## BITCONF

#### Ethereum no mundo

Solange Gueiros



#### Solange Gueiros

- Instrutora na Blockchain Academy
- Professora no MBA de Blockchain da FIAP
- Blockchain Leader na Atlas Project
- E mais alguns projetos...

# Programa Bitconf 2019 - Solange Gueiros

#### 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

**BLOCK 01** 

**PROOF OF WORK** 

0000009857vvv

PREVIOUS BLOCK

000000432qrza1

**TRANSACTON** 

lk54lfvx

**TRANSACTON** 

09345w1d

TRANSACTON

vc4232v32

**BLOCK 02** 

**PROOF OF WORK** 

000000zzxvzx5

**PREVIOUS BLOCK** 

0000009857vvv

**TRANSACTON** 

dd5g31bm

**TRANSACTON** 

22qsx987

**TRANSACTON** 

001hk009

**BLOCK 03** 

PROOF OF WORK

00000090b41bx

**PREVIOUS BLOCK** 

000000zzxvzx5

**TRANSACTON** 

94lxcv14

**TRANSACTON** 

abb7bxxq

**TRANSACTON** 

34oiu98a

**BLOCK 04** 

**PROOF OF WORK** 

000000jjl93xq49

**PREVIOUS BLOCK** 

00000090b41bx

**TRANSACTON** 

555lbj4j12

**TRANSACTON** 

bn24xa0201

**TRANSACTON** 

bn24xa0201

#### Transações e máquina de estado

#### Transação

#### Estado 1

- Saldo 10
- Info A

#### Estado 2

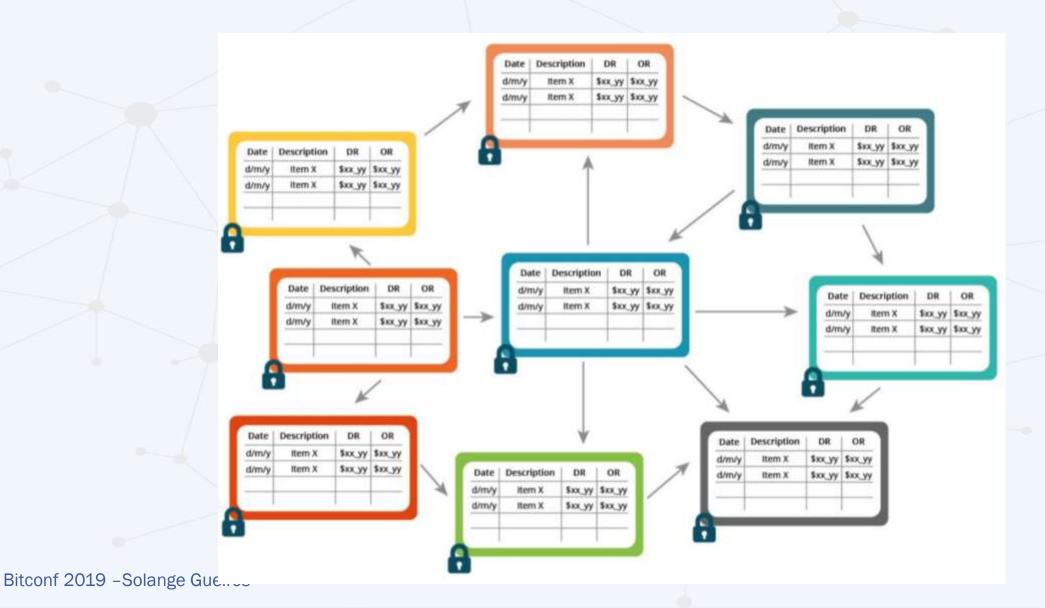
- Saldo 5
- Info B

Bitconf 2019 - Solange Gueiros

#### 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 wei

#### UTXO x Balance

Bitcoin: UTXO - Unspent Transaction Output

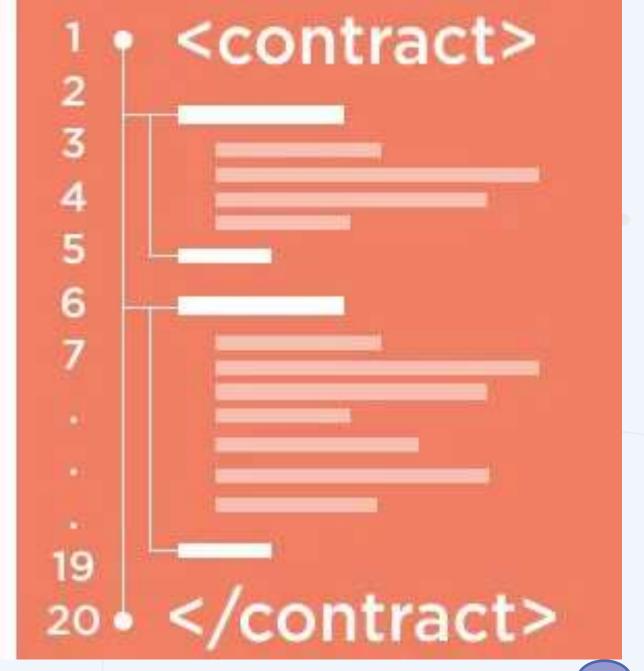
Ethereum: Balance e nonce

#### Fee x Gas

- Bitcoin: Fee
  - Troco

- \* Ethereum: Gas
  - Gas (quantidade) X Gas price (wei)





Bitconf 2019 – Solange Gueiros

#### **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!

### 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% (Thirdening)
- De 3 para 3 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/
- Aplicações que não possam ser paradas / desativadas
- Plataforma para desenvolvimento e ambiente para execução de aplicações descentralizadas
- 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



#### Quorum

- https://www.jpmorgan.com/global/Quorum
- JP Morgan
- \* PoA



#### Zilliqa

- https://zilliqa.com/
- Plataforma escalável para smart contracts
- Para resolver congestinamentos de rede causados por limites de gás e largura da banda
- Utiliza sharding

#### Bloom

- https://bloom.co/
- Login descentralizado
- Identidade
- Score de crédito



# NuCypher



- https://www.nucypher.com/
- Infra-estrutura de privacidade para web descentralizada
- Criptografar e descriptografar transações

#### Skale

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



#### Clearmatics



- https://www.clearmatics.com/
- plataformas p2p baseadas no Ethereum
- mercado financeiro
- \* transações de forma transparente e segura
- sem intermediários desnecessários

#### AAVE

- https://ethlend.io/#/main
- DeFi Serviços financeiros descentralizados



## SALT

- https://saltlending.com/
- Empréstimos garantidos em criptos
- \* Bitcoin, Ether, Dash, Dogecoin, Litecoin, ...



## Chainlink

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



Bitconf 2019 - Solange Gueiros

#### **Fortmatic**

- https://fortmatic.com/
- Produto para que usuários consigam interagir diretamente com as aplicações decentralizadas sem precisar de extensões no navegador ou aplicativos de terceiros

**Fortmatic** 

# Opolis

# OPOLIS

- https://opolis.co/
- DEO decentralized employment organization
- Protocolo para que indivíduos tenham trabalhos e benefícios democraticamente escolhidos por meio de uma organização de emprego descentralizada

# Wyre

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





# BuffiDai



Bitconf 2019 – Solange Gueiros

# BuffiDai



# BootCamp Atlas

# Crie sua criptomoeda em poucas horas

15h - Satoshi Lab

#### **BLOCKCHAINACADEMY.COM**



















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



#### Contatos

```
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
#womeninblockchainbr (whatsapp / telegram)
```

Bitconf 2019 - Solange Gueiros

