JAI - 43ª Jornada de Atualização em Informática

44º CSBC 2024

Finanças Descentralizadas em Redes Blockchain: Perspectivas sobre Pesquisa e Inovação em Aplicações, Interoperabilidade e Segurança

Glauber D. Gonçalves

Josué N. Campos

Luis H. S. de Carvalho

INSTITUTO FEDERAL Bahia

Universidade Federal do Piauí

UFV Universidade Federal de Viçosa

ufjf Universidade Federal de Juiz de Fora

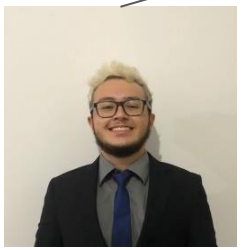
Grupo de pesquisa

Alex Borges
Doutor

Josué Nacif
Doutor

Glauber Dias
Doutor

Allan Freitas
Doutor



Rafael Coelho
Graduando

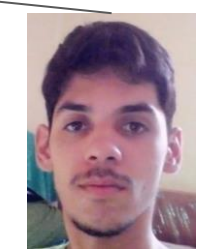
Ronan Dutra
Doutorando

Josué Campos
Mestrando

Luís Carvalho
Mestrando

Ítallo Cardoso
Graduando

Alexandre Fontinele
Pós-doutorando



Isdael Oliveira
Graduando

Grupo de pesquisa

Agradecimento a todas as agências que apoiam o grupo de pesquisa

- CAPES
- CNPQ
- FAPEPI
- FAPEMIG
- FAPESB

Publicações selecionadas para JAI 2024

Mecanismos de Interoperabilidade em Blockchains: Um Comparativo de Custo de Transações Cross-chain para Tokens ERC-20. *WBlockchain - Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (2024)*

Análise de Ataques Sanduíche sob as Transações da Blockchain Ethereum. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (2024)*

Comparação e Análise de Custo e Desempenho entre Nós de Redes Blockchain Permissionadas e Públicas. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (2023)*

Detecção de Vulnerabilidades em Contratos Inteligentes Utilizando Árvore Sintática Abstrata. *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (2023)*

Tokens Não Fungíveis (NFTs): Conceitos, Aplicações e Desafios. *Minicursos do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (2022)*

Aplicações DeFi Inovadoras

Finanças

- Processos de gerenciamento e investimentos
  - Envolvendo dinheiro e ativos financeiros
- Ativos financeiros
  - Bens não físicos que derivam de um contrato entre partes
  - Exemplos: depósitos, ações, títulos de dívidas, empréstimos
- Serviços financeiros
  - Bancos, financeiras, seguradoras, fundos
- Mercado financeiro
  - Local (físico ou virtual) para negociar ativos

Finanças Centralizadas (CeFi)

- Serviços financeiros tradicionais
  - Bancos, financeiras, corretoras e fundos
- Custodia os ativos de seus usuários (podem congelar contas ☹)
- Servem como intermediários em transações financeiras
  - Pedir emprestado e emprestar considerando juros e tarifas

- Aderentes a regulações de governos (CVM e BC)
  - Impedir fraudes e lavagem de dinheiro
  - Necessita conhecer a identidade dos usuários (sem privacidade ao serviço)
- Aplicações e bancos de dados com governança centralizada
  - Necessita da confiança dos usuários

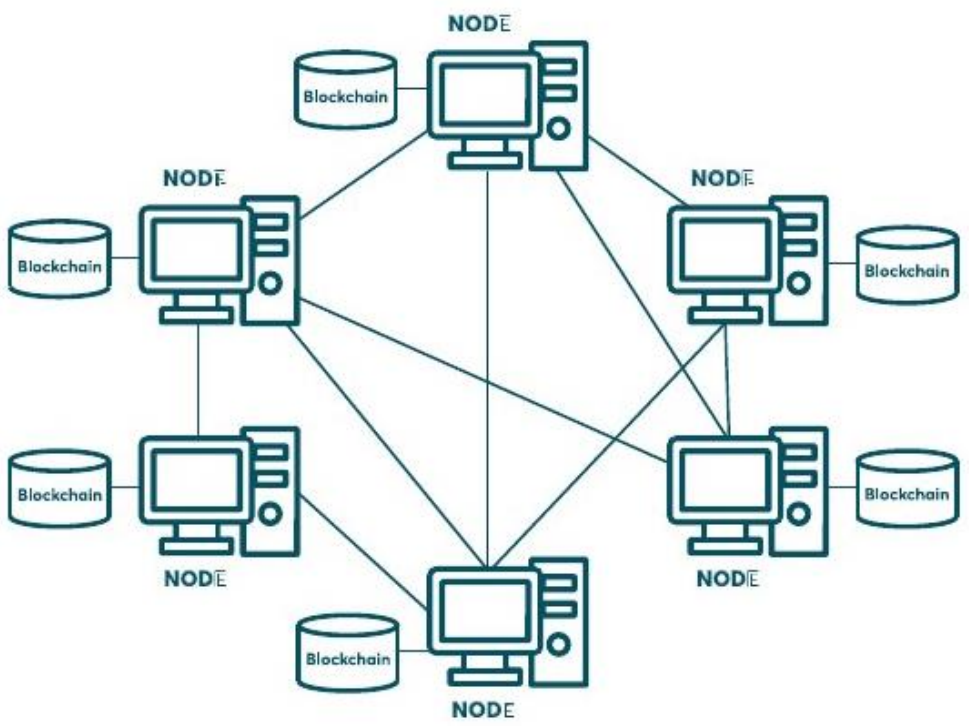
Finanças Descentralizadas (DeFi)

- Serviços financeiros eletrônicos baseados em redes par-a-par
  - Sistema com governança descentralizada entre participantes da rede
  - Não há restrições para participar do sistema
  - Sistema precisa ser a prova de participantes não confiáveis

- Blockchain é a tecnologia base para DeFi
  - Concebida originalmente para o sistema de dinheiro eletrônico Bitcoin
    - Bitcoin a Peer-to-Peer Eletronic Cash System (Satoshi Nakamoto, 2008) www.bitcoin.org
  - Permite processar e armazenar dados de forma distribuída
    - Sem delegar o controle a uma autoridade central
    - Mesmo na existência de alguma parte não-confiável

Sistema Descentralizado

- Rede de computadores participantes (pares distribuída via rede par-a-par (P2P)
- Banco de dados de transações **(blockchain)** replicado em cada par



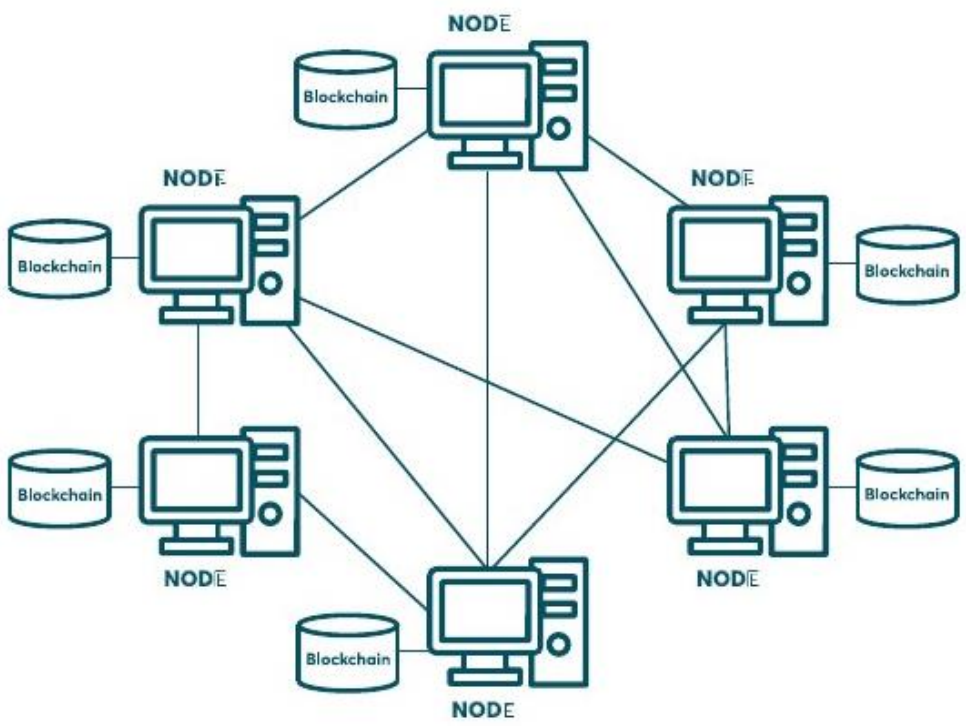
Cada par da rede segue o protocolo distribuído:

- pode se eleger (eleição!) para gerar o próximo bloco
  - O líder recebe remuneração pelo esforço na moeda da rede
- se não é líder, recebe novo bloco e o encadeia
  - processa as transações do bloco
  - atualiza variáveis que dependem de transações (e.g., saldo)

Hackear o protocolo requer uma maioria de pares desonestos coordenados (*conluio*)

Sistema Descentralizado

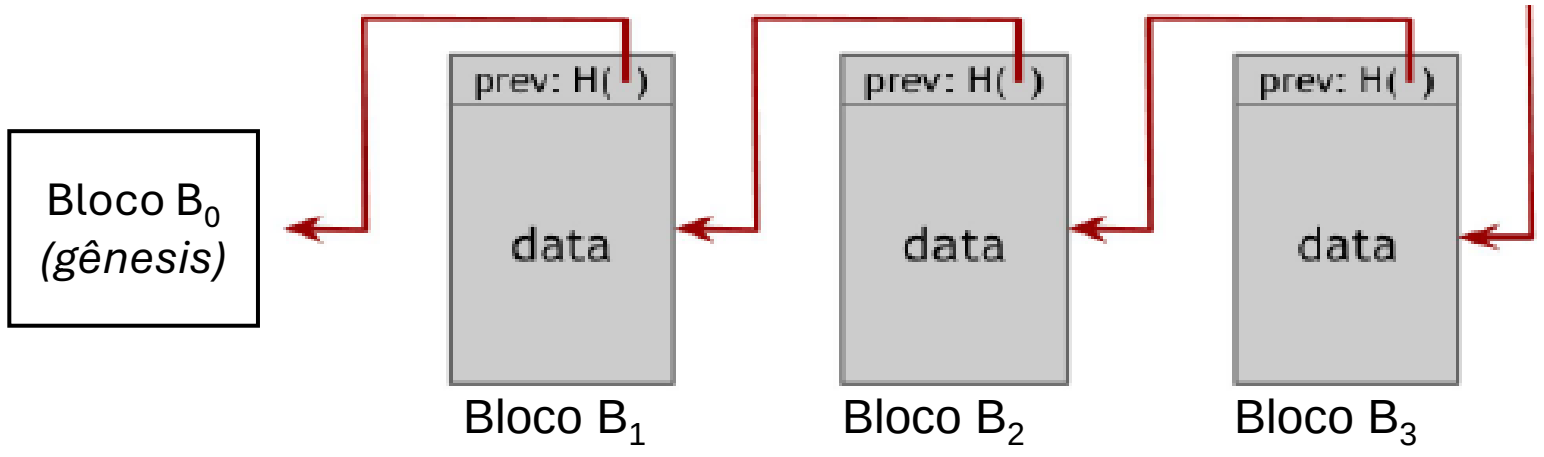
- Rede de computadores participantes (pares distribuída via rede par-a-par (P2P)
- Banco de dados de transações **(blockchain)** replicado em cada par



- Modelo de consistência das réplicas (blockchain) nos pares
  - Geralmente menos restrito ou eventual
  - Deve ser resiliente e convergir para estados consistentes em cada par se observar um bloco X

Estrutura de Dados de uma Blockchain

- Transações são organizadas em blocos
- O cabeçalho do bloco contém as informações relevantes
- Blocos são encadeados por *hash* no cabeçalho (blockchain)
  - *Modificação em B_i invalida todos os dados a partir de B_{i+1}*



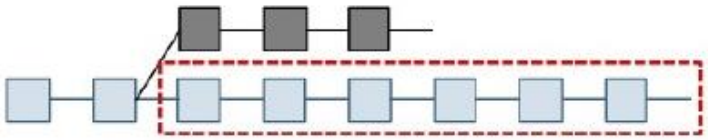
Quanto mais longa a cadeia

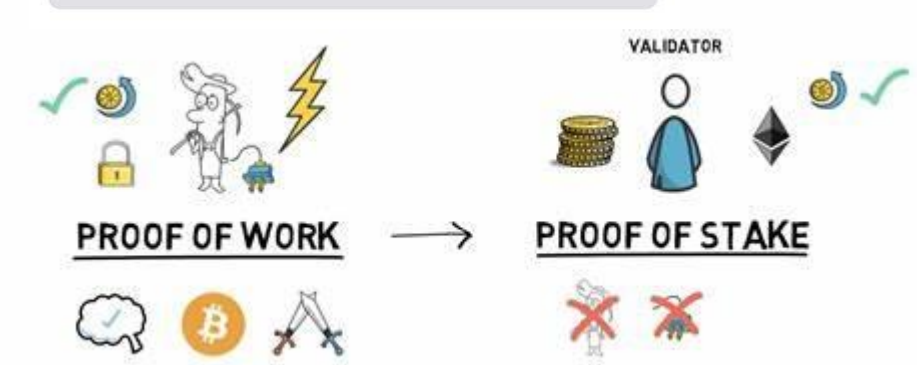
maior a imutabilidade dos blocos antigos...

ou maior o esforço para modificar um bloco antigo com consistência

Protocolo de Consenso Distribuído

- Eleição de um líder para incluir o próximo bloco na blockchain
  - Deve seguir regras (protocolo) acordado entre os participantes
    - O líder recebe uma recompensa pelo bloco validado





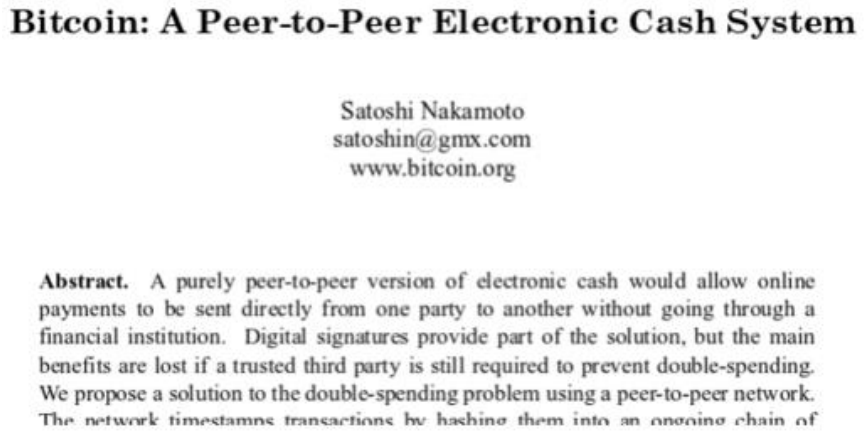
Mais sobre fundamentos blockchain

- Greve, Fabíola Greve et al. Blockchain e a Revolução do Consenso sob Demanda. Minicursos SBRC, 2018.

Referências Clássicas:

- Buterin, Vitalik et al. A next-generation smart contract and decentralized application platform. White Paper, v. 3, n. 37, 2014. https://ethereum.org/en/whitepaper
- NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, p. 21260, 2008. https://www.debr.io/

Marcos fundamentais de DeFi



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

Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
By Vitalik Buterin (2014).

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price.

2008

2014

custódia do dinheiro
pelo próprio usuário

dinheiro e ativos eletrônicos
programáveis

Aplicações Descentralizadas (DApps)

- Aplicação ou serviço baseado (registrado) em uma blockchain
  - Um ou mais ***contratos inteligentes***: programa completo (código/bytecode)

```
1   contract C {
2       bool truth = false;
3       function get() public view returns(bool) {
4           return truth; }
5       function set(bool value) public {
6           truth = value; }
7   }
```

1 – Smart Contract *C*.

Créditos: Lucas Palma (Candidato a Doutorado PPGCC-UFSC)

Aplicações Descentralizadas (DApps)

- Estados de um DApp registrados na blockchain

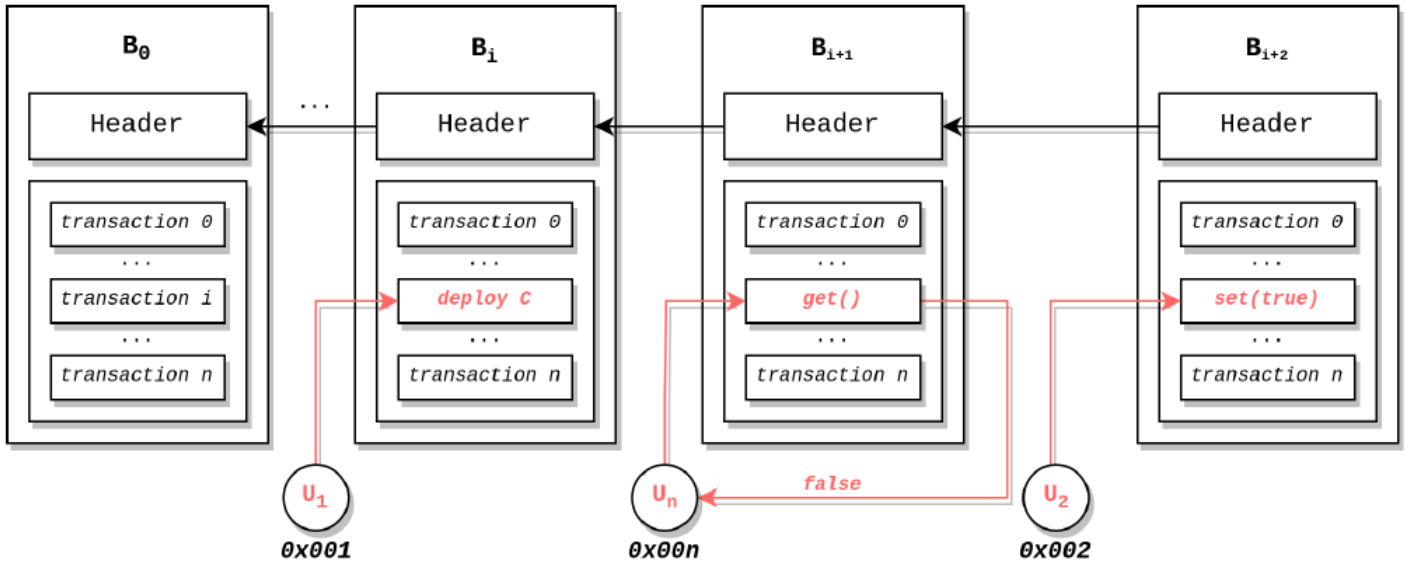


Figure 5 – Smart Contract *C* states.

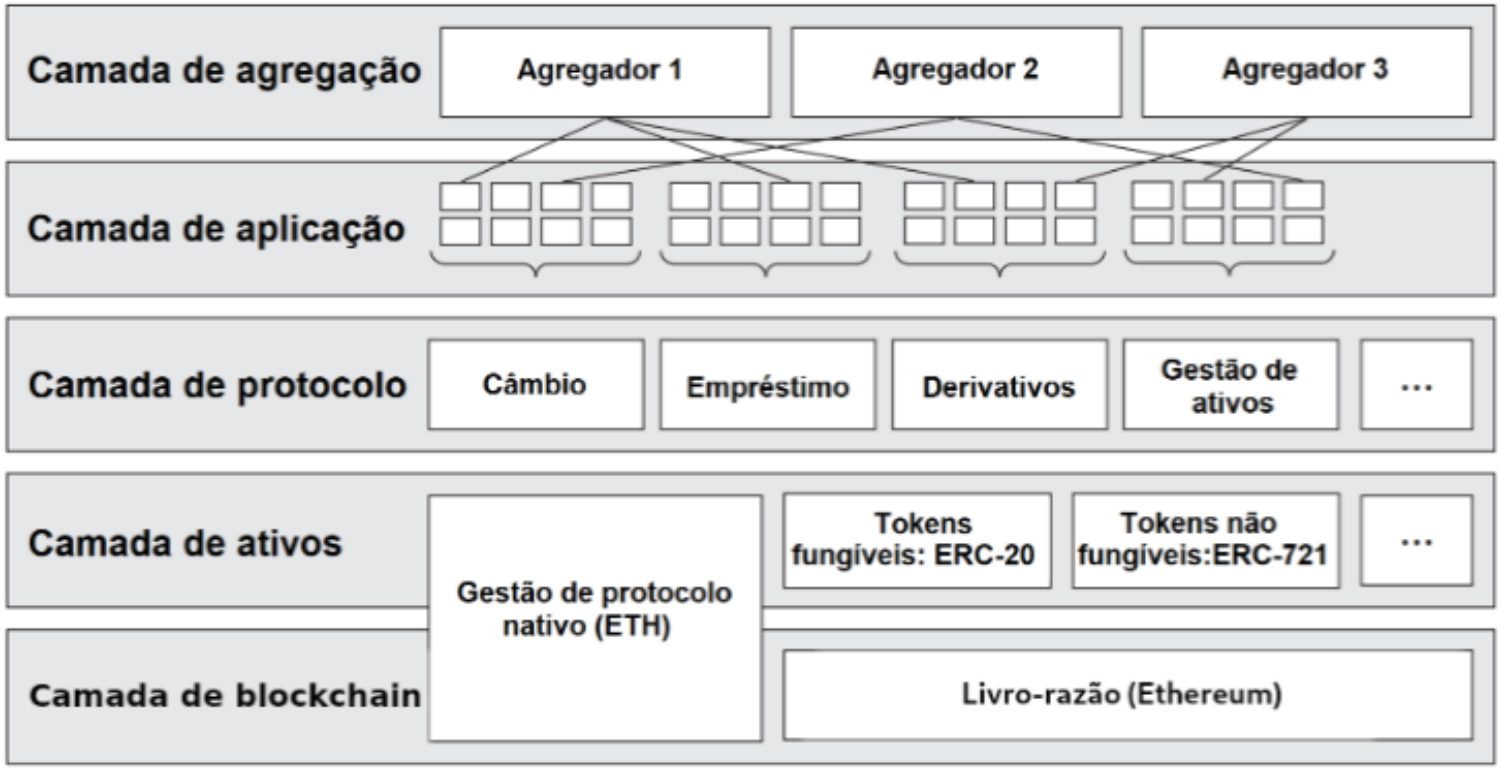
Créditos: Lucas Palma (Candidato a Doutorado PPGCC-UFSC)

Vantagens de DeFi via DApps

- Remove intermediários em contratos de transações financeiras
- Acessibilidade universal (não há restrições de participantes)
- Transparência e verificabilidade pública
  - Inspeção do código do contrato inteligente
  - Verificação da execução e do estado do sistema
- Automação e programabilidade
- Simplicidade e rapidez para desenvolver serviços financeiros
  - Exemplos de inovação: *Uniswap*, *flash-loan*

Arquitetura DeFi

- Cinco camadas hierárquicas usualmente adotadas por DApps DeFi



Adaptado de Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review

Interfaces multi aplicações
Exemplo: carteiras, APIs

Interfaces de usuários para acessar serviços. Ex: App clientes

Serviços financeiros implentados em Contratos inteligentes

Tipos (padrões) de ativos financeiros

Transações em registro consistente e imutável

Principais Blocos de Construção DeFi

- (I) Tipos de ativos
  - Tokens fungíveis
  - Tokens não fungíveis
  - Stablecoin
- (II) Corretoras descentralizadas
  - Livro de ordens
  - Criadores de mercado

- (III) Outros: oráculos, mantenedores, pontes [serviços off-chain]

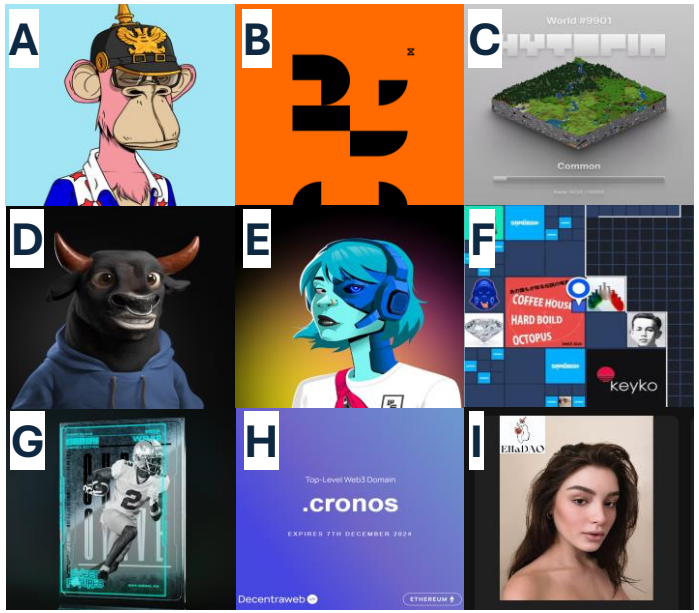
"Tokenização" de ativos

- *Token*
  - Uma representação de um ativo em blockchain
- *Tokenização*
  - Processo de acrescentar novos tokens para uma blockchain
- Motivação para *tokenizar*
  - Tornar um ativo mais acessível
  - Fácil de transferir
  - Programável

Tokens Não Fungíveis (NFT)

- Um objeto digital com atributos únicos
  - Registrado em blockchain garante autenticidade e propriedade

- Casos de uso
  - Obras de arte digitais
  - Itens de jogos,
  - Música
  - Fotografia
  - Todo criatividade humana ...
  - Veja mais em https://opensea.io



Exemplos de NFT por Categoria da OpenSea: PFPS (a), ART (b), GAMMING (c), MEMBERSHIPS (d), MUSIC (e), VIRTUAL-WORLDS (f), SPORTS-COLLECTIBLES (g), DOMAIN NAMES (h), PHOTOGRAPHY (i)

Tokens Não Fungíveis (NFT)

- O tipo NFT geralmente usa o padrão ERC 721

- Oferece as interfaces para objetos colecionáveis
  - Exemplos
    - Transferência de propriedade
    - Royalty por venda ao criador original

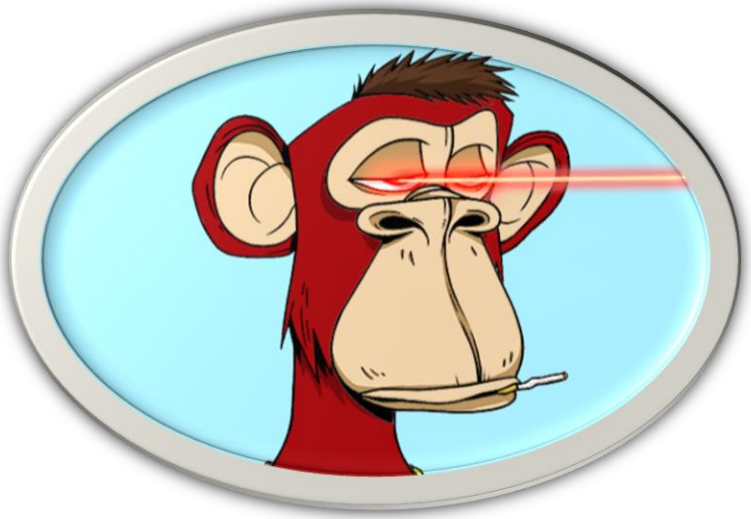
- Um contrato inteligente é uma coleção de NFTs (geralmente)
  - Cada NFT associado ao contrato possui metadados específicos
    - Características visuais (*traits*), valor, proprietário, royalty e etc

Non-fungible tokens (NFT)

- Artes digitais, marketing, imagens, músicas
  - Autenticidade, raridade, tipo de mídia (Arte digital, memes, músicas, etc.)

A animação “Nyan Cat” foi leiloada em NFT por US$ 500 mil

O presidente do Twitter, Jack Dorsey, vendeu seu primeiro tuíte por US$ 2,9 milhões



Neymar desembolsa R$ 6 milhões e entra no mundo dos NFTs

Tokens Não Fungíveis (NFT)

- Esse é o seu primeiro NFT?
  - Faça sua carteira Metamask
  - Nos envie o identificador de sua conta
  - Receba esse NFT *raríssimo gratuitamente*

Tokens Fungíveis

- Foi o primeiro padrão de token concebido
  - Conhecido como o padrão ERC 20

- Oferece as interfaces para comercialização geral de ativos
  - Exemplos
    - Transferência de propriedade
    - Unidade relativa ao token nativo (exemplo token X vale 0.01 ETH)
    - Quantidade total de emissão do token (*total supply*)
    - Permissão para outro usuário gerenciar o token (*approval*)
    - Emissão de novo token (*mint*) permitido apenas ao dono do contrato
    - Queima do token (*burn*) permitido apenas ao dono do token

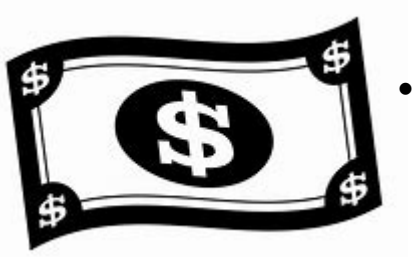
Tokens Fungíveis

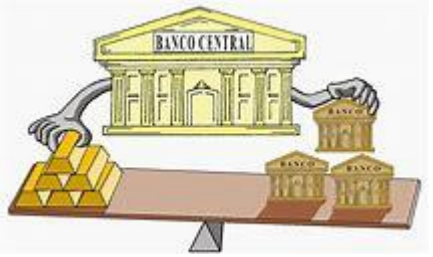
- Categorias usuais de tokens fungíveis são:
  - Tokens de utilidade: permite acessos exclusivos a serviços *on/off chain* aos seus proprietários oferecidos pela organização emissora
  - Tokens de segurança: representam ativos financeiros do mundo real, já regulamentado em alguns países como Malásia e Georgia
  - Tokens de governança: permitem aos proprietários votar em decisões de organizações, e.g., DAOs (decentralized autonomous organizations)

Stablecoins

- Recurso para lidar com a volatilidade tokens nativos
  - Por conseguinte todos os tokens fungíveis e não fungíveis associados

- Utiliza um conceito comum em CeFi: lastro de moedas e ativos
    - Lastro é uma equivalência de um ativo a um bem físico (preferível) ou outro ativo
  - Exemplos
    - O real (BRL) é lastreado ao dólar
      - Banco central do Brasil não pode emitir BRL sem ter valores em dólar equivalentes!
    - O dólar (USD) é lastreado ao produto interno bruto do USA atualmente
      - O dólar (USD) foi lastreado ao ouro até 1970
    - O Banco central USD não pode emitir USD se a economia não crescer!





Stablecoins

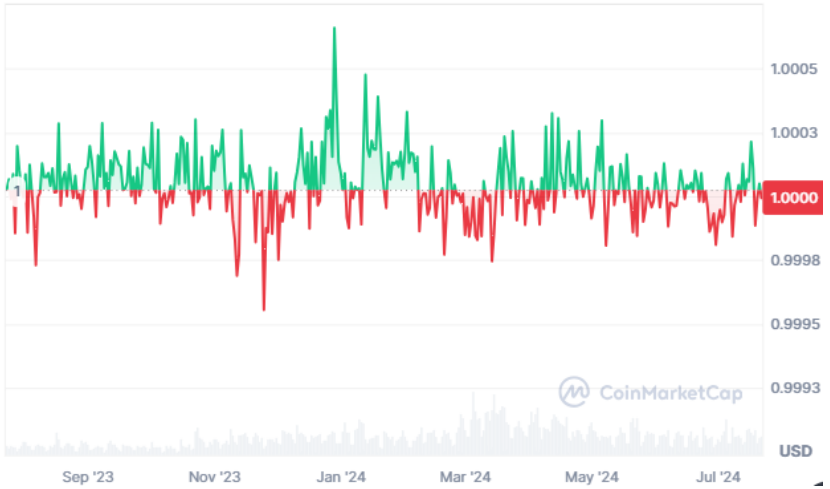
- Implementados via token ERC 20
  - Ideia para manter relação 1:1 do lastro (lei de mercado)
    - Se o valor da stablecoin sobe então vende para trocar pela moeda fiduciária.
    - Se o valor cai então usuários passam a comprar a stablecoin causando sua escassez, e alta no preço voltando novamente a paridade

- Principais categorias
  - Stablecoin *off-chain*: lastreado a um fundo de moeda CeFi
    - Exemplos: Tether (USDT), Coinbase stablecoin (USDC) lastreado a 1 USD
  - Stablecoin *on-chain*: lastreado a um fundo de moeda DeFi
    - Exemplo: DAI lastreado a 1 USD baseado em ETH

Stablecoins

- Variação no valor do stablecoin no último ano

USDT



USDC

DAI

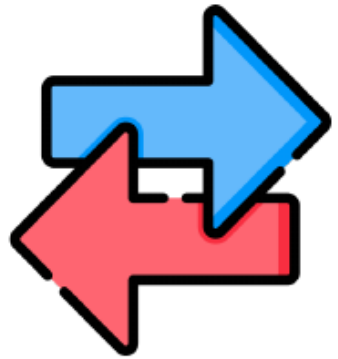
- Note que o eixo *y* central é USD 1.00
  - Missão das stablecoins é desafiante, mas conduzida razoavelmente bem!

Corretoras Descentralizadas

- Mercado financeiro para negociar diferentes tipos de ativos

- Corretora centralizada (CEX) é o modelo tradicional
  - Exemplos: Coinbase, Binance, Mercado Bitcoin e etc
  - Pouca transparência (terceiro confiável) e propensa a falhas
    - Custodia ativos dos usuários, mas pode haver corrupção e roubo de senhas/chaves

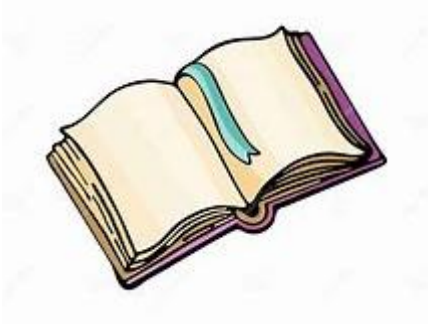
- Corretora descentralizada (DEX) – *descentralized Exchange*
  - Exemplos: Uniswap, DyDx, Sushiswap
  - Visa tratar os problemas de CEX
    - Sem custódia: usuários não transferem ativos para a corretora
    - Transparência: trocas automatizadas via DApps



Corretoras Descentralizadas

- Principais protocolos em corretoras descentralizadas
  - Livro de ordem
  - Criadores de mercado automatizados (*AMM - Automated Marked Maker*)

Livro de ordem (DEXes)



- Registro digital de ordens de compra e venda de um ativo
  - Usuários cadastram intenções de compra ou venda e seu valor
    - Valor máximo e mínimo que deseja pagar ou comprar
  - A transação é realizada quando uma ordem de compra corresponde a uma ordem de venda
  - Nos exemplos abaixo ordens #1 e #3 se correspondem:
    - #1, compra, x, 0.121, 0.133
    - #2, vende, y, 0.131, 0.133
    - #3, vende, x, 0.111, 0.122

Desvantagem: tarifa da rede para cada ordem! Melhor offline?

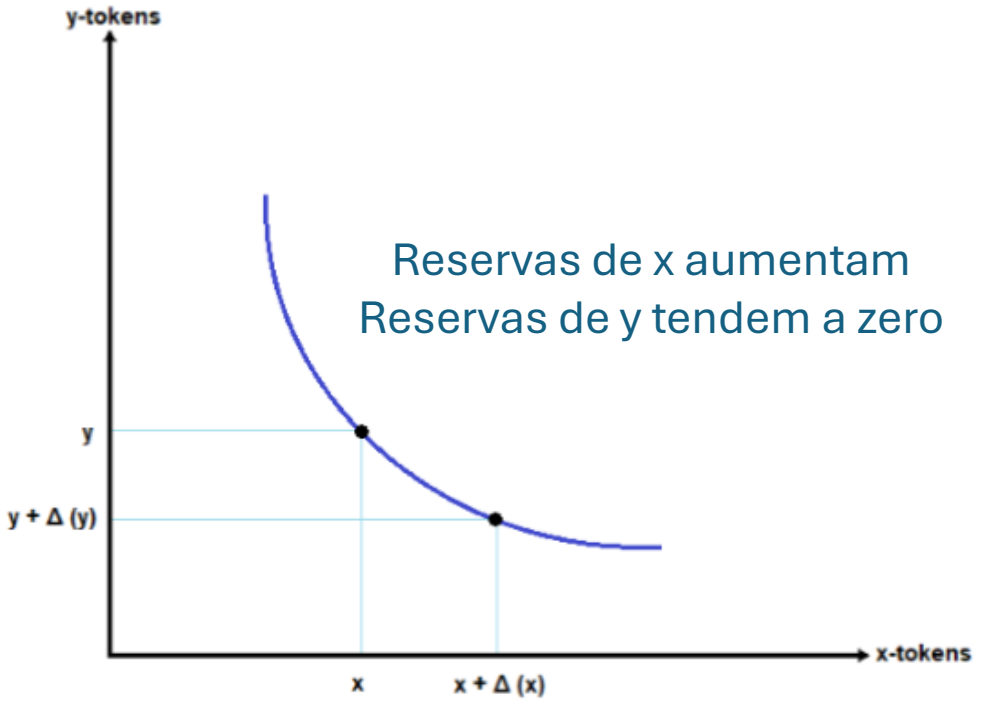
Criadores de mercado automatizados (AMM)

- Modelo matemático para determinar os preços dos ativos
  - Modelos simples funcionam! Exemplo Uniswap
- Contratos controlados pela AMM pagam recompensas por depósitos recebidos de usuários (*pools* de liquidez)
- Cada tipo de ativo negociado tem seu pool de liquidez
- Pares de ativos são correspondentes a uma taxa contante
    - *Constant Function Market Maker (CFMM)*
  - Exemplo: $xy = k$, *reservas* dos ativos x e y tem equivalência constante k

Criadores de mercado automatizados (AMM)

- Exemplo de CFMM $xy=k$
  - trocas entre x e y *precisam manter a relação*
  - Aumentar Δx *tokens* implica em aumentar Δy *tokens, logo:*
    - $(x+\Delta x)\,(y+\Delta y) = k$
    - $\Delta y = k / (x+\Delta x) - y$
    - Δy é negativo
    - significa queda nas reservas y

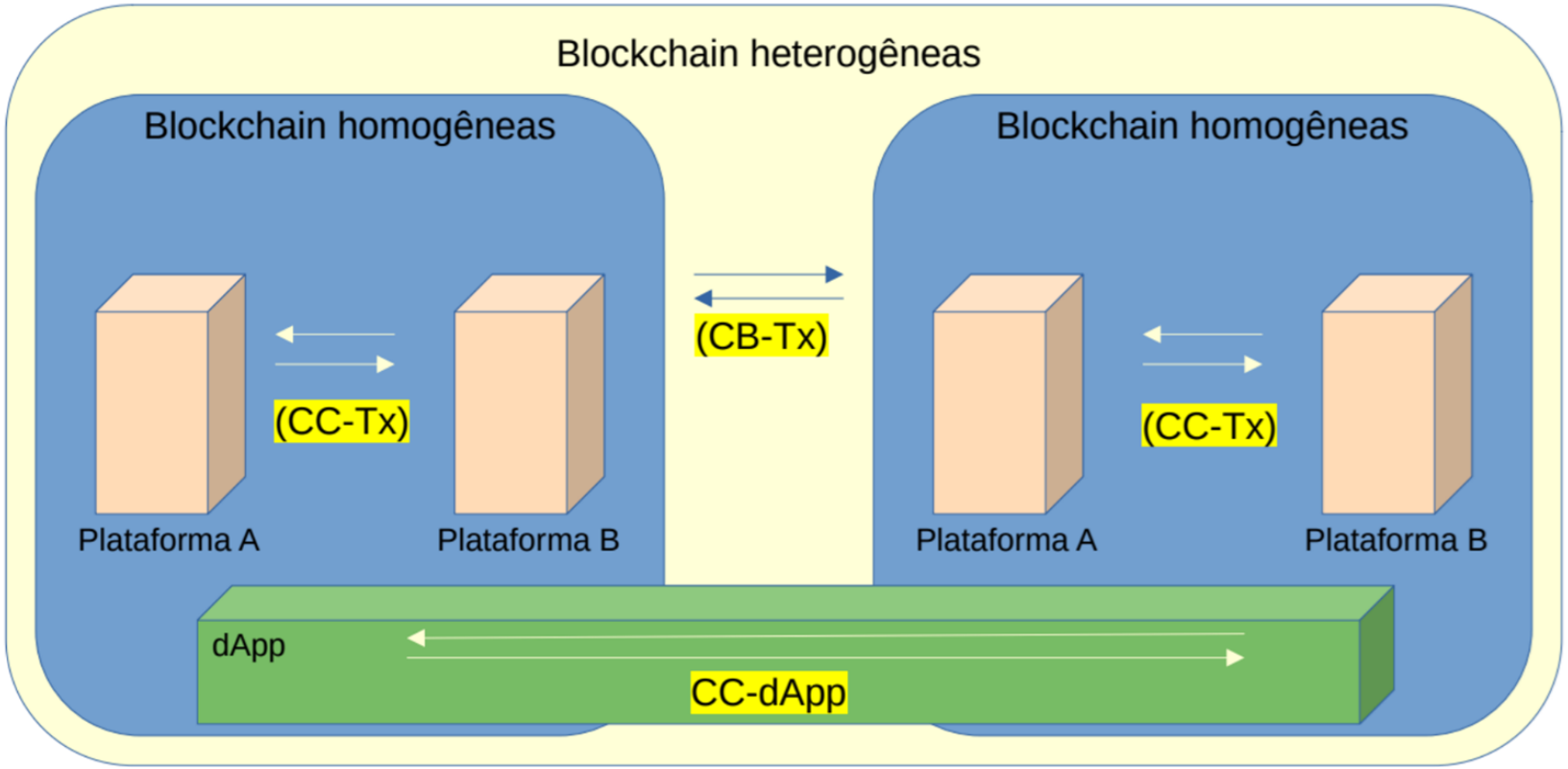
Conforme a reserva do token de se aproxima de zero o seu valor aumenta no pool de liquidez visando sua reposição



Interoperabilidade

Interoperabilidade

- Blockchains distintas → Sistemas heterogêneos → Dificuldade de trocas de informações
- Ecossistema DeFi demanda que tokens funcionem em redes blockchains diferentes

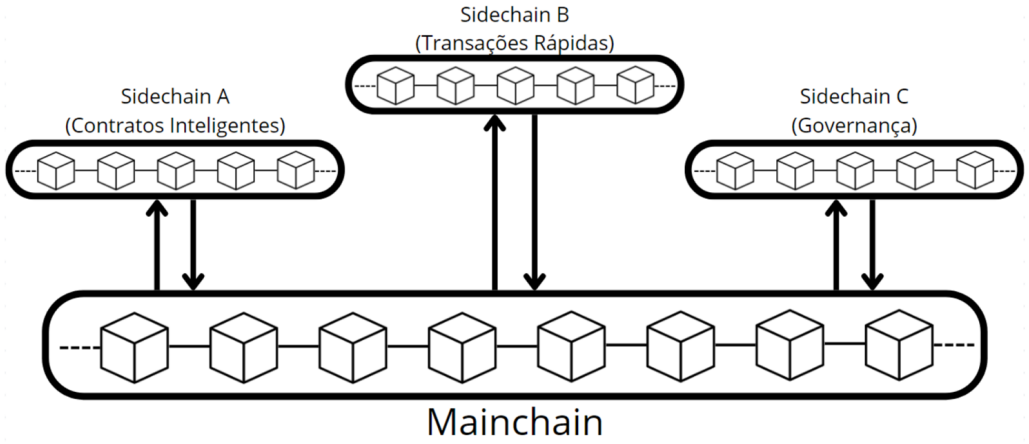


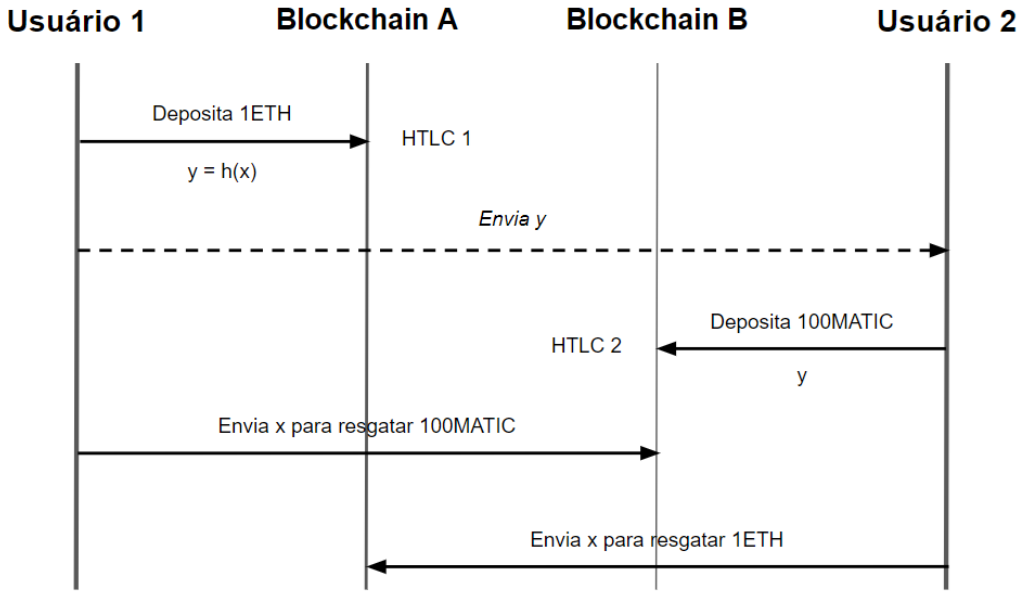
Interoperabilidade: Vantagens

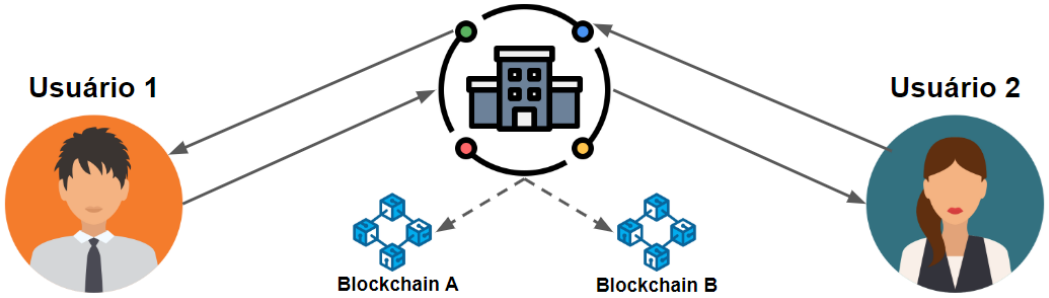
- **Usabilidade**
- Troca de ativos digitais entre cadeias
- Conduzir transações em diferentes redes
- Troca de informações sobre operações executadas em uma cadeia
    - Compartilhamento do histórico de transações de um determinado item

Mecanismos de Interoperabilidade

- Sidechains
- *Hash Time-Lock Contract* (HTLC)
- Mecanismo Notarial

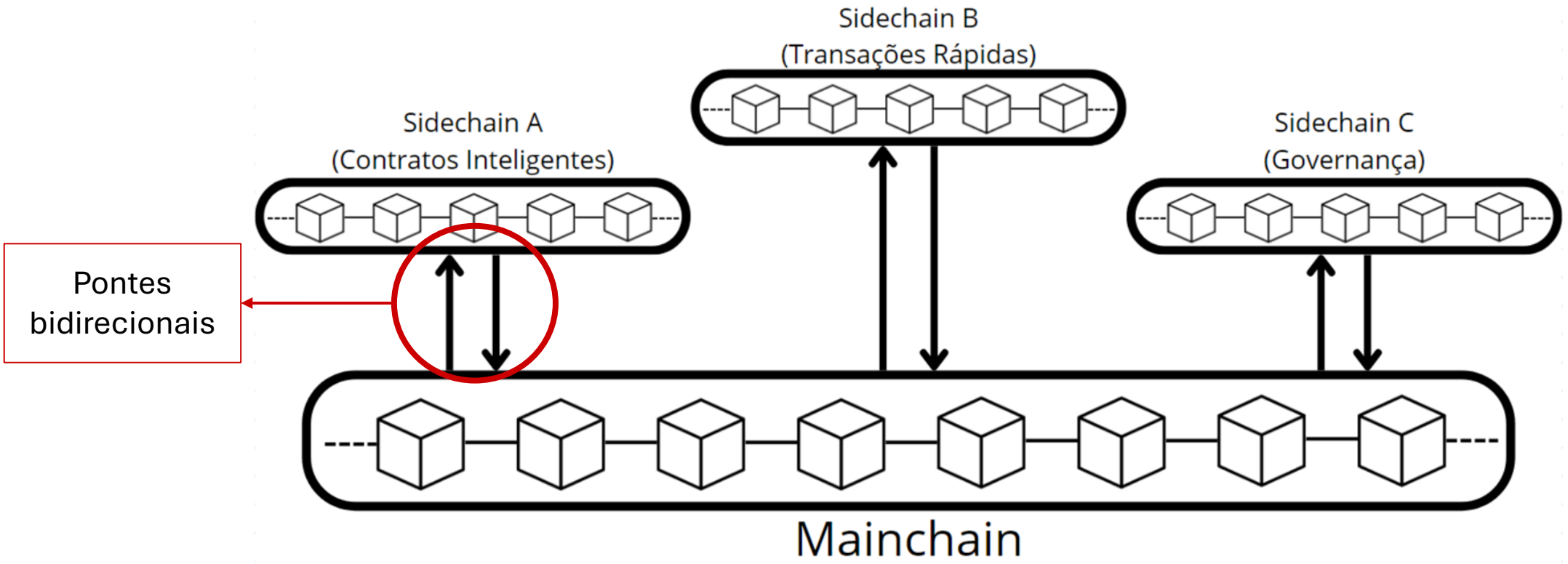






Sidechains

- Blockchains independentes que operam em paralelo à blockchain principal (*mainchain*)
- **Funcionalidade principal:** Eliminar a sobrecarga da blockchain principal e implementar novas funcionalidades

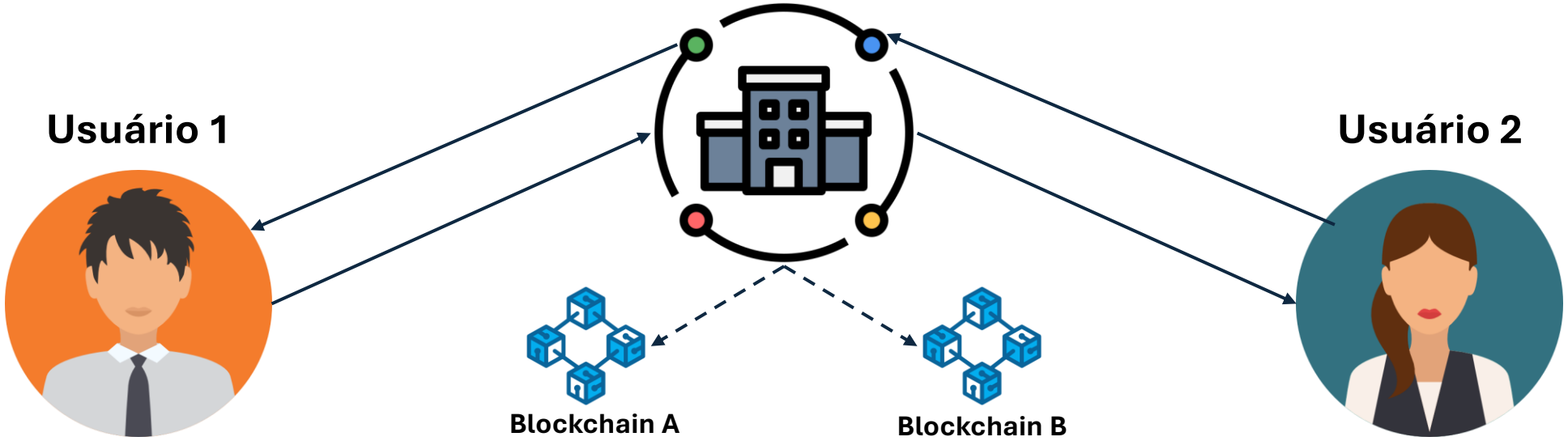


Mecanismo Notarial

- Mecanismo que consiste em verificar e encaminhar mensagens entre cadeias por meio de uma entidade confiável intermediária chamada de **notário**
- Uma ou mais organizações podem ser designadas como notário para monitorar eventos entre as cadeias
- Nas redes blockchains: **notário = contratos inteligentes**
- Mecanismo notarial de assinatura única
- Mecanismo notarial de múltiplas assinaturas

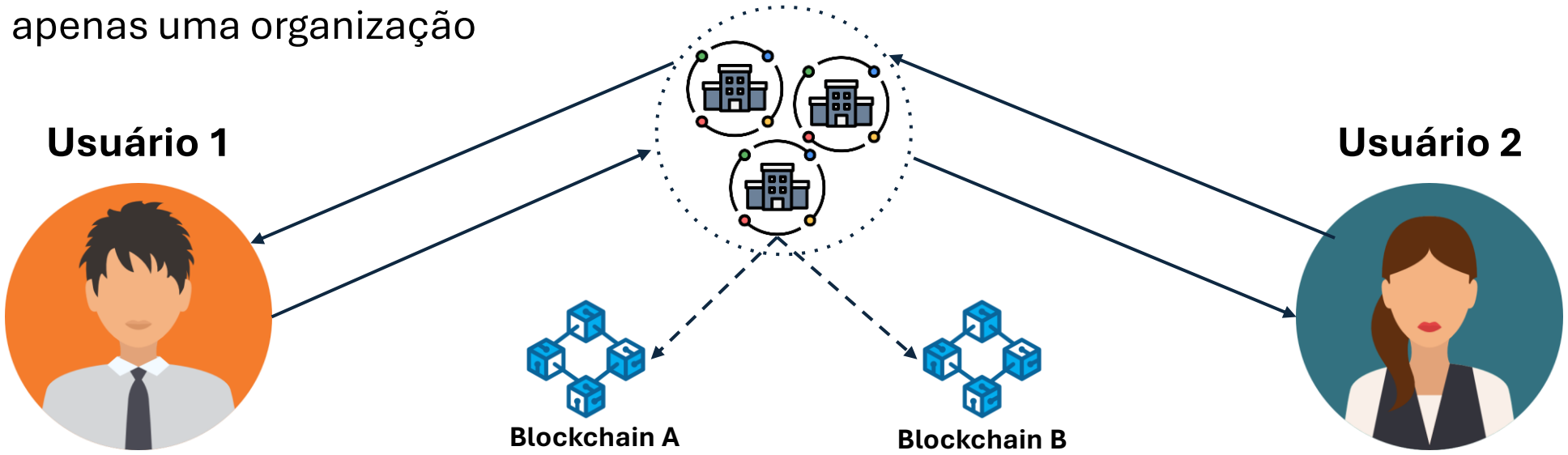
Mecanismo Notarial: Assinatura única

- Também chamado de **mecanismo notarial centralizado**
- Uma **única organização** independente atua como o notário
- Processamento rápido de transações
- Pode apresentar riscos por ser um único ponto de falha



Mecanismo Notarial: Múltiplas assinaturas

- Um notário é composto por um **grupo de organizações**
- Somente quando uma determinada porcentagem destas organizações assinam em conjunto é que há um consenso e **as transações entre cadeias podem ser confirmadas**
- **Notários são selecionados aleatoriamente** do grupo, diminuindo a dependência em confiar em apenas uma organização



Mecanismo Notarial: Exemplo

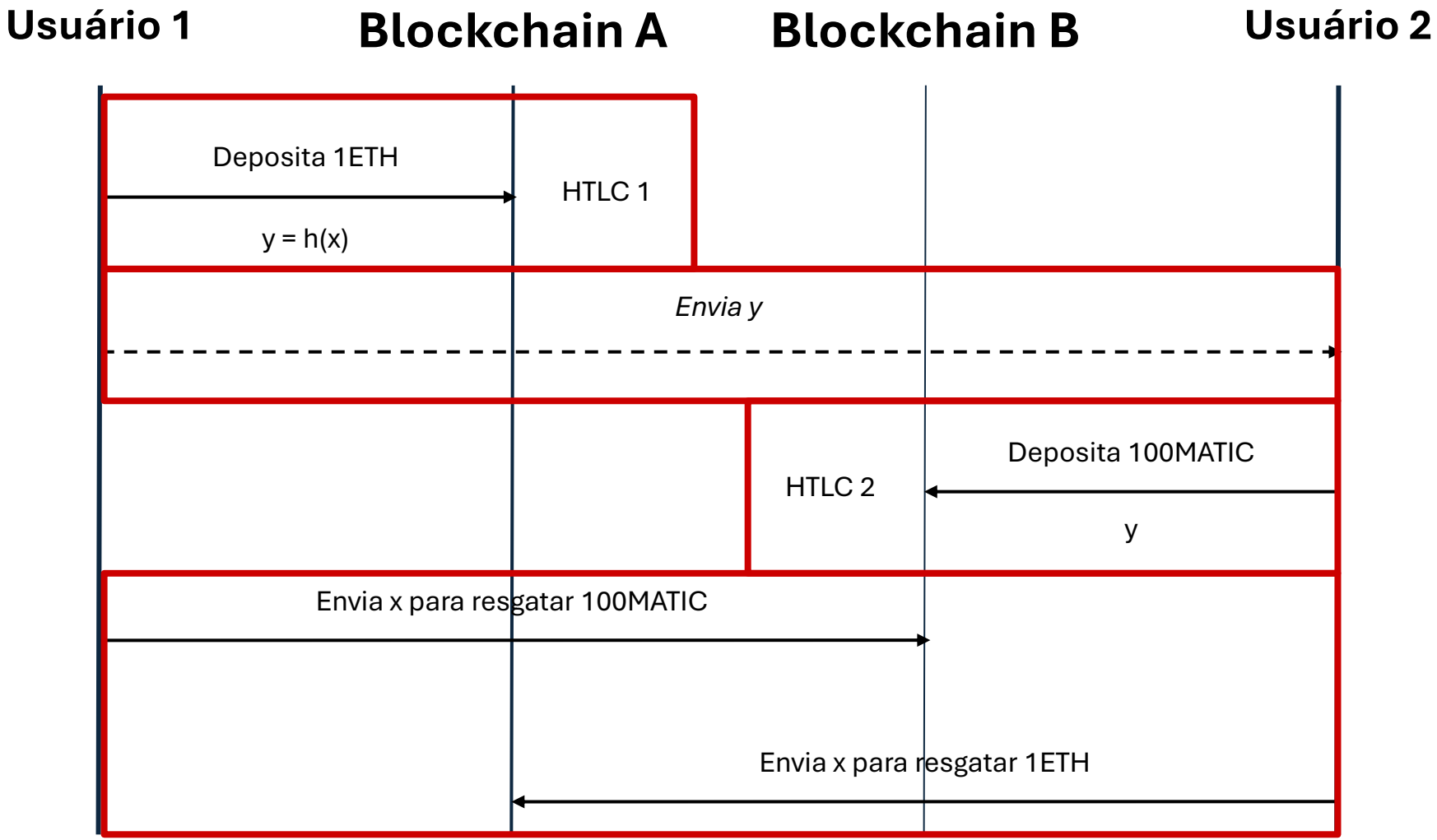
- Mecanismo notarial de assinatura única
- Testes realizados nas redes:
  - Sepolia (Ethereum)
  - Amoy (Polygon)
- Contrato inteligente implementado em Solidity

https://github.com/italloferreira27/Notary-Mechanism/tree/sepolia-amoy--hardhat

Hash Time-Lock Contract (HTLC)

- Um dos mecanismos de cross-chain de comunicação bi-direcional
- Protocolo de transferência de ativos entre duas blockchains que dispensa uma terceira entidade centralizadora
- Concebido inicialmente para resolver o problema de “atomic swaps” de criptomoedas
- **Objetivo principal:** Garantir que as transações nas duas blockchains sejam efetivadas ao mesmo tempo ou que nenhuma delas aconteça

Hash Time-Lock Contract (HTLC)



HTLC: Considerações

- Necessidade de utilizar um canal de comunicação *off-chain* (Linha pontilhada)
- Pressupõe que as duas blockchains possuem a mesma função de *hash*
- Custo de implantação dos contratos na rede sempre que for realizado um *swap*
- Maioria dos protocolos baseados em HTLC não possuem privacidade
- **Podem ocorrer falhas como:**
  - *Lockup griefing*
  - Ataques DDOS
  - Erros de rede

HTLC: Exemplo

- Testes realizados nas redes:
  - Sepolia (Ethereum)
  - Mumbai (Polygon)
- Contrato inteligente implementado em Solidity

https://github.com/RafaelPCoelho/Hash-Time-Lock-Contract/tree/redes-de-teste-sepolia-mumbai

Perspectivas em Interoperabilidade

- Blockchains heterogêneas:
  - **Blockchains públicas vs. permissionadas**
  - Diferentes algoritmos de consenso, padrões e criptografia
- **Interoperabilidade entre blockchains de linguagem de scripts limitadas:**
  - Ethereum e Bitcoin

Segurança

Segurança

- Segurança em uma blockchain
  - Métodos de ataque
  - Mecanismos de defesa
- Auditoria de contratos inteligentes
- Ameaças ocasionadas do comportamento dos usuários
- Perspectivas em segurança

Segurança - Auditoria de Contratos Inteligentes

- Contratos inteligentes são amplamente usados em aplicações DeFi
  - Emissão de tokens, delegação de posse, transferência de ativos
- Importância da auditoria
  - Garantir a segurança e corretude
  - Evitar vulnerabilidades que podem ser exploradas
  - Proteger fundos dos usuários

Segurança - Auditoria de Contratos Inteligentes

- Processo de Auditoria
  - Após o desenvolvimento do código
  - Inspeção Manual
    - CWE (Common Weakness Enumeration), EEA (Enterprise Ethereum Alliance)
  - Análise Automática
    - Estática
    - Dinâmica

Segurança - Auditoria de Contratos Inteligentes

- Ferramentas Automáticas de Auditoria
  - Auxiliar no processo de auditoria
  - Utilizam técnicas como fuzzing, e execução simbólica

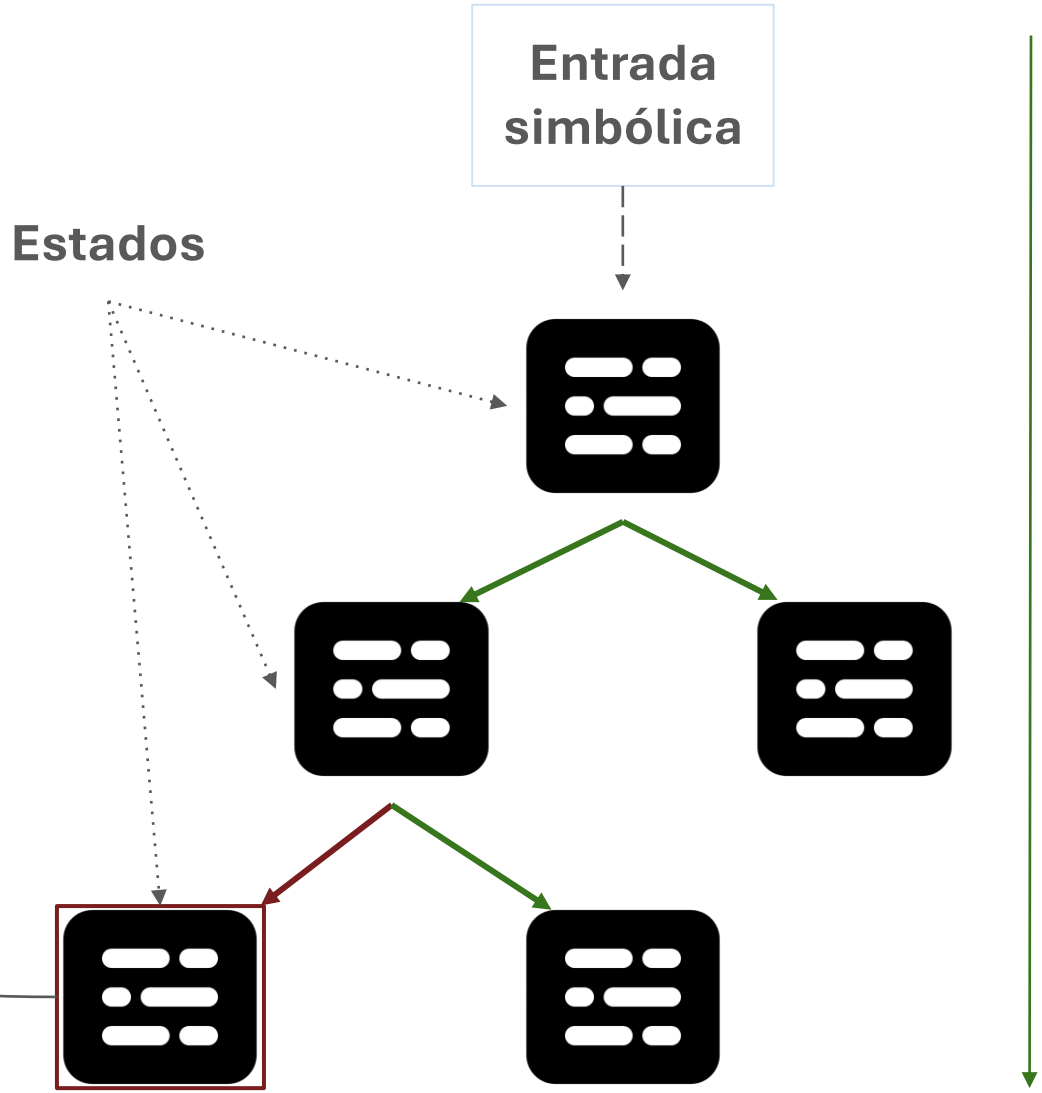
Trabalho	Análise	Entrada	Técnica	Rede
[Xu et al. 2021]	Estática	Código	Aprendizado de máquina	Ethereum
[Yan et al. 2022]	Estática	Código	Aprendizado de máquina	Ethereum
[Li et al. 2022]	Estática/Dinâmica	Código	Execução simbólica	Hyperledger
[Ghaleb et al. 2023]	Estática	Bytecode	Execução simbólica	Ethereum
[Beillahi et al. 2022]	Estática	Opcodes	Grafo de fluxo de controle	Ethereum
[Zhang et al. 2023a]	Estática	Código	Grafo de fluxo de controle	Ethereum
[Xu et al. 2023]	Estática	Código	Árvore Sintática Abstrata	Hyperledger
[Yadav and Naval 2023]	Estática	Bytecode	Execução simbólica	Ethereum
[Ye et al. 2020]	Estática	Código	Grafo de fluxo de controle	Ethereum
[Wang et al. 2020]	Dinâmica	Opcodes	Aprendizado de máquina	Ethereum
[Rodler et al. 2023]	Dinâmica	Bytecode	Fuzzing	Ethereum
[Liu et al. 2023]	Dinâmica	Código	Fuzzing	Ethereum
[Liao et al. 2022]	Estática	Bytecode	Rede Neural	Ethereum

Tabela 1.1. Trabalhos que propõem ferramentas para auditoria de contratos inteligentes.

Segurança - Auditoria de Contratos Inteligentes

- **Execução Simbólica:**

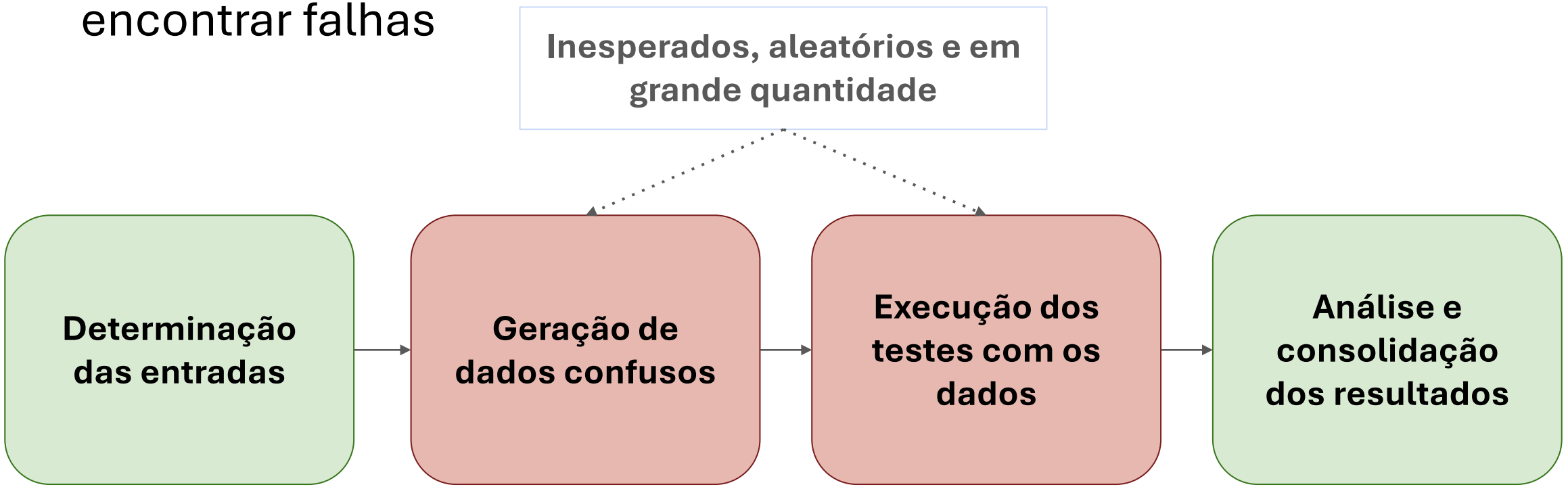
  Explora o espaço de estados do programa para identificar vulnerabilidades



Pergunta chave: Esse estado deveria ser intangível, mas ele realmente é?

Segurança - Auditoria de Contratos Inteligentes

- **Fuzzing:** Técnica que insere entradas aleatórias no código para encontrar falhas

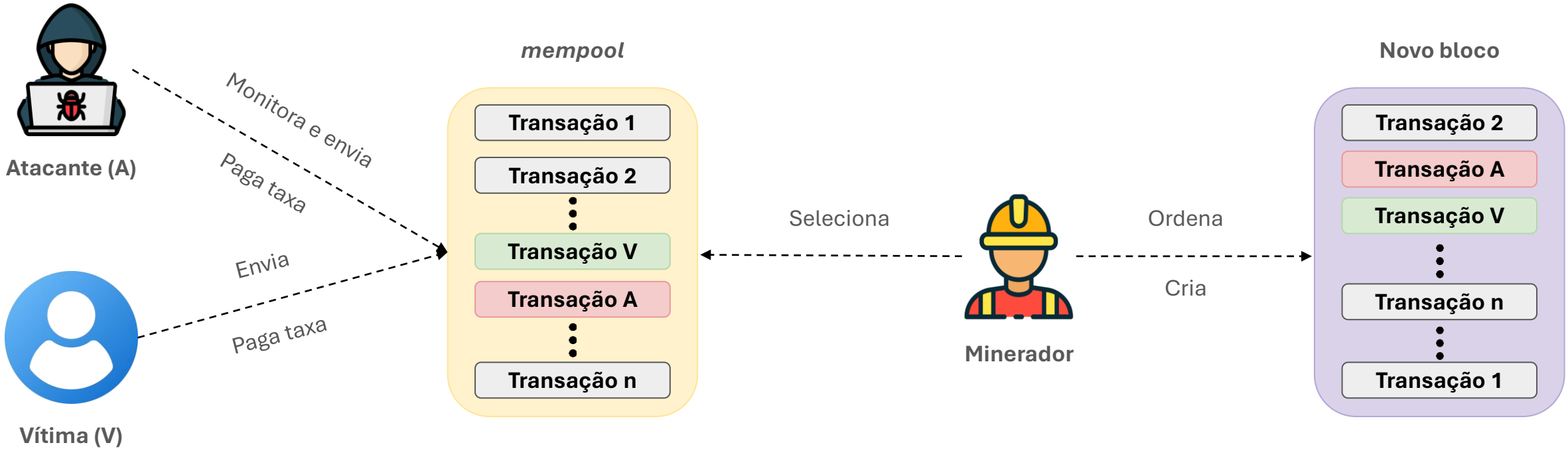


Segurança - Principais ataques no ecossistema DeFi

- Front-running em Redes Blockchain
  - Ação de manipulação da ordem de transações na mempool por usuários estratégicos.
  - Funcionamento
    - Transações são ordenadas pelo preço do gás
    - Atacantes monitoram a fila pública de transações pendentes (mempool).
  - Tipos de Ataques
    - Deslocamento: Transação de ataque com preço de gás mais alto desloca a transação da vítima.
    - Supressão: Múltiplas transações de ataque com preços de gás altos suprimem a transação da vítima.
    - Sanduíche: Atacante cerca uma transação grande com duas próprias, manipulando o preço do ativo.
  - Bots automatizam as tarefas necessárias para o ataque, utilizando múltiplas contas externas.

Segurança - Principais ataques no ecossistema DeFi

- Front-running em Redes Blockchain

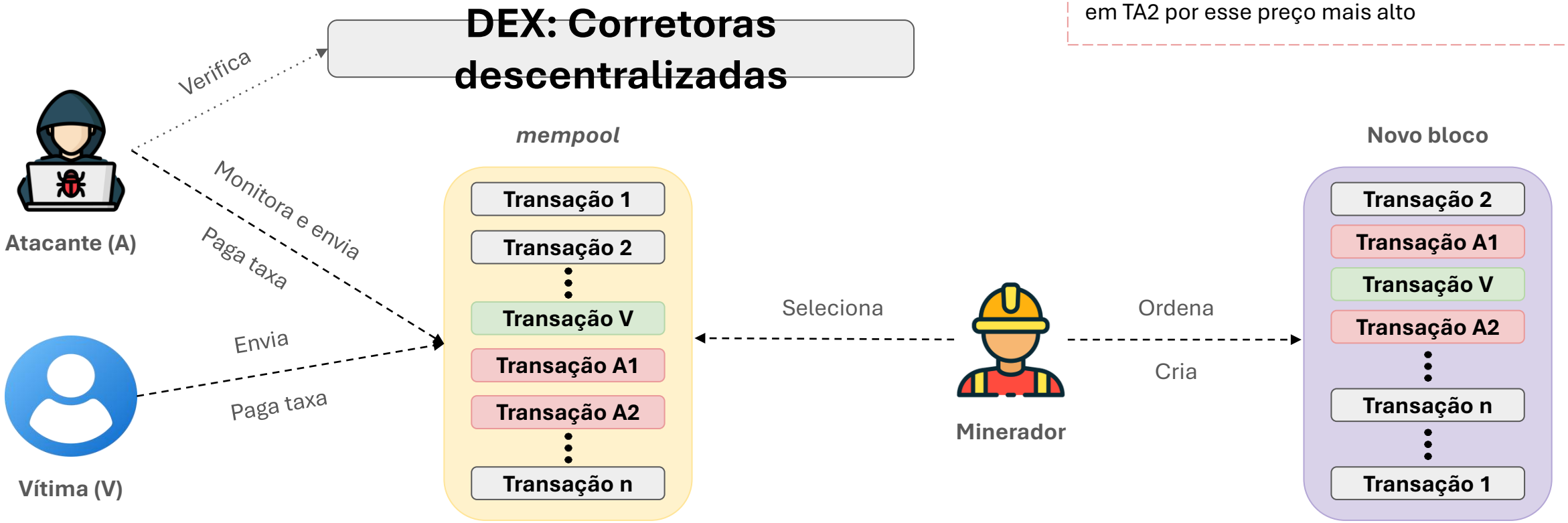


Segurança - Principais ataques no ecossistema DeFi

- Ataque Sanduíche em Redes Blockchain

- A vítima compra os tokens em TV por um preço mais alto do que o esperado devido à compra feita pelo atacante em TA1

- Logo em seguida, o atacante vende os tokens em TA2 por esse preço mais alto



Algoritmo de coleta de dados

1) As transações devem possuir esta ordem: $\mathbf{T_{A1}}$, $\mathbf{T_V}$ e $\mathbf{T_{A2}}$
2) O atacante e a vítima devem comprar o mesmo token em $\mathbf{T_{A1}}$ e $\mathbf{T_V}$
3) O atacante deve vender em $\mathbf{T_{A2}}$ aproximadamente a mesma quantidade de tokens comprada em $\mathbf{T_{A1}}$
4) O atacante e a vítima fazem uso da mesma corretora para realizar as operações de compra e venda dos tokens
5) Sobre os preços de *gas* (taxas):
    a) **Perspectiva Restrita (PR):** O preço do *gas* de $\mathbf{T_{A1}}$ deve ser maior que o preço de *gas* de $\mathbf{T_V}$, e o preço do *gas* de $\mathbf{T_V}$ deve ser maior ou igual ao preço do *gas* de $\mathbf{T_{A2}}$.
    b) **Perspectiva Abrangente (PA):** Sem restrições

Exemplo de dado coletado

T_{A1}	T_V	T_{A2}
Preço do gás: 0.000000013355135653 ETH (13.355.135.653 WEI) **Token:** ETH para FireWorX **Qtde.:** 24.999.081,46 (0.24 ETH)	**Preço do gás:** 0.000000023355135653 ETH (23.355.135.653 WEI) **Token:** ETH para FireWorX **Qtde.:** 1.791.268,54 (0.1 ETH)	**Preço do gás:** 0.000000013355135653 ETH (13.355.135.653 WEI) **Token:** FireWorX para ETH **Qtde.:** 24.999.081,46 (1.12 ETH)

Ordem

Ganho ≈ USD $1059.56

Custo ≈ USD $4.41

Lucro ≈ USD $1055.15

https://github.com/LABPAAD/blockchain_defi

Segurança - Principais ataques no ecossistema DeFi

- Manipulação de Oráculos
  - Conectar a blockchain com provedores de dados externos, crucial para a execução de contratos inteligentes
  - Problemas:
    - Falhas Bizantinas
    - Ponto Único de Falha
  - Mitigação:
    - Quórum Descentralizado
    - Canais Seguros e Considerações Temporais

Segurança - Principais ataques no ecossistema DeFi

- Ataques de Flash Loan
  - Empréstimos rápidos sem garantia
  - Etapas do Ataque
    - Tomada do Empréstimo - Manipulação do Mercado - Realização do Lucro - Reembolso do Empréstimo
  - Requer análise das transações para inferir intenções dos remetentes

Segurança - Principais ataques no ecossistema DeFi

- Ataques de Liquidez
  - Exploração das diferenças de preço entre diferentes pools de liquidez ou corretoras
  - Funcionamento:
    - Arbitragem de Liquidez: Bots exploram diferenças de preços comprando barato e vendendo caro
    - Informações Privilegiadas: Utilização de informações para realizar arbitragem agressiva
  - Embora a arbitragem não seja maliciosa, pode causar desestabilização se realizada com vantagem injusta.

Segurança - Perspectivas em Segurança de DApps

- Importância da Segurança em DApps
  - Contratos inteligentes gerenciam grandes quantidades de criptomoedas
  - Vulnerabilidades são alvo frequente de ataques
  - Imutabilidade das redes blockchain exige um rigoroso teste e design
- Interoperabilidade entre Redes Blockchain
  - Segurança como Desafio Crítico
  - Privacidade e Interoperabilidade
- Desafios de Privacidade em DApps
  - Rastreamento de Transações
  - Privacidade de Dados

Submeta o formulário e ganhe o NFT do JAI!!

https://forms.gle/hVnL5n8c7eMuzqq4A

JAI - 43ª Jornada de Atualização em Informática

44º CSBC 2024

Finanças Descentralizadas em Redes Blockchain: Perspectivas sobre Pesquisa e Inovação em Aplicações, Interoperabilidade e Segurança

Glauber D. Gonçalves

Josué N. Campos

Luis H. S. de Carvalho

INSTITUTO FEDERAL Bahia

Universidade Federal do Piauí

UFV Universidade Federal de Viçosa

ufjf Universidade Federal de Juiz de Fora