

# SMART CONTRACTS NO BLOCKCHAIN ETHEREUM

Solange Gueiros

# SOLANGE GUEIROS

---

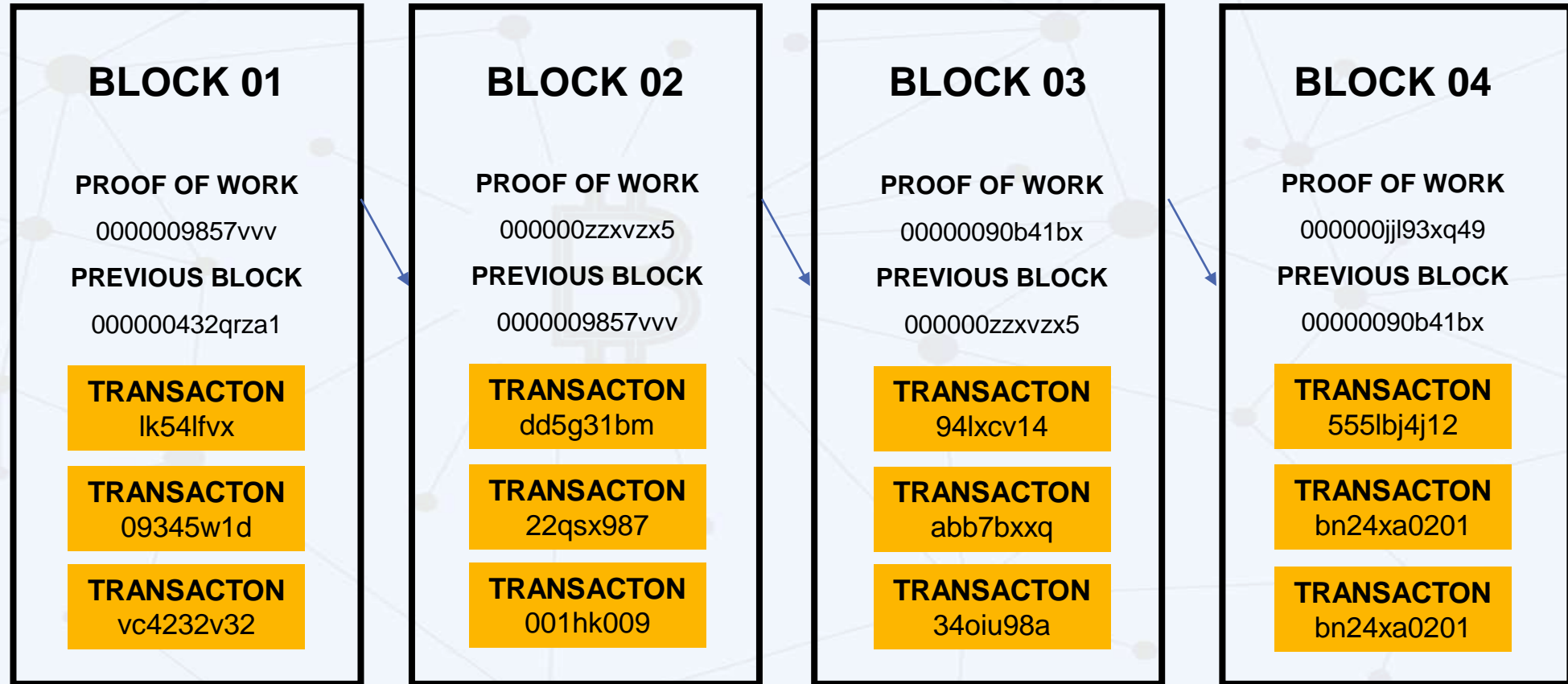
- ❖ Ciência da computação na USP – Universidade de São Paulo
- ❖ Pedagogia – Universidade de São Paulo
- ❖ Mestranda em Digital Currencies na Universidade da Nicosia
- ❖ Desenvolvedora há mais de 20 anos

# SOLANGE GUEIROS

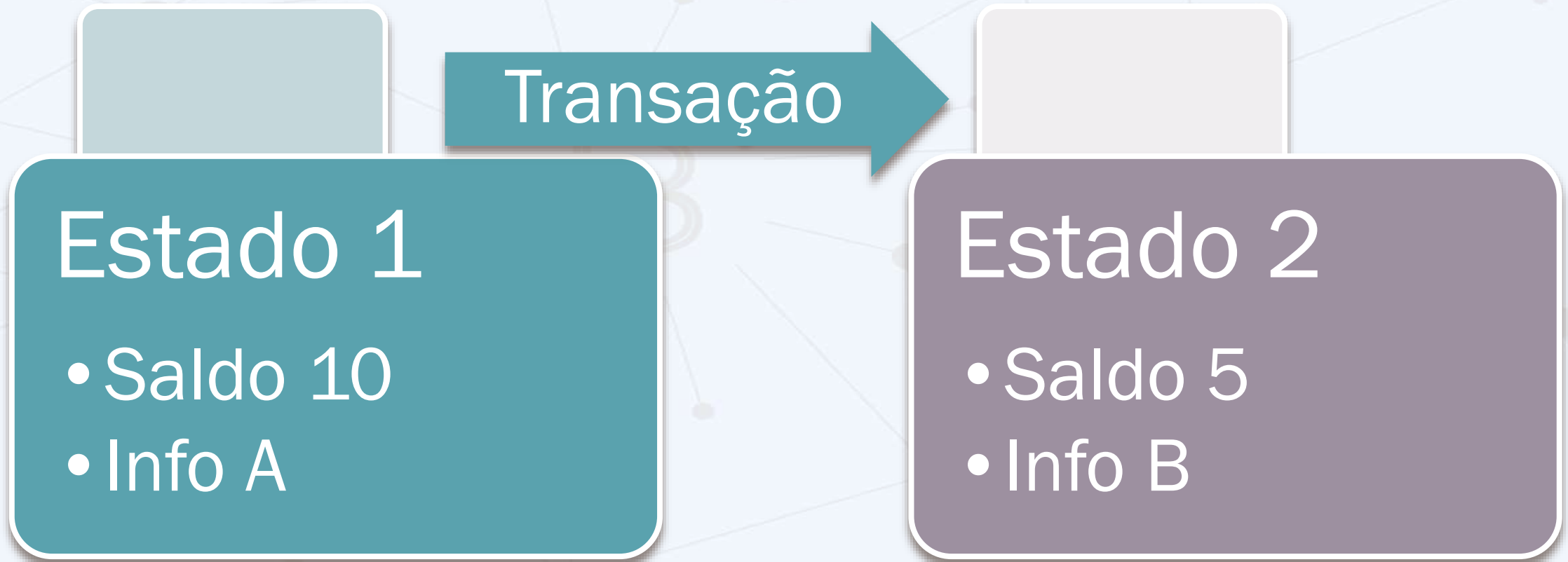
---

- ❖ Consultora especializada em Blockchain:
- ❖ Bitcoin, Ethereum, Smart contracts, Hyperledger
- ❖ Instrutora na Blockchain Academy
- ❖ Professora no MBA de Blockchain da FIAP – São Paulo
- ❖ Primeira desenvolvedora mulher a publicar smart contract em produção no Brasil
- ❖ Prêmio da AirSwap no EthNewYork – mai/2019
- ❖ Prêmio da Waves no EthBerlin – ago/2019

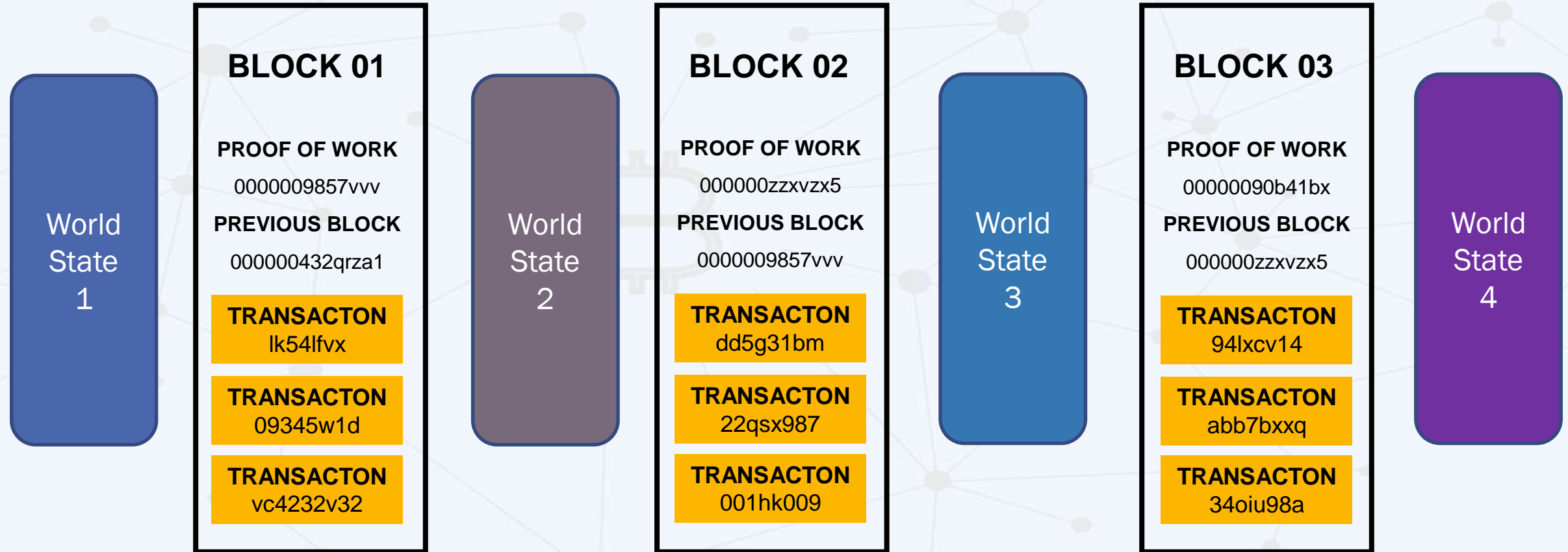
# BLOCKCHAIN = CADEIA DE BLOCOS



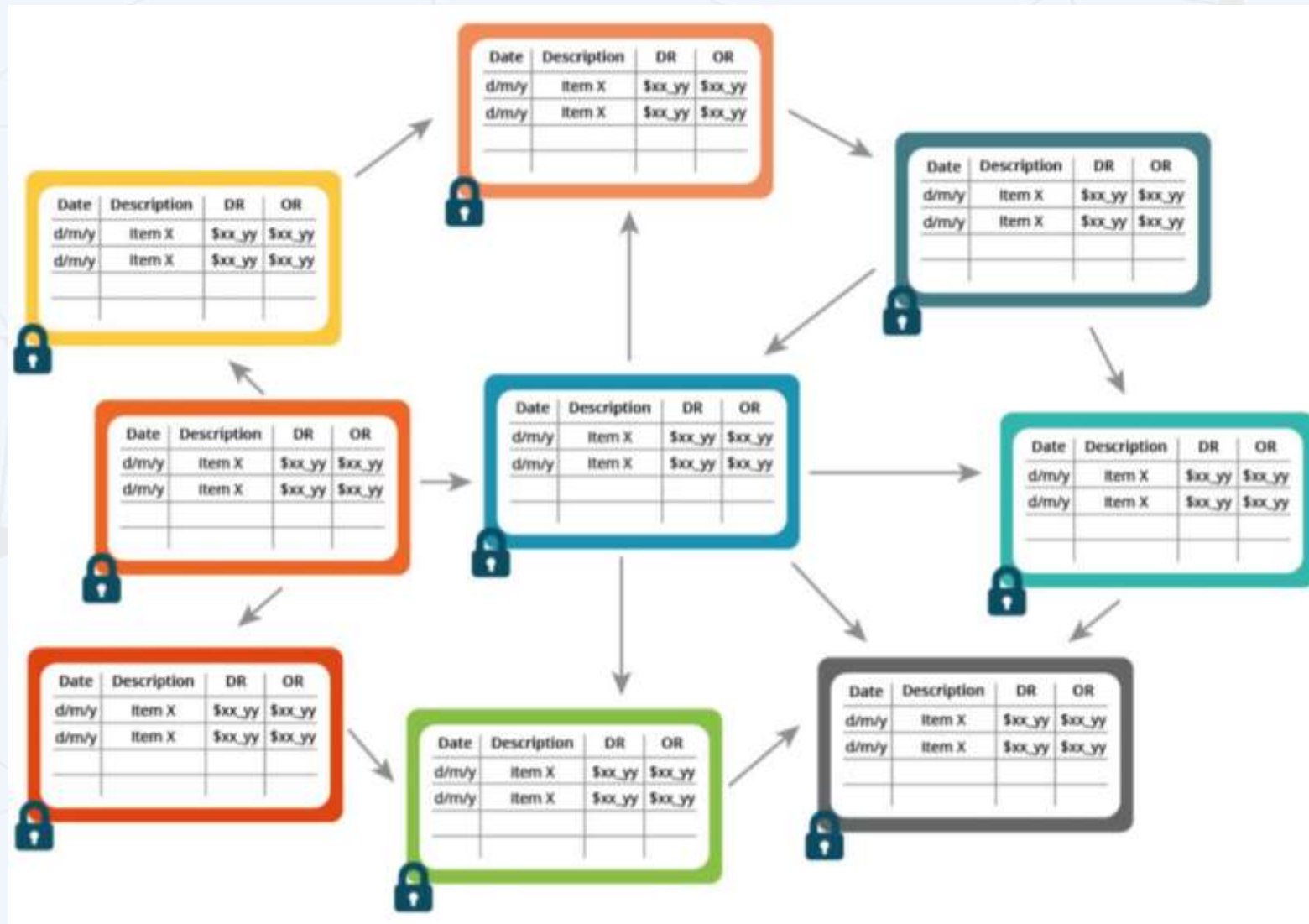
# TRANSAÇÕES E MÁQUINA DE ESTADO



# ESTADOS alterados no BLOCKCHAIN



# BLOCKCHAIN = LIVRO RAZÃO DISTRIBUÍDO









# 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

# Transações no Ethereum

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



# Bitcoin x Ether

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

# 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



# 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

# CONTRACT

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



# 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

## Present

Smart Contracts: Building Blocks for Digital Markets  
Copyright (c) 1996 by Nick Szabo

## Past

permission to redistribute without alteration hereby granted

## Subjects

---

Smart Contracts Glossary

## Projects

## Misc

(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





# 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
- ❖ Assinatura digital

# 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!

A background network diagram consisting of numerous small grey dots (nodes) connected by thin grey lines, forming a complex web. A large, semi-transparent Bitcoin symbol (a yellow 'B' with two vertical lines) is centered behind the text.

**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.



**SÃO INTELIGENTES?**

**NÃO!**

# SÃO INTELIGENTES?

---

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



# 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

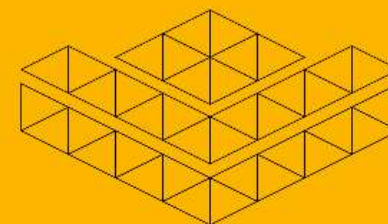
2- Testar

3- Testar!!!



**BLOCKCHAINACADEMY.COM.BR**

Início:  
25/nov



**BLOCKCHAIN  
ACADEMY**



## **Blockchain & Legal Immersion**

CONSTRUINDO O FUTURO DO DIREITO

Mais do que uma aula técnica, é uma porta de entrada para reflexão inicial sobre os pilares do Direito atual e do que poderia fazer sentido manter, ou não, a partir da rápida evolução dos negócios e da sociedade em geral.



**MBA<sup>+</sup>**

**BLOCKCHAIN  
TECHNOLOGIES &  
DEVELOPMENT**



# CONTATOS

---



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

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

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

twitter, facebook, instagram: solangegueiros

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

Grupo womeninblockchainBR (whatsapp / telegram)



