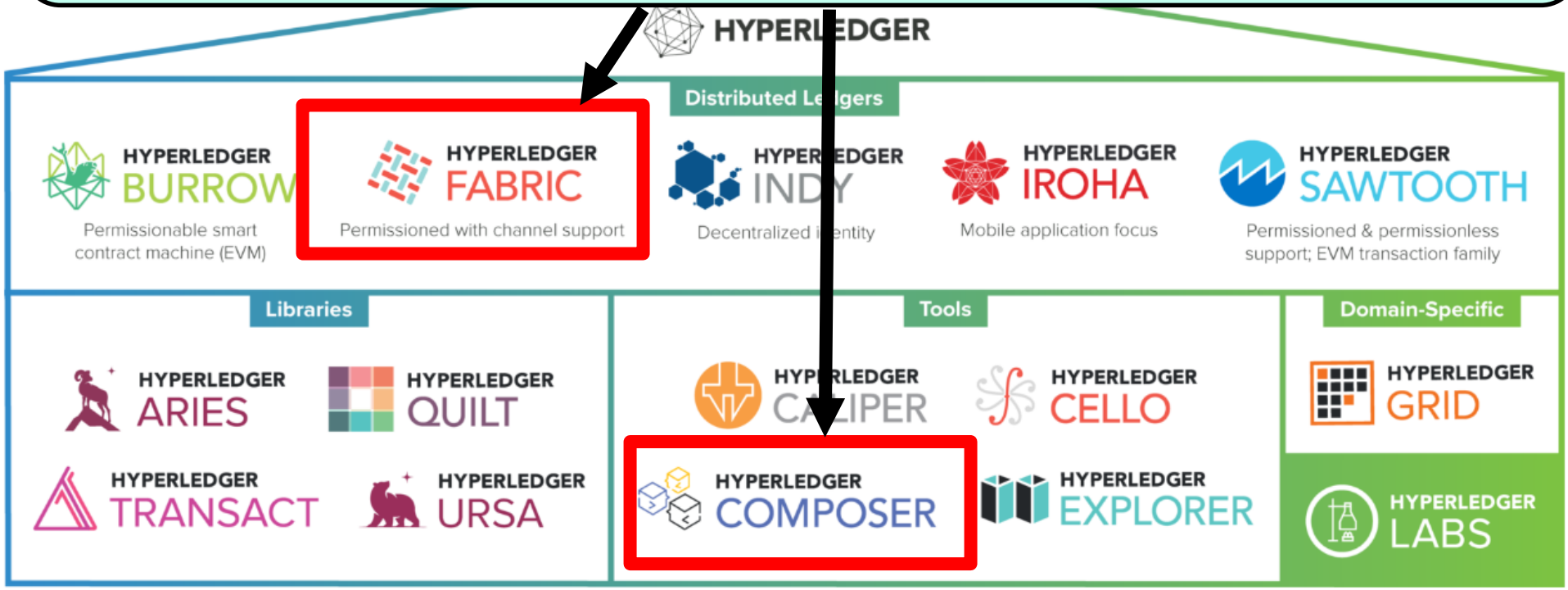
A Iniciativa Hyperledger



A Iniciativa Hyperledger

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Focaremos no **Hyperledger Fabric** e no **Hyperledger Composer**, os mais utilizados em ambientes empresariais



COPPE UFRJ

Hyperledger Fabric

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

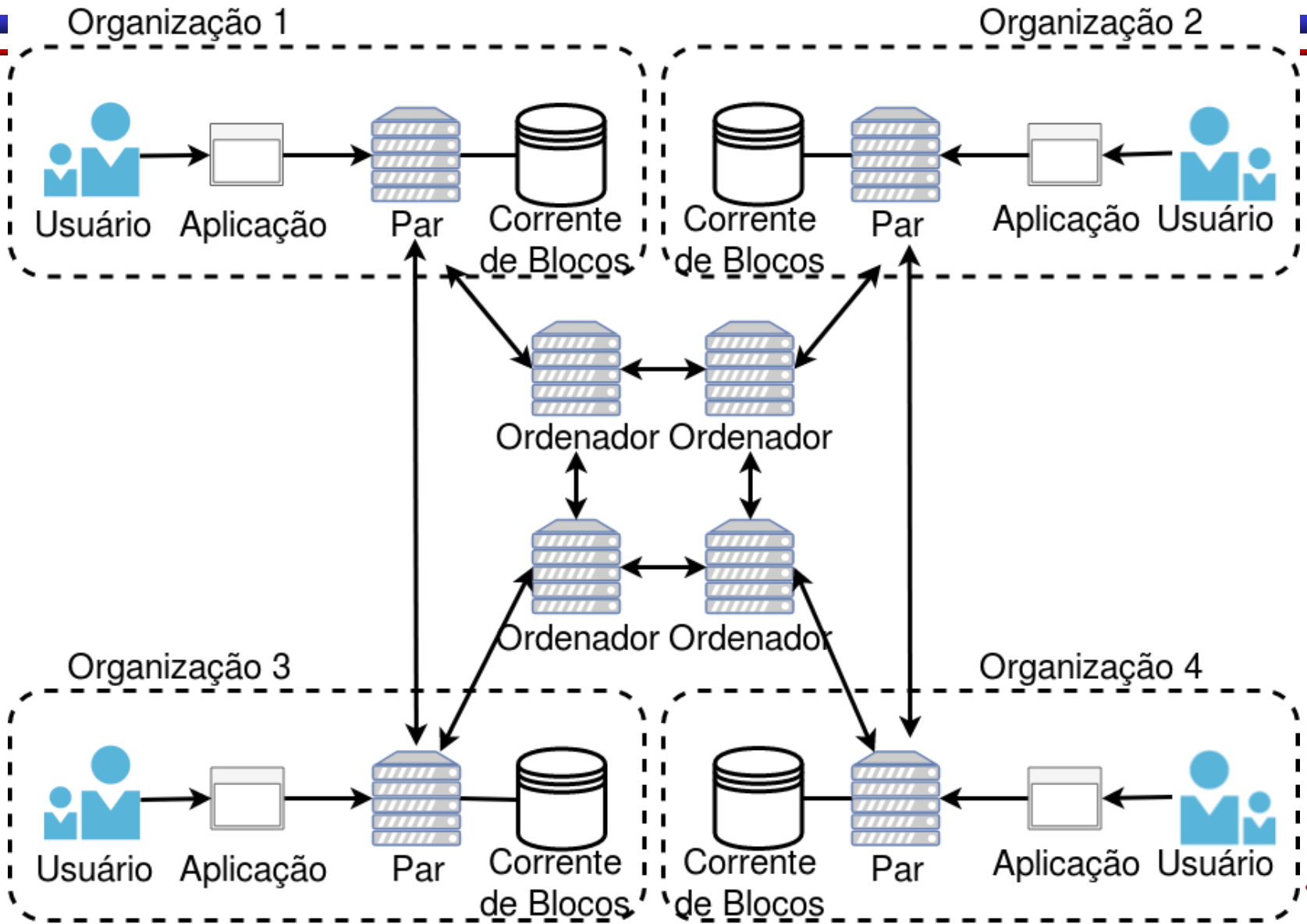
- Iniciativa da Linux Foundation patrocinada pela IBM para desenvolver correntes de blocos privadas

- Arquitetura modular que permite definir
  - Protocolos de consenso
  - Modelo do ativo
  - Estrutura de uma transação
  - Topologia da rede
  - Linguagens de programação para criar contratos inteligentes

HYPERLEDGER

HYPERLEDGER
FABRIC

A Arquitetura do Fabric



Parte III
Aula Prática

Recursos Utilizados

- Para a aula, só será necessário um PC com acesso à Internet
  - Junte com o colega do lado se não tiver!

- Os códigos utilizados estão disponíveis em
  - http://dontpad.com/se2019-blockchain

Parte IV
Conclusão e Perspectivas Futuras

Corrente de Blocos e a Internet

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

COPPE UFRJ 50

Corrente de Blocos e a Internet

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Blockchain proverá a camada de confiança distribuída

COPPE UFRJ

Corrente de Blocos e a Internet

- Blockchain proverá a camada de confiança distribuída
- A Internet do Futuro será a blockchain

Corrente de Blocos e a Internet

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Blockchain proverá a camada de confiança distribuída
- A Internet do Futuro será a blockchain
- A Internet atual de transferência de mensagens e arquivo será substituída pela Internet do Futuro com *blockchain* que será a **Internet de Valores**

COPPE UFRJ

Blockchain:
Hype ou Realidade?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Blockchain é o futuro
- Blockchain proverá confiança distribuída
- Blockchain eliminará intermediários
- Blockchain acabará com os Bancos
- Blockchain eliminará os governos

COPPE UFRJ

Blockchain:
Hype ou Realidade?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Blockchain é o futuro
- Blockchain proverá confiança distribuída
- Blockchain eliminará intermediários
- Blockchain acabará com os Bancos
- Blockchain eliminará os governos
  - Blockchain acabará com a fome
  - Blockchain acabará com a miséria
  - Blockchain acabará com as doenças
  - Blockchain acabará com a dor de dente
  - Blockchain acabará com a TPM

COPPE UFRJ

Desafios de Blockchains

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

- Gastos energéticos com o algoritmo de consenso
- Vazão de transações
- Perda/roubo de chaves privadas
- Governança distribuída
- Internet das Coisas

COPPE UFRJ

Economia compartilhada

- Empresas que se servem de economia compartilhada deixarão de mesmo de existir?
  - AirB&B, Uber, eBAY, MercadoLivre, etc.

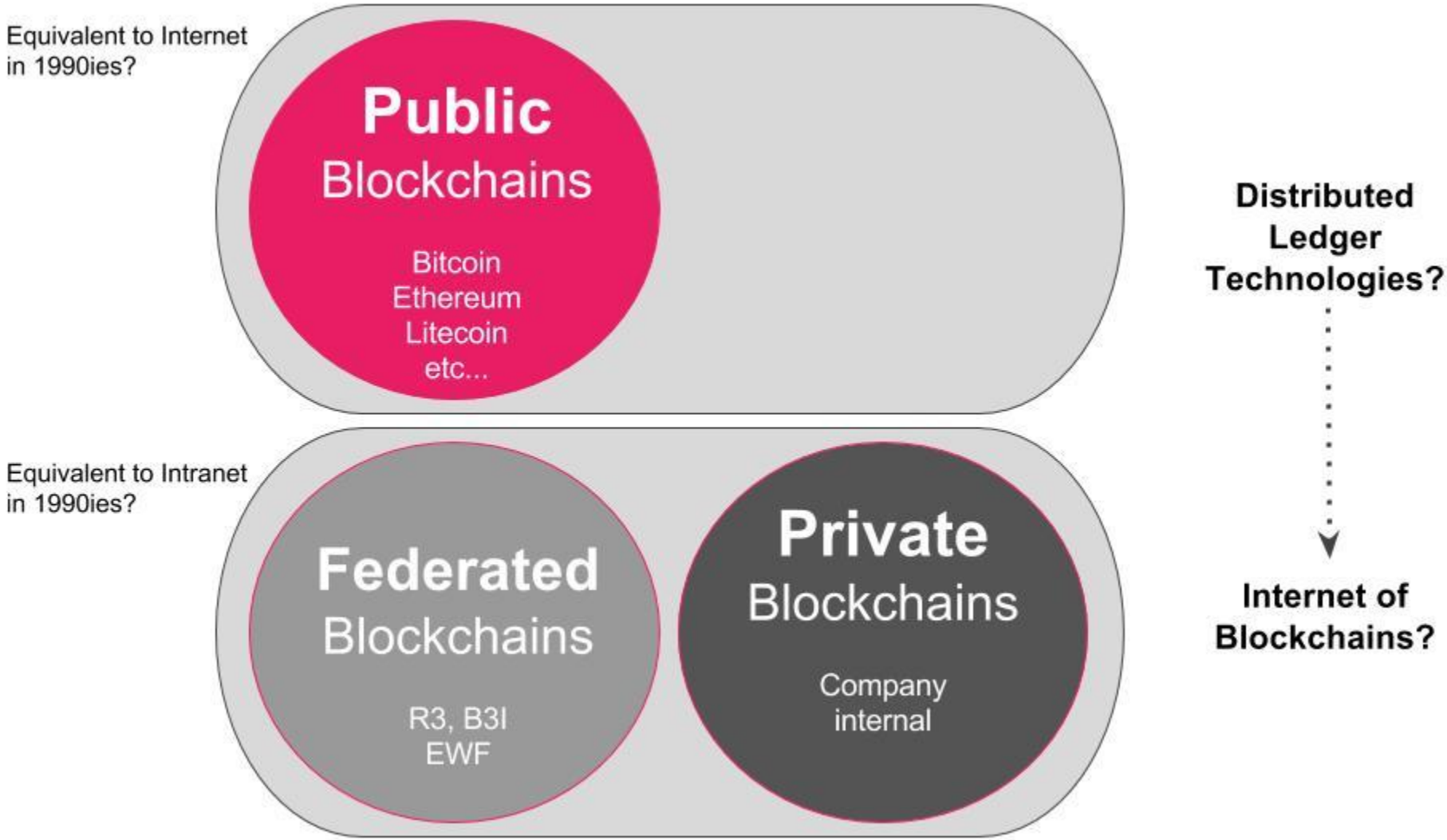
- Haverá pressão de governos e grandes empresas contra as blockchains?

Normatização e legalização

- International Organization for Standartization - ISO)
  - comitê técnico ISO/TC 307 2016
    - formalizar os riscos de segurança, ameaças e vulnerabilidades da tecnologia, além de normalizar a arquitetura de referência, taxonomia, contratos inteligentes e a proteção de privacidade e de informações pessoais.
- Internet Research Task Force (IRTF)
  - criou o grupo de pesquisa da infraestrutura descentralizada da Internet (De-centralized Internet Infrastructure Research Group - DINRG)
    - serviços de infraestrutura beneficiados pela descentralização
- International Telecommunications Union - ITU)
  - Focus Group on Applications of Distributed Ledger Technology - FG DLT)
- Europe Blockchain Working Group
  - Association Trade Communication - ISITC
    - discute a adoção da tecnologia de livro-razão

Internet de Blockchains?

GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO



GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Blockchain:
Das Criptomoedas à Internet do Futuro

Gabriel Antonio F. Rebello

Semana de Eletrônica UFRJ 2019

Grupo de Teleinformática e Automação – GTA/UFRJ
Programa de Engenharia Elétrica - PEE/COPPE/UFRJ
Universidade Federal do Rio de Janeiro

COPPE UFRJ