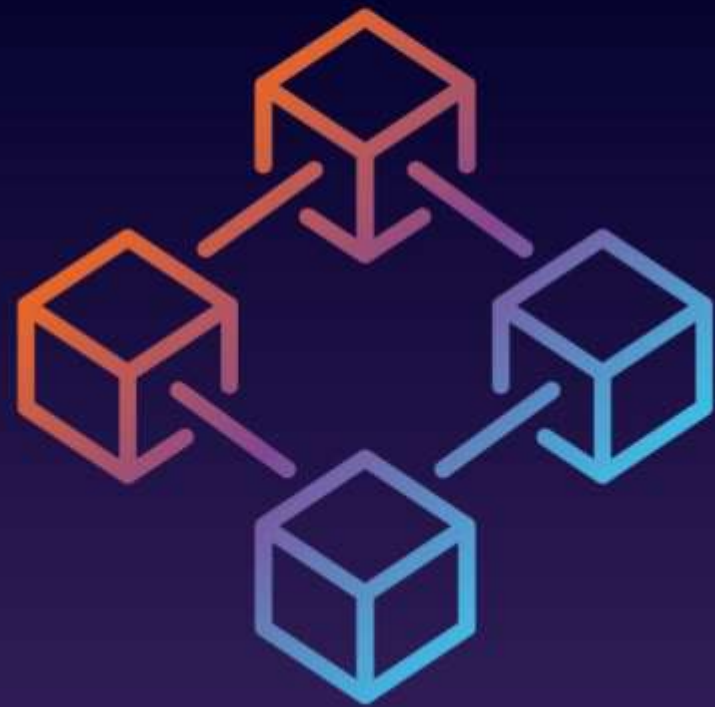


# Ethereum e smart contracts pelo mundo

Solange Gueiros



BLOCKCRYPTO EXPO

# Solange Gueiros

- ❖ Blockchain Leader na 4Cadia
- ❖ Instrutora na Blockchain Academy
- ❖ Professora no MBA de Blockchain da FIAP
- ❖ E mais alguns projetos...

The background of the slide features a light blue gradient with a network diagram. The diagram consists of numerous small, semi-transparent grey circles (nodes) connected by thin, light grey lines. A large, semi-transparent Bitcoin logo (a yellow 'B' with two vertical bars) is centered in the background. On the left side, there is a vertical black line.

# Programa

# Programa

1. Desmistificando conceitos
2. Constantinople
3. Ethereum no mundo





# Bitcoin x Ethereum

- ❖ Falando de blockchain...
- ❖ Bitcoin: mecanismo para troca de valores, seguro e resistente à censura
- ❖ Ethereum: computador descentralizado mundial para criar e executar aplicativos através da EVM - Ethereum Virtual Machine





# Bitcoin x Ether

- ❖ Falando das criptomoedas...
- ❖ Bitcoin: troca de valor
- ❖ Ether: combustível para execução de smart contracts



# Ethereum x Ether

**Ethereum**

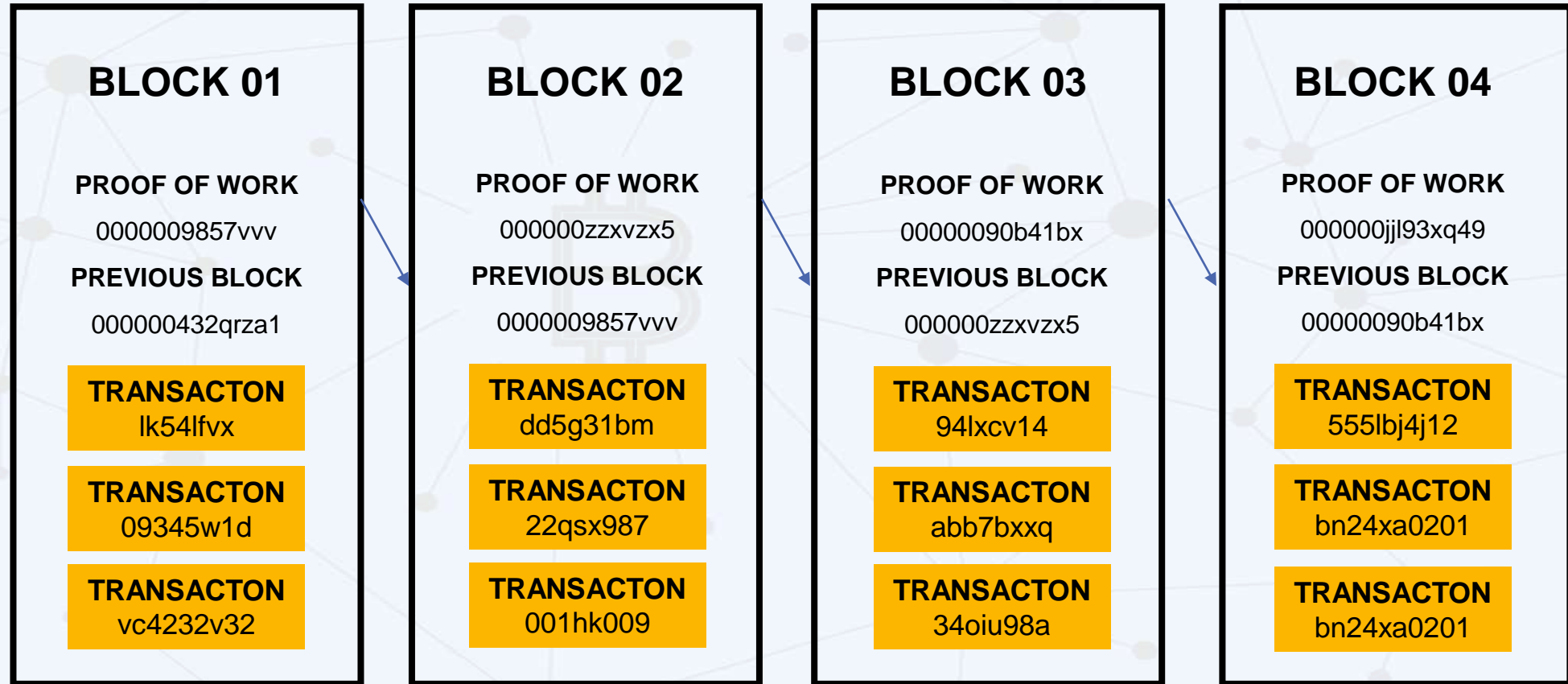
Blockchain  
Infraestrutura  
Tecnologia  
Transações



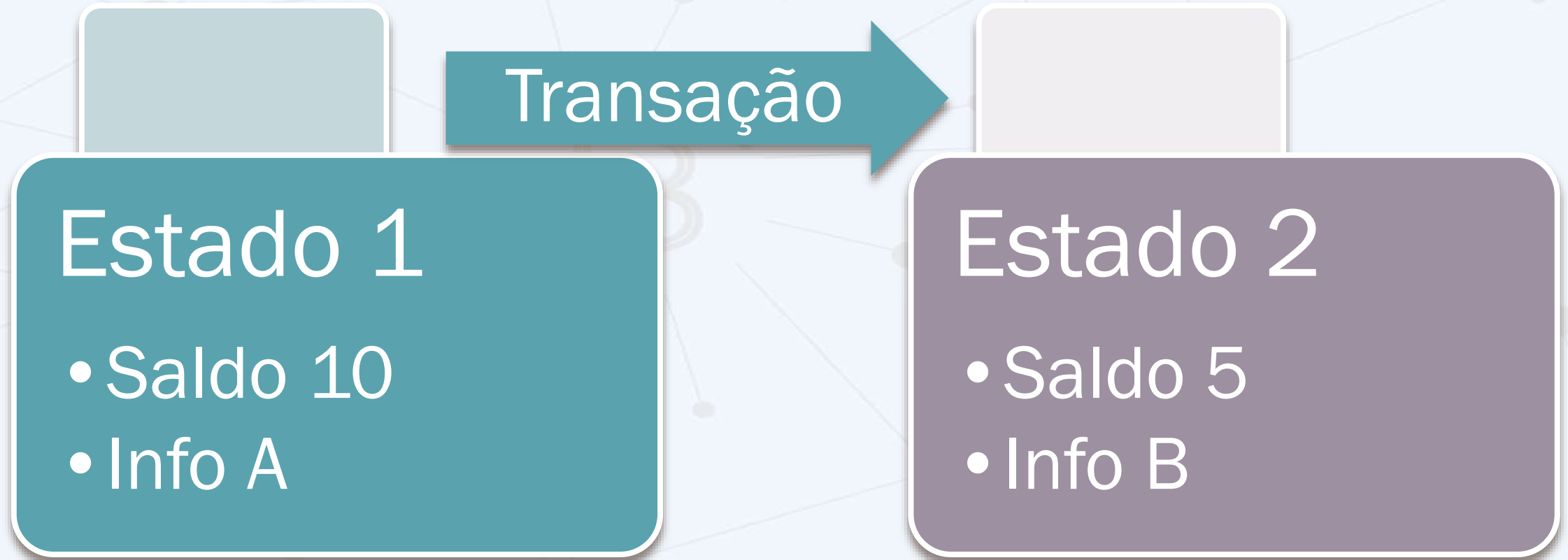
**Ether**

Criptomoeda

# BLOCKCHAIN = CADEIA DE BLOCOS



# Transações e máquina de estado

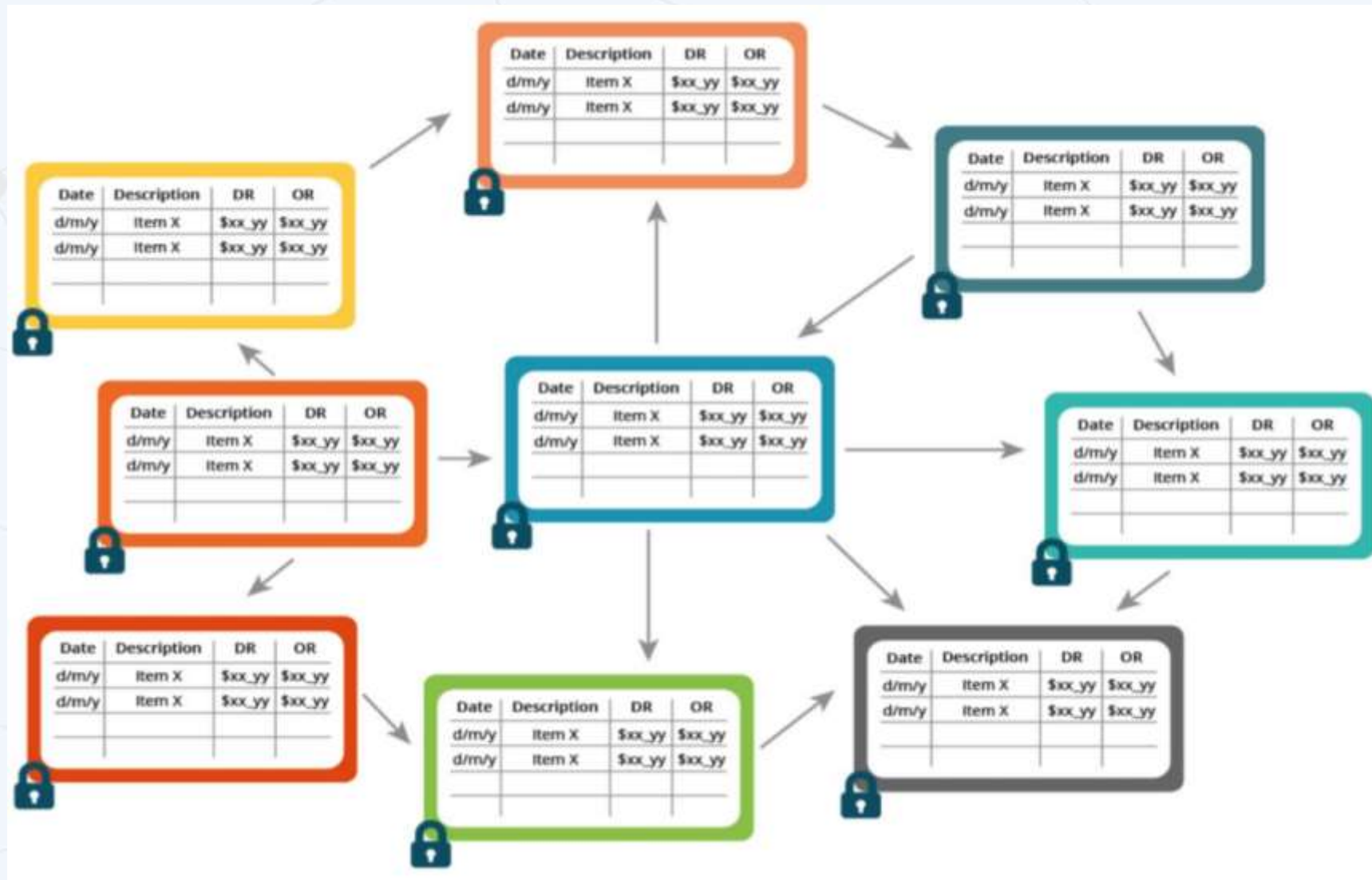


# Transações no Ethereum

- Para transferir Ethers
- Para publicar um smart contract (deploy)
- Para executar alguma função em um smart contract já publicado



# BLOCKCHAIN = LIVRO RAZÃO DISTRIBUÍDO





# Satoshi x Wei

## Bitcoin

Menor unidade: satoshi  
 $10^{-8}$

1 bitcoin = 100.000.000  
satoshi

## Ether

Menor unidade: wei  
 $10^{-18}$

1 ether =  
1.000.000.000.000.000.000  
wei

# UTXO x Balance

- ❖ Bitcoin: UTXO - Unspent Transaction Output
- ❖ Ethereum: Balance e nonce



# Fee x Gas

- ❖ Bitcoin: Fee

- ❖ Troco

- ❖ Ethereum: Gas

- ❖ Gas (quantidade) X Gas price (wei)

# CONTRACT

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]





**SÃO CONTRATOS?**

**NÃO!**



**SÃO INTELIGENTES?**

**NÃO!**



# Imutabilidade

- ❖ Não pode corrigir o código!
- ❖ O smart contract pode ter funções para alterar dados
- ❖ Não pode alterar o histórico:

A informação pode ser registrada em um bloco

E pode ser apagada em outro

Fica o histórico: auditoria!

The background features a complex network diagram with numerous nodes (small circles) connected by thin lines, creating a web-like structure. A large, semi-transparent Bitcoin symbol (a stylized 'B' with two vertical bars) is centered in the background. The overall color scheme is light blue and grey.

# Constantinople

# Constantinople

- ❖ 27-28/fev/2019 - bloco 7.280.000
- ❖ Passo para a transição de PoW para PoS (update Casper)
- ❖ Diminuiu a recompensa de 3 para 2 ETH

# EIP - Ethereum Improvement Upgrade

- ❖ EIP 145
- ❖ EIP 1014
- ❖ EIP 1052
- ❖ EIP 1234





# EIP 145 - Bitwise Shifting (deslocamento de bits)

- ❖ Aumenta a velocidade aritmética na EVM (Ethereum Virtual Machine)
- ❖ Equivalente a operações de multiplicação / divisão com exponenciação.
- ❖ Otimização - shift é mais econômico.

# EIP 1014 - Canais de estado (State Channels)

- ❖ Adiciona canais de status no Ethereum
- ❖ Canais de comunicação bidirecionais entre os participantes que habilitam interações fora do blockchain (off-chain)
- ❖ Diminui o tempo de confirmação de uma transação
- ❖ Não depende de um minerador validá-la

# EIP 1052 - Otimizando verificação do código fonte de um smart contract (Optimizing Large-Scale Code)

- ❖ Altera a maneira que os smart contracts interagem entre si.
- ❖ Inclui um novo opcode na VM do Ethereum
- ❖ EXTCODEHASH
- ❖ Retorna o hash keccak256 do código fonte de um smart contract.
- ❖ a verificação de um smart contract não precisa mais ser realizada com seu código fonte completo, pode-se utilizar apenas seu hash.

# EIP 1234 - Ajuste da recompensa por bloco e adiamento de "Difficulty Bomb"

- ❖ Redução da recompensa de mineração em 33% (Thirddening)
- ❖ De 3 para 2 ETH
- ❖ Adia Difficulty Bomb por 12 meses
- ❖ Difficulty Bomb - aumento exponencialmente da dificuldade da mineração, de modo que ela fique insustentável
- ❖ Objetivo: forçar a transição para Proof of stake

# Trilema - Desafio

- ❖ Escalabilidade
- ❖ Descentralização
- ❖ Segurança



# Escalabilidade - definição

- ❖ Capacidade de manter ou melhorar o desempenho
- ❖ Com aumento do número de usuários / transações
- ❖ Sem prejudicar a experiência do usuário, em termos de
  - ❖ Tempo de confirmação de uma transação
  - ❖ Preços de gás



# Ethereum é escalável?

- ❖ Atualmente não
- ❖ Foi projetado desta maneira
- ❖ Projetos pensando em escalabilidade:
  - ❖ Cosmos, Sharding, Plasma, Raiden and Polkadot

# PoA – Proof of Authority

- ❖ Giveth, POA Network, TomoChain, Rublix, Swarm City, Colony and GoChain.
- ❖ Testnets do Ethereum: Kovan e Rinkeby.
- ❖ Limitações:
  - ❖ Governança
  - ❖ Segurança





- ❖ <https://mainframe.com/>
- ❖ Plataforma para desenvolvimento e ambiente para execução de aplicações descentralizadas
- ❖ Aplicações que não possam ser paradas / desativadas
- ❖ Armazenamento descentralizado

# POA Network

- ❖ <https://poa.network/>
- ❖ Produtos para deixar o Ethereum econômico, rápido e escalável
- ❖ TokenBridge - interoperabilidade
- ❖ Transferência de tokens
- ❖ POA Network - Ethereum Network
- ❖ XDai - representação do DAI - Stable Coin USD







- ❖ <https://www.airswap.io/>
- ❖ Infraestrutura para trade em Dex – Exchanges descentralizadas.
- ❖ Ganhei um prêmio no hackaton EthNewYork em maio/2019, utilizando uma ferramenta deles.





- ❖ <https://elixxir.io/>
- ❖ David Chaum
- ❖ Infra-estrutura de privacidade para web descentralizada
- ❖ Mensagens, pagamentos, aplicações descentralizadas
- ❖ Criptografar e descriptografar transações



- ❖ <https://www.jpmorgan.com/global/Quorum>
- ❖ JP Morgan
- ❖ PoA

# Skale



- ❖ <https://skalelabs.com/>
- ❖ Sidechains “elásticas”
- ❖ Smart contracts e armazenamento de arquivos com custos baixos sem perder a descentralização em favor da performance

# Wyre

- ❖ <https://www.sendwyre.com/>
- ❖ Acesso a evolução das finanças
- ❖ Ferramentas para desenvolvedores blockchain e serviços financeiros



# AAVE

- ❖ <https://ethlend.io/#/main>
- ❖ DeFi – Serviços financeiros descentralizados



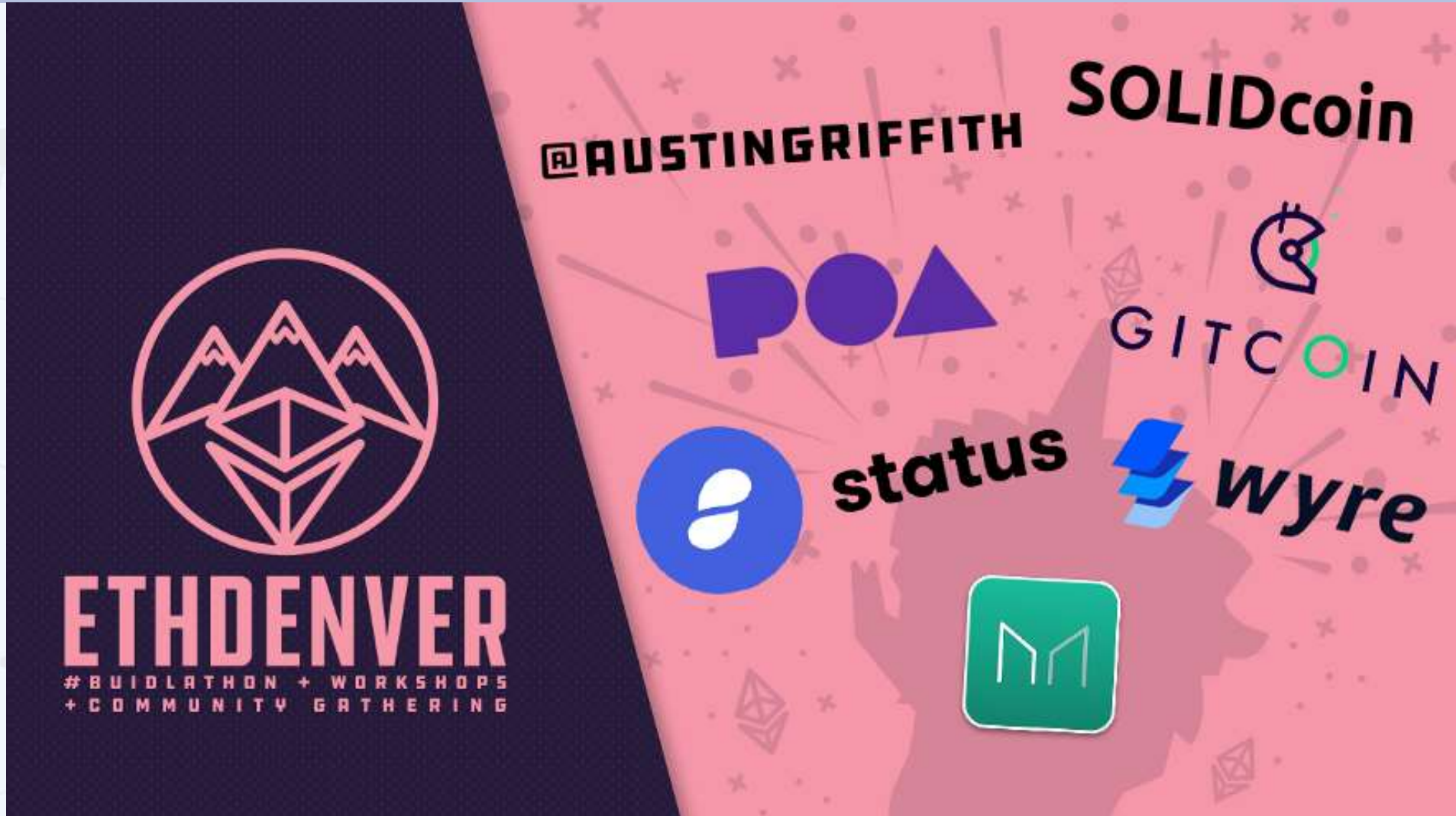
# Chainlink

- ❖ <https://blog.chain.link/>
- ❖ Smart contracts conectados - Oracles
- ❖ Eventos do mundo real e pagamentos





# BuffiDai





[https://cdn-images-1.medium.com/max/2600/1\\*vLW5kHdpnLX6FqjBsm1Swg.png](https://cdn-images-1.medium.com/max/2600/1*vLW5kHdpnLX6FqjBsm1Swg.png)



**Jeff Scott**  
@jeffscottward



♡ 3

&gt;

# Janus Platform



# Janus Plataforma

- ❖ Blockchain Ethereum e IPFS
- ❖ Projeto Alpha (interno)
- ❖ Conjunto de ferramentas para indexação, publicação e pesquisa na Web 3.0





**BLOCKCHAIN  
IMMERSION DAY**



**DLT FOR BANKING**



**ETHEREUM PARA  
DESENVOLVEDORES  
AVANÇADO**



**BLOCKCHAIN &  
LEGAL IMMERSION**  
ASPECTOS LEGAIS NA ERA BLOCKCHAIN



**DEEPLY  
UNDERSTANDING  
ETHEREUM - HANDSON**



**ETHEREUM PARA  
DESENVOLVEDORES  
BÁSICO**



**HYPERLEDGER PARA  
DESENVOLVEDORES  
BÁSICO**



**DEEPLY  
UNDERSTANDING  
ETHEREUM**



<https://www.fiap.com.br/mba/mba-em-blockchain-development-e-technologies/>



# Contatos

[solangegueiros@gmail.com](mailto:solangegueiros@gmail.com)

<https://www.linkedin.com/in/solangegueiros>

<https://twitter.com/solangegueiros>

<https://medium.com/@solangegueiros>

<https://www.facebook.com/solangegueiros>

[www.blockchainacademy.com.br](http://www.blockchainacademy.com.br)

#womeninblockchainbr (whatsapp / telegram)



