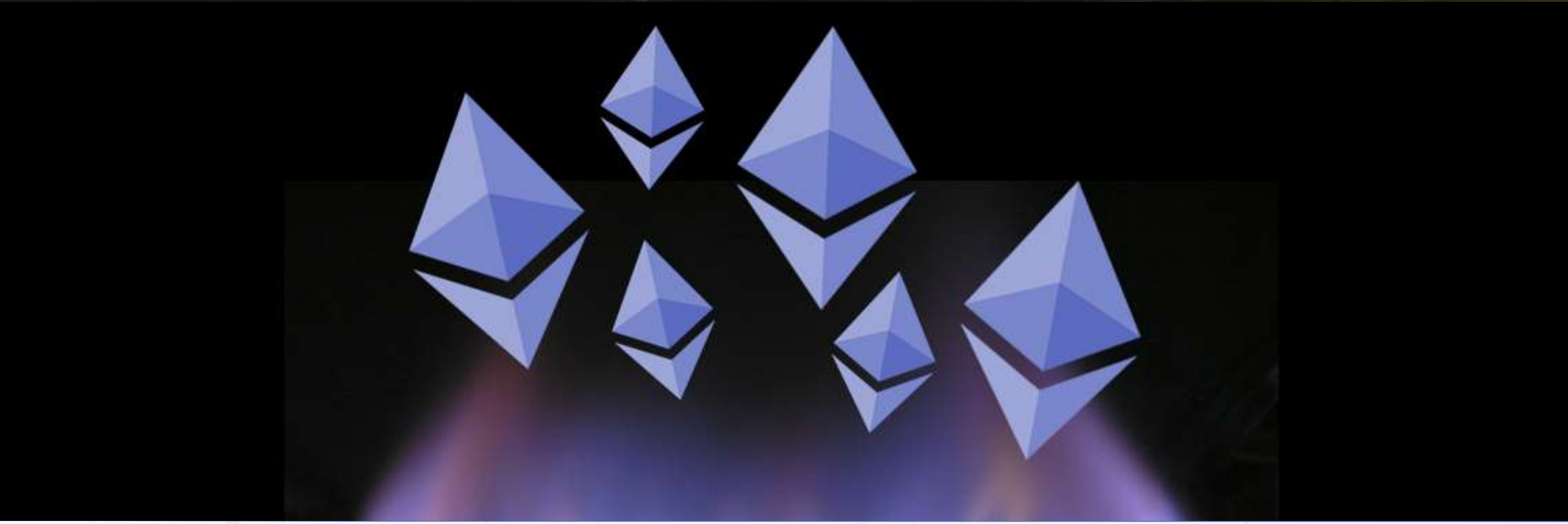
CRIPTO & BLOCKCHAIN DAY 2019



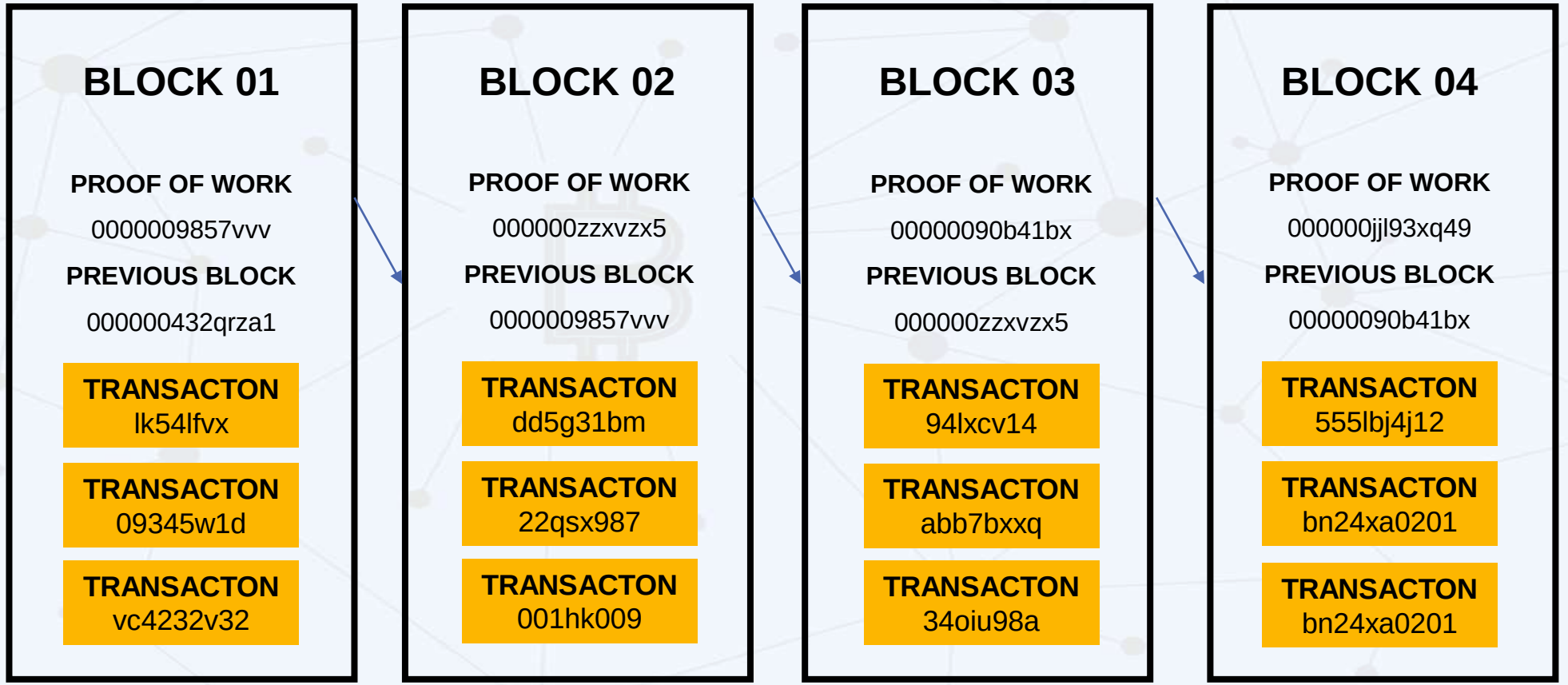
# SMART CONTRACTS NO BLOCKCHAIN ETHEREUM

Solange Gueiros

# SOLANGE GUEIROS

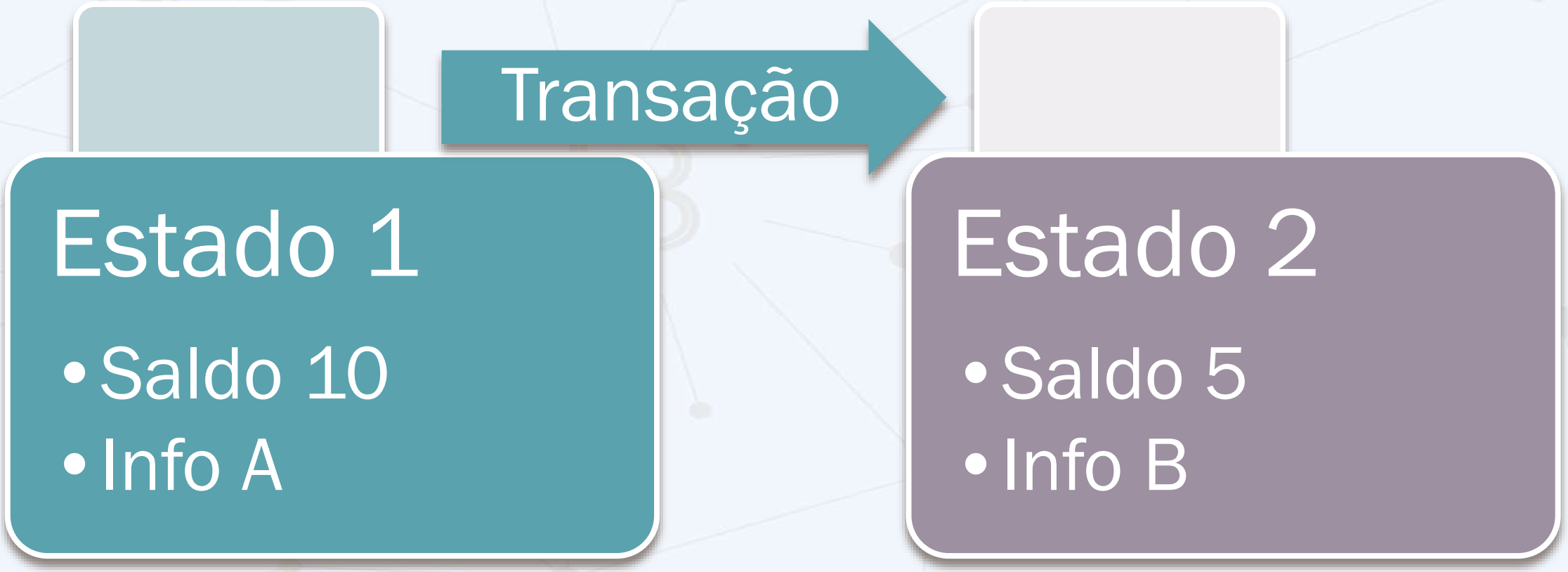
- Ciência da computação na USP – Universidade de São Paulo.
- Pedagogia – Universidade de São Paulo.
- Desenvolvedora há mais de 20 anos.
- Especialista em Blockchain:
  - Bitcoin
  - Ethereum
  - Smart Contracts
  - Solidity
  - Hyperledger
- Primeira desenvolvedora mulher a publicar smart contracts em produção no Brasil

# BLOCKCHAIN = CADEIA DE BLOCOS

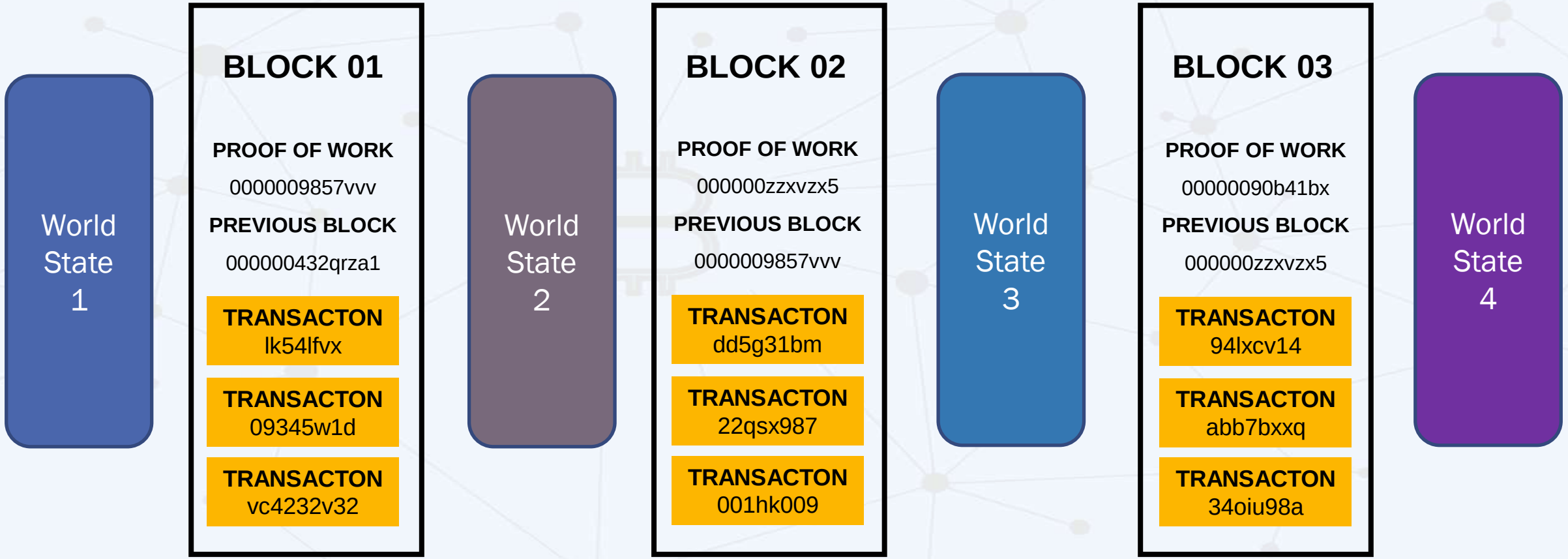



BLOCKCHAIN ACADEMY

# TRANSAÇÕES E MÁQUINA DE ESTADO



# ESTADOS alterados no BLOCKCHAIN




BLOCKCHAIN ACADEMY


ethereum
BLOCKCHAIN APP PLATFORM

# ETHEREUM

- Idealizado em 2013 por Vitalik Buterin
- Primeiras implementações em Go e C++ em Fevereiro/2014
- Lançado em 2015

# ETHEREUM

- Máquina virtual ‘Turing-complete’
- Determinístico
- Execução de smart contracts
- Criação de aplicativos distribuídos

# ETHEREUM - REDES

- PrivateNet
- Testnet
  - Morden - descontinuada
  - Ropsten - mineração
  - Kovan - Parity
  - Rinkeby
- Mainnet
  - Frontier
  - HomeStead
  - Metropolis - atual
    - Byzantium
    - Constantinople: atual - fev/19
  - Serenity

# ETHEREUM - CLIENTS

- http://ethdocs.org/en/latest/ethereum-clients/
- Rodam a EVM - Ethereum Virtual Machine
  - Geth (Go)
  - Parity (Rust)
  - Cpp-ethereum (C++)
  - Pyethapp (Python)
  - Ethereumjs (Javascript)
  - Harmony/ethereumj (Java)
  - EthereumH (Haskell)
  - Ruby-ethereum (Ruby)

# ETHEREUM – COMUNICAÇÃO COM O CLIENT

- Protocolo IPC = Inter-Process Communication endpoint

- Protocolo JSON-RPC
- http://ethdocs.org/en/latest/connecting-to-clients/index.html
  - web3.js (JavaScript)
  - web3j (Java)
  - Nethereum (C# .NET)
  - ethereum-Ruby (Ruby)

# LINGUAGENS DE SMART CONTRACTS ETHEREUM

- Solidity, similar a JavaScript
- Vyper, derivada do Python 3
- Serpent, similar a Python – pouco uso
- Mutan, similar a C - descontinuada
- LLL (low-level Lisp-like language), similar a Lisp

# ETHEREUM X ETHER

## Ethereum

Blockchain

Infraestrutura

Tecnologia

Transações

## Ether

Criptomoeda

Menor unidade: wei

10^-18

1 ether = 1.000.000.000.000.000.000 wei

# GAS X GAS PRICE

Gas (quantidade)

X

Gas price (wei)

https://ethgasstation.info/

# SMART CONTRACTS: SÃO CONTRATOS? SÃO INTELIGENTES?

Solange Gueiros

# SMART CONTRACTS

- Nick Szabo – 1993
- Vending machine - ancestral do Smart Contract
- Assinatura digital
- Verificação por protocolos de computador
- Regras e consequências estritas (documento jurídico):
  - Obrigações
  - Benefícios
  - Penalidades

# NICK SZABO

- Cientista da computação e criptógrafo Nick Szabo
- 1993 / 1994
- Publicação: 1996
- Na época não havia um ambiente apropriado para executar os smart contracts.

https://bitconnect.co/bitcoin-news/800/nick-szabo-developed-a-method-of-sending-bitcoin-transactions-over-radio

# SMART CONTRACTS

## Smart Contracts: Building Blocks for Digital Markets



---

Smart Contracts Glossary

(This is a partial rewrite of the article which appeared in Extropy #16)

### Introduction

The contract, a set of promises agreed to in a "meeting of the minds", is the traditional way to formalize a relationship. While contracts are primarily used in business relationships (the focus of this article), they can also involve personal relationships such

# SMART CONTRACTS

- Vending machine
- Ancestral do Smart Contract


http://www.intelligentvending.co.uk/combi-vending-machines-snacks-drinks/g-snack-smx-vending-machine-elevator-fridge.htm

# SMART CONTRACTS

- Mais do que uma transferência de moeda virtual
- Duas ou mais partes (como todo contrato)
- Implementados com linguagem de programação
- Executados em um computador

# AUTÔNOMIA – SEM INTERMEDIÁRIOS

- Implementação sem envolvimento humano.
- Capaz de obter informações, processá-las e agir de acordo com as regras do contrato, de forma autônoma.
- Capaz de ser executado ou de se fazer cumprir por si só.
- Sem intermediários!

# SÃO CONTRATOS?

# NÃO!

# CONTRATOS JURÍDICO

- Etapas da relação jurídica contratual:
  1. Negociações
  2. Preliminares
  3. Proposta
  4. Aceitação
  5. Elaboração
  6. Execução

# CONTRATOS JURÍDICO

- Regras e consequências estritas (documento jurídico):
  - Obrigações
  - Benefícios
  - Penalidades

# SMART CONTRACTS

- Registro e execução da transação
- A parte executável ou executada do contrato.

# SMART CONTRACT X CONTRATO TRADICIONAL

- Totalmente digital
- Inalterável
- Padronizado
- Economia e velocidade (sem intermediários)
- Automaticamente executado

- Linguagem jurídica passível de múltiplas interpretações.
- Validação depende de terceiros
- Sistema judicial público
  - Caro
  - Demorado
  - Ineficiente

# SÃO INTELIGENTES?

# NÃO!

# SÃO INTELIGENTES?

- Executam apenas o que foi definido
- Não aprendem nada sozinho

# PRÉ REQUISITOS

- Acesso ao objeto do contrato (bloqueio / desbloqueio)
- Assinaturas digitais (chaves privadas)
- Termos do contrato (sequência exata de operações)
- Plataforma descentralizada
- Implantado no Blockchain da plataforma
- Distribuído entre os nós da rede

# SMART CONTRACTS NO ETHEREUM

- Turing-complete
- Os contratos são compilados para a máquina virtual do Ethereum - EVM e em seguida gravados no blockchain
- Programa de computador auto executável

# 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!

# CONSELHOS...

- Três conselhos:

1- Testar

2- Testar

3- Testar!!!

# BOAS PRÁTICAS

- Definir owner
- Quem pode executar o quê
- Imutabilidade = não pode corrigir o código
- Prever uma “saída”
- Cuidado com a lógica e a ordem das operações

# UTILIZAÇÕES

- Logística
- Eleições
- Seguros
- Registro de propriedade
- Registro de autenticidade
- Pagamentos, empréstimos
- IoT

ORIGINALMY.COM

ORIGINAL MY
BLOCKCHAIN

# Desburocratize agora!
# Mais segurança, economia de tempo e dinheiro.

# BLOCKCHAINACADEMY.COM

BLOCKCHAIN ACADEMY








# 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)