

Vamos falar de

Blockchain

Executando  
uma votação  
eletrônica na  
blockchain

Hands on

Carlos Leonardo S. Mendes  
[caleo@prodemge.gov.br](mailto:caleo@prodemge.gov.br)  
Prodemge



**INOVA** 2020  
3ª semana de inovação  
ressignificando o futuro

Acesse o site e confira a programação completa:  
[www.inova.mg.gov.br](http://www.inova.mg.gov.br)

Realização

Correalização

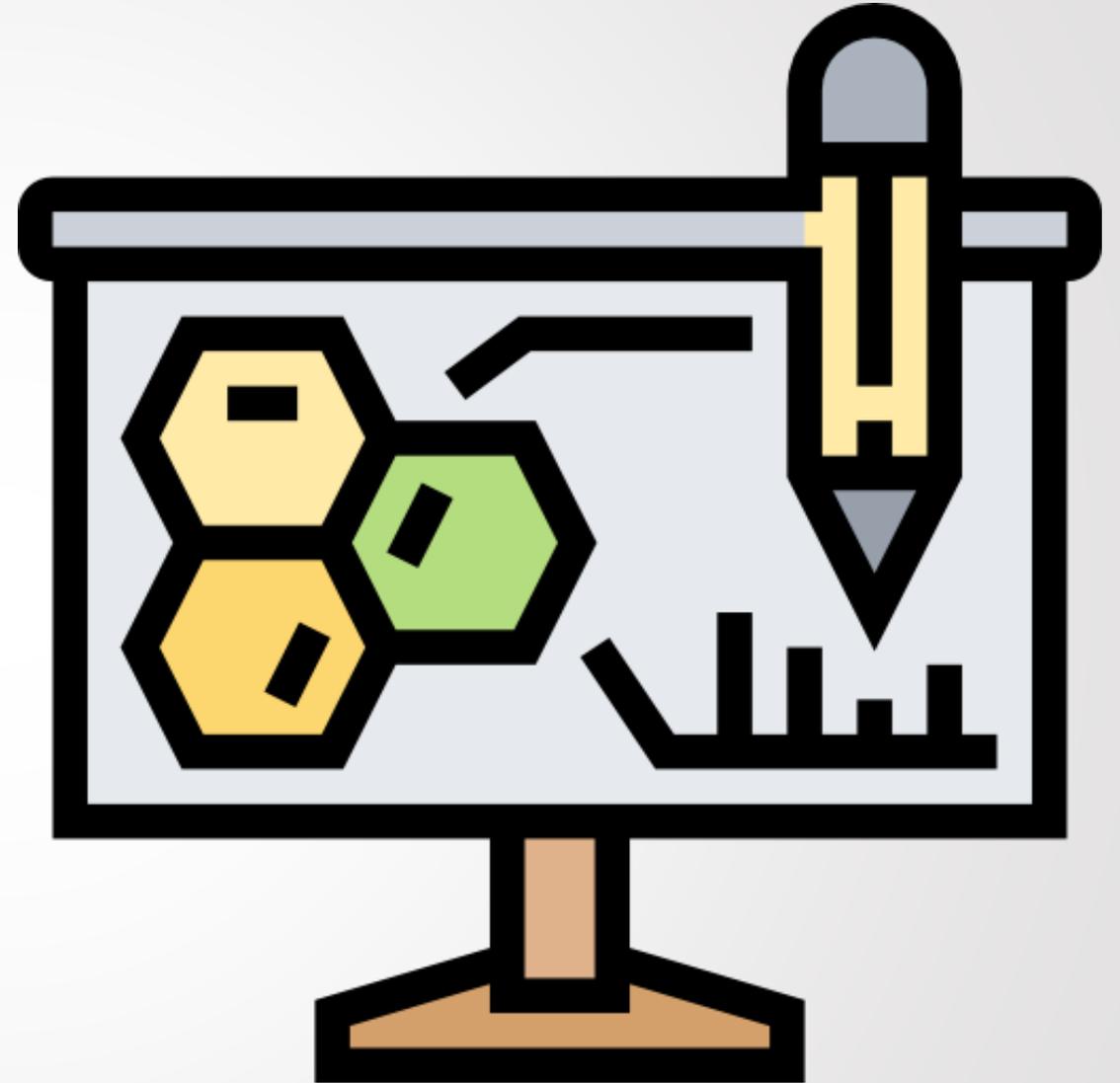
# Objetivos

- ✓ Re(ver) conceitos básicos sobre blockchain.
- ✓ Criar uma carteira digital.
- ✓ Interagir com uma rede de blockchain.
- ✓ Conhecer uma IDE online para codificação e publicação de contratos inteligentes.
- ✓ Ver um exemplo de contrato inteligente.
- ✓ Conhecer como uma aplicação web pode interagir com um contrato inteligente.

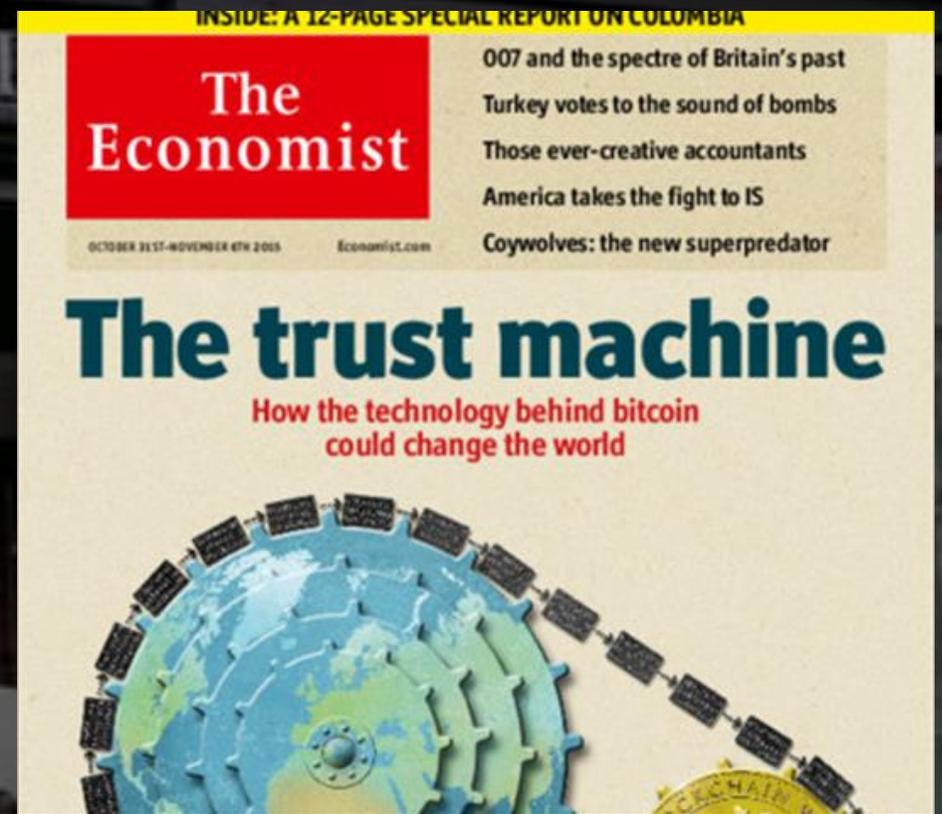


## Parte 1/4

- Origem e definição.
- Redes públicas, privadas e híbridas.
- Bitcoin e Ethereum.



A origem do Blockchain



# O problema do duplo gasto

- Duplo gasto é o risco de uma criptomoeda ser gasta duas vezes.
- É um problema comum a ativos digitais porque informações digitais podem ser reproduzidas com mais facilidade do que ativos físicos (ex.: moeda digital x moeda fiduciária).

## Double Spending of Bitcoin

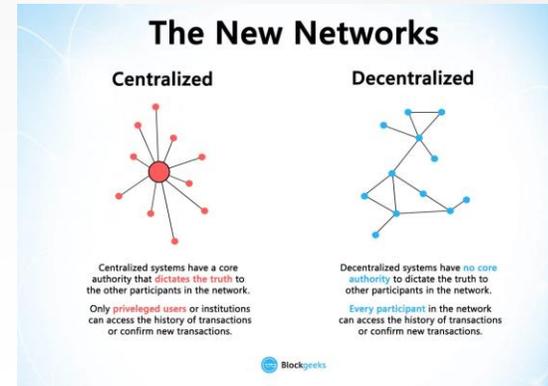


**Buyer**



# Bitcoin, a 1ª plataforma de Blockchain

- Pilares
  - Descentralização
  - Transparência
  - Imutabilidade
- Tecnologias de suporte
  - Hash criptográfico
  - Chaves públicas e privadas
  - Assinatura digital



TxHash	Block	Age	From	To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	0x2bdc9191de5c1b...	0,004741591554641 Ether	0,000294
0xb4d37c791f4cde...	5629306	16 secs ago	0x6c3b4fa413e0e4...	0xf14cb3acac7b230...	0,744767225 Ether	0,000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	0x2d42ee86390c59...	0,016294 Ether	0,000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	0xd39681bb0586fb...	0,01 Ether	0,000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	0x01995788f14357...	0 Ether	0,00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	0x8a91cac422e55e...	0,029594 Ether	0,000294

# O que é Blockchain?

- ✓ Blockchain é um registro distribuído e imutável que facilita o processo de gravação de transações e rastreamento de ativos.



À medida que cada transação ocorre e as partes concordam com os detalhes, ela é codificada em um bloco de dados digitais e assinada digitalmente.

Cada bloco é conectado ao seu antecessor e ao seu sucessor, criando assim uma cadeia irreversível e imutável.



O encadeamento de blocos impede que qualquer bloco seja alterado ou que um bloco seja inserido entre dois blocos existentes.

# Tipos de Blockchain



- ▶ Acesso limitado a uma organização ou consórcio.
  - ▶ Participação autorizada e identidades são conhecidas.
  - ▶ Participação pré-aprovada. Algoritmos de consenso “mais leves”.
  - ▶ Transações mais rápidas (maior *throughput*).
- ▶ Acesso livre.
  - ▶ Participação anônima e sem necessidade de autorização.
  - ▶ Segurança provida por mecanismo de consenso (*proof of work, proof of stake, etc.*).
  - ▶ Transações mais lentas (menor *throughput*).



## Blockchain Público- Permissionada

- Apenas alguns participantes da rede podem escrever novos blocos, mas qualquer um que se junte à rede pode ler.
- Adequadas para soluções de governo, onde apenas algumas instituições podem escrever, mas todas as transações podem ser verificadas pelo público em geral.
- Podem se beneficiar das vantagens de cada tipo de rede, como algoritmos de consenso mais leves, maior throughput, maior transparência.



# Bitcoin

- Proposta por Satoshi Nakamoto em 2008 em um artigo enviado a um grupo de discussão de criptoanalistas.
- A primeira versão da plataforma foi disponibilizada no início de 2009.
- A plataforma foi criada com o objetivo de ser um sistema de pagamento eletrônico com o uso de uma moeda digital (criptomoeda).
- Usada inicialmente no mercado negro, como operações na deep web, a adoção do Bitcoin ampliou consideravelmente e “estimulou” vários governos a implantarem estudos e regulações para uma moeda digital.



# Ethereum

- Proposta por Vitalik Buterin em 2013.
- A rede provê uma máquina virtual descentralizada (EVM), o que permite o registro e a execução de código na rede de blockchain (smart contracts).
- A EVM permitiu o desenvolvimento de milhares de aplicações na plataforma Ethereum.
- A rede Ethereum é a plataforma de sustentação para mais de 250.000 criptomoedas.
- Um grande esforço está em andamento para o desenvolvimento da Ethereum 2.0.

# Redes Ethereum

- Existem redes Ethereum para uso em desenvolvimento, teste e produção.

Network	Chain	Chain ID	Network ID	Type
<code>mainnet</code>	ETH	1	1	Production
<code>ropsten</code>	ETH	3	3	Test
<code>rinkeby</code>	ETH	4	4	Test
<code>goerli</code>	ETH	5	5	Test
<code>dev</code>	ETH	2018	2018	Development
<code>classic</code>	ETC	61	1	Production
<code>mordor</code>	ETC	63	7	Test
<code>kotti</code>	ETC	6	6	Test

# Ethereum



ethereum

Ethereum Blockchain Explorer

Quick links: [ERC-20 Tokens](#) [ERC-721 Tokens](#)

All Filters Search by Address / Txn Hash / Block / Token / Ets Search

ETHER PRICE: \$177.93 @ 0.02197 BTC (+2.26%)  
MARKET CAP: \$19,249,431,908.318

LATEST BLOCK: 8759752 (13.4s)  
TRANSACTIONS: 562.98 M (0.2 TPS)  
DIFFICULTY: 2,499.77 TH  
HASH RATE: 190,287.24 GH/s

ETHEREUM TRANSACTION HISTORY IN 14 DAYS

Latest Blocks			Latest Transactions				
Bk	8759752	Miner Ethermine 34 txns in 6 secs	2,03452 Eth	Tx	0x2af30fa1dee... 34 secs ago	From 0x581b34d2cd391... To 0x07771716d1957952...	0 Eth
Bk	8759751	Miner PandaMiner 151 txns in 17 secs	2,10742 Eth	Tx	0x2992e3b5c3... 34 secs ago	From 0x03e7db3c1ab99f... To 0x0fa8a6059ea8192...	0 Eth
Bk	8759750	Miner Spark Pool 53 txns in 6 secs	2,08753 Eth	Tx	0x39cd90730c... 34 secs ago	From 0x751f03163e43b5c... To 0x0fa8a6059ea8192...	0 Eth
Bk	8759749	Miner Spark Pool 1 mins 2 secs ago	2,01840 Eth	Tx	0xa9f69e3cfc5c... 34 secs ago	From 0x17c930879f85ca... To 0xb60329af456cb15...	0 Eth
Bk	8759748	Miner Ethermine 227 txns in 13 secs	2,12223 Eth	Tx	0x1459eb4eab... 34 secs ago	From 0x9a75eabb817b9e... To 0xbc2aad1ec40757...	0 Eth
Bk	8759747	Miner Nanopool 167 txns in 6 secs	2,02306 Eth	Tx	0xf6c9e5f5d65... 34 secs ago	From 0x9a75eabb817b9e... To 0xbc2aad1ec40757...	0 Eth

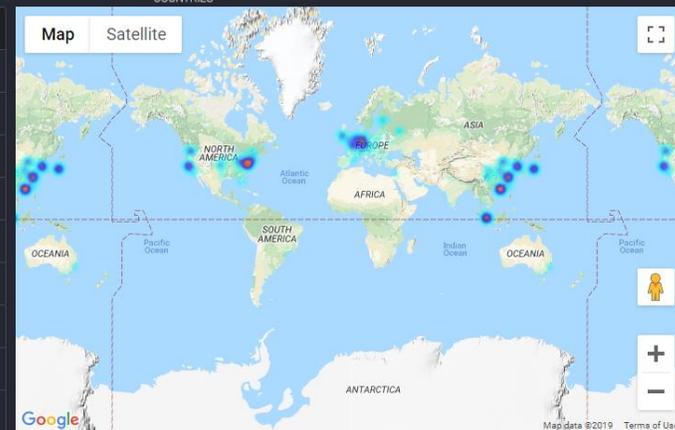
<https://etherscan.io/>

## Ethereum Mainnet Statistics

Clients Sync Status OS **Countries** Network Types History

COUNTRIES

Total	6746 (100%)
United States	1838 (27.25%)
China	1086 (16.10%)
Germany	595 (8.82%)
Singapore	499 (7.40%)
Hong Kong	438 (6.49%)
South Korea	354 (5.25%)
Japan	345 (5.11%)
France	214 (3.17%)
Netherlands	162 (2.40%)



<https://www.ethernodes.org/>

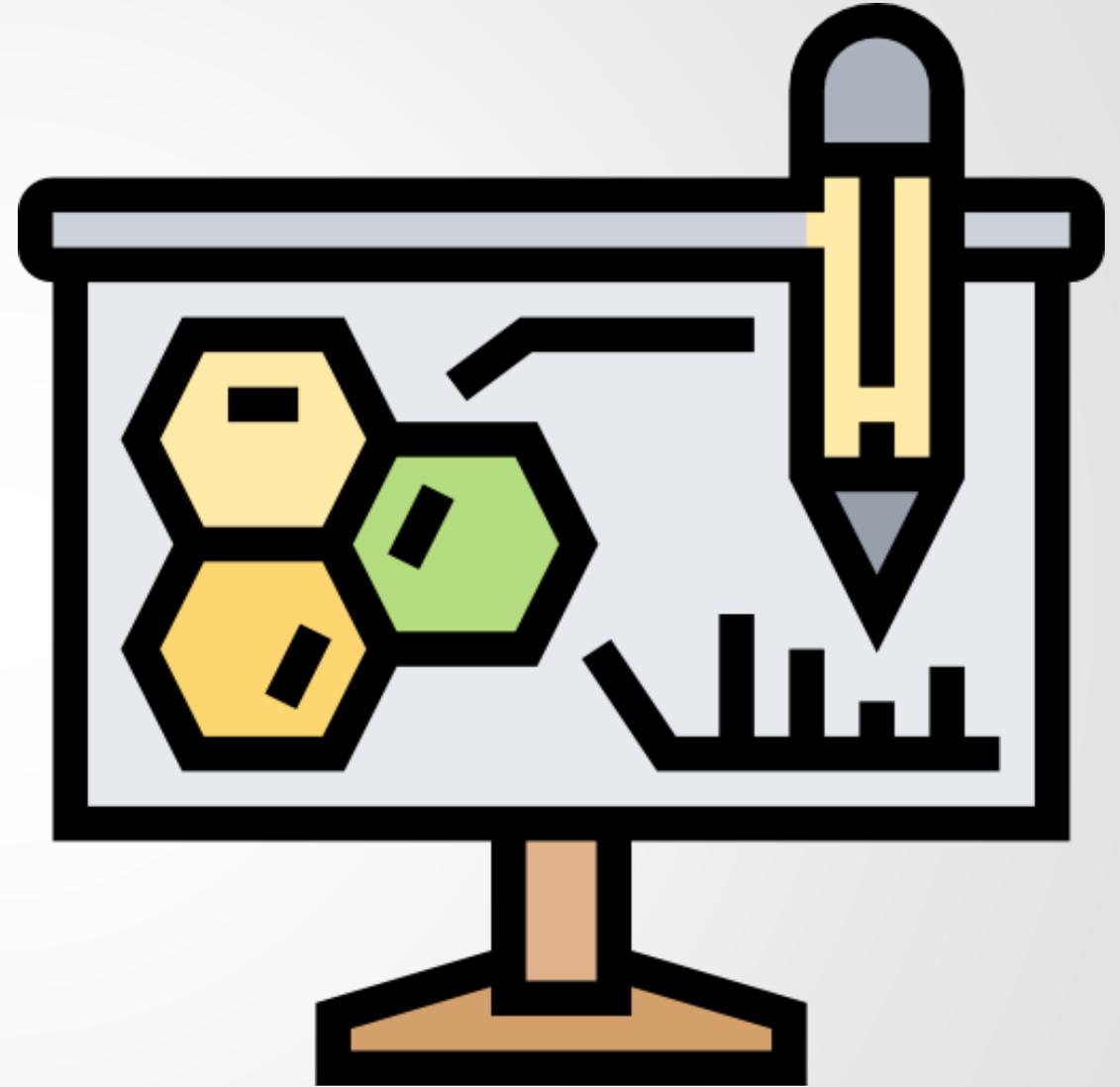
## Parte 2/4

- Criar uma carteira digital.
- Transferir Ether.



## Parte 3/4

- Contratos inteligentes (smart contracts).



# Smart Contracts

# Contratos inteligentes

*Uma evolução do Bitcoin*

## TRADITIONAL CONTRACT



*"The code is the law"*

## SMART CONTRACT

*(blockchain programável)*



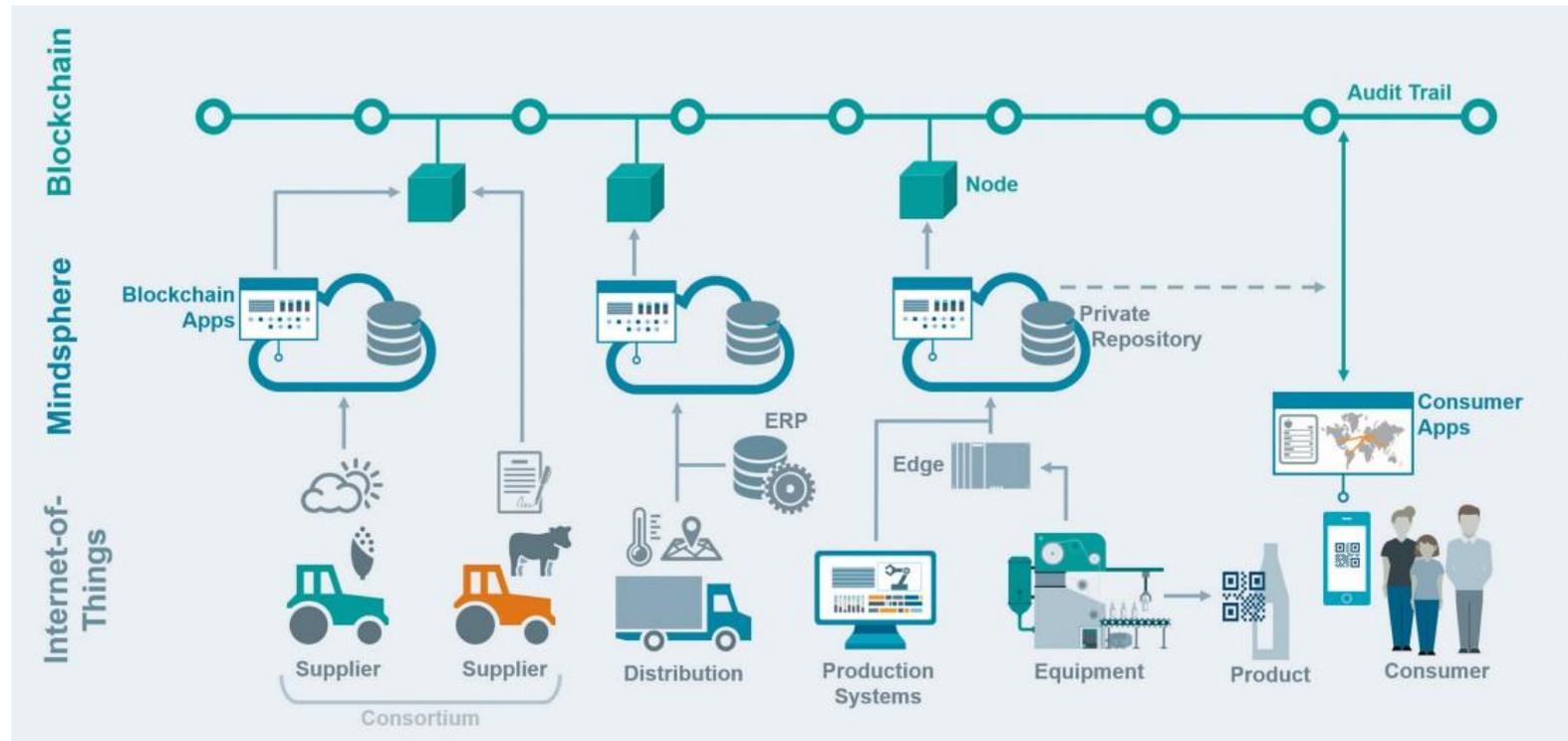
# Smart Contracts



[https://youtu.be/r-ja\\_ZQLCGE](https://youtu.be/r-ja_ZQLCGE)

# Smart Contracts

*Exemplo: cadeia de suprimentos*



<https://www.hyperledger.org/resources/publications/walmart-case-study>

## Parte 4/4

- Remix, uma IDE online para codificação e publicação de contratos inteligentes.
- Contrato inteligente (votação eletrônica).
- Aplicação web de votação.



# Onde obter mais informações

- Ethereum
  - <https://ethereum.org/en/>
- Remix
  - <https://remix-ide.readthedocs.io/en/latest/>
- Solidity
  - <https://docs.soliditylang.org>
  - <https://cryptozombies.io/pt/>
- Web3.js
  - <https://web3js.readthedocs.io/>



Vamos falar de

*Blockchain*

**Executando uma  
votação eletrônica na  
blockchain**

**Obrigado!**



**INOVA** 2020  
3ª semana de inovação  
ressignificando o futuro

**4 dez  
10h as 11h**

**Minas Gerais na Vanguarda: Blockchain e o  
monitoramento da Cadeia do Carvão Vegetal**  
Tiago Aroeira Marliere  
SEMAD/MG

**Programando um Token ERC20 na Blockchain**  
José Nogueira  
BNDES

**3 dez  
10h as 12h**

**Decifrando o Blockchain, sem o hype: entendendo  
os benefícios e limitações da tecnologia**  
Marcos Antônio Simplício Junior - USP

**4 dez  
11h as 12h**

Acesse o site e confira a programação completa:

[www.inova.mg.gov.br](http://www.inova.mg.gov.br)

Realização

Correalização

