

XXI ESCOLA REGIONAL DE COMPUTAÇÃO BAHIA - ALAGOAS - SERGIPE



**ERbase 2021**  
O FUTURO E O PAPEL DA COMPUTAÇÃO PÓS PANDEMIA

## BLOCKCHAIN E IOT INTEGRADOS A SISTEMAS WEB

Jauberth Abijaude  
jauberth@uesc.br

Péricles Sobreira  
pericles.delimasobreira@uqo.ca

Fabíola Greve  
fabiola@ufba.br

Realizado por:  


Patrocínio:  


1

## AUTORES



**Fabíola Greve**  
Doutora em Informática pela Université Rennes 1 e Laboratórios IRISA-INRIA, França  
Professora UFBA



**Jauberth Weyll Abijaude**  
Doutorando em Ciência da Computação – UFBA  
Professor UESC



**Péricles Sobreira**  
Doutor em Ciência da Computação pela Université Grenoble Alpes, França  
Professor University of Quebec at Outaouais e Granby College



**Henrique Serra**  
Graduando em Ciência da Computação – UESC  
Bolsista de IC

ERBASE 2021- Jauberth Abijaude (UESC)

2

2

# BLOCKCHAIN E IOT INTEGRADOS A SISTEMAS WEB

## Introdução

Blockchain, arquitetura e protocolos de Consenso

IoT e Aplicações Blockchain-IoT

Plataforma Ethereum e Contratos Inteligentes

Aplicações e Prática

Desafios de Pesquisa e Conclusões

ERBASE 2021- Jauberth Abijaude (UESC)

3

# BLOCKCHAIN

- Vamos apresentar:
  - Blockchain
  - Características
  - Protocolos de Consenso

ERBASE 2021- Jauberth Abijaude (UESC)

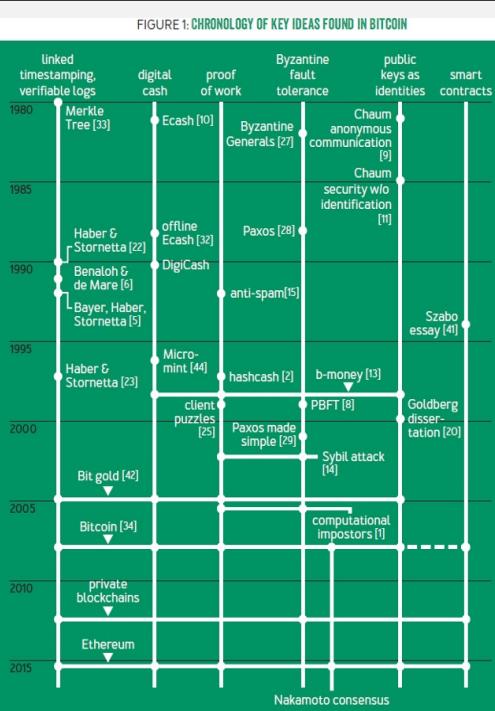
4

# Blockchain: Rede de Confiança Digital



5

5



## HISTÓRICO

- M. E. Hellman e Whitfield Diffie, 1976, *Criptografia de chave pública*.
- Lamport, 1982, *Consenso dos Generais Byzantinos*
- N. Szabo, 1994, *Smart Contracts*
- Satoshi Nakamoto, 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System".
- Bitcoin, 2009
- Vitalik Buterin, 2014, "A next generation smart contract and decentralized application platform"
- Ethereum, 2015

6

6

## COMPONENTES DE UMA BLOCKCHAIN

**Rede P2P**

**Criptografia**

**Protocolos de Consenso**

**Máquina de Estados**

**Cadeia de blocos  
(blockchain)**

**Mecanismos de Incentivo**

ERBASE 2021 - Jauberth Abijaude (UESC)  
Blockchain Aberta

7

7

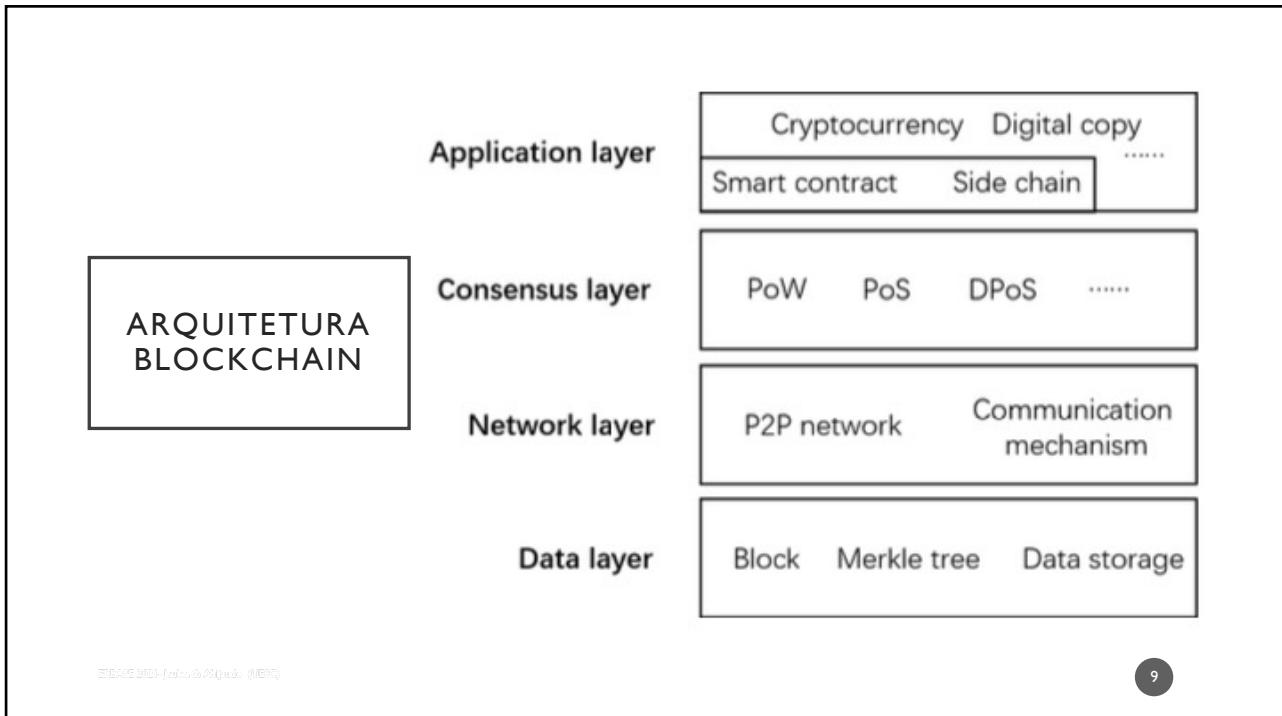
**PROPRIEDADES DA BLOCKCHAIN**

- Descentralização
- Disponibilidade e Integridade
- Transparência e Auditabilidade
- ✓ Imutabilidade e Irrefutabilidade
- Privacidade e Anonimidade
- ✗ Desintermediação
- 握手图标 Cooperação e Incentivos

ERBASE 2021 - Jauberth Abijaude (UESC)

8

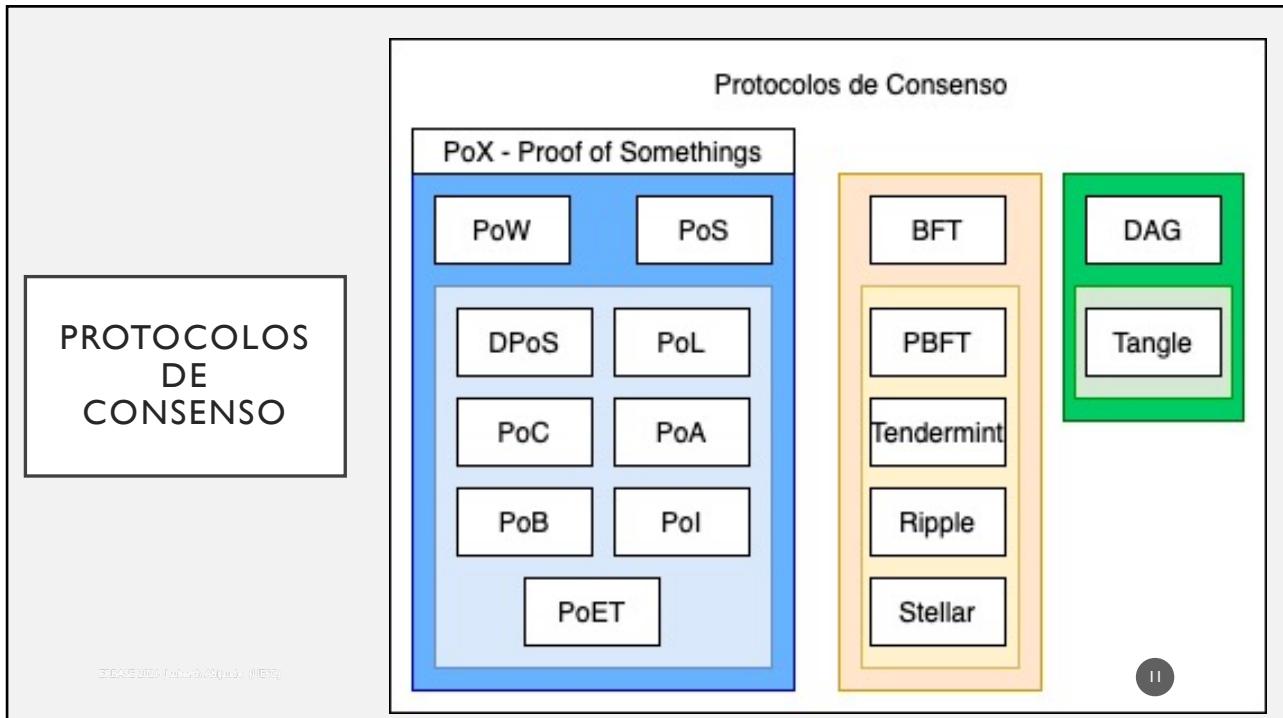
8



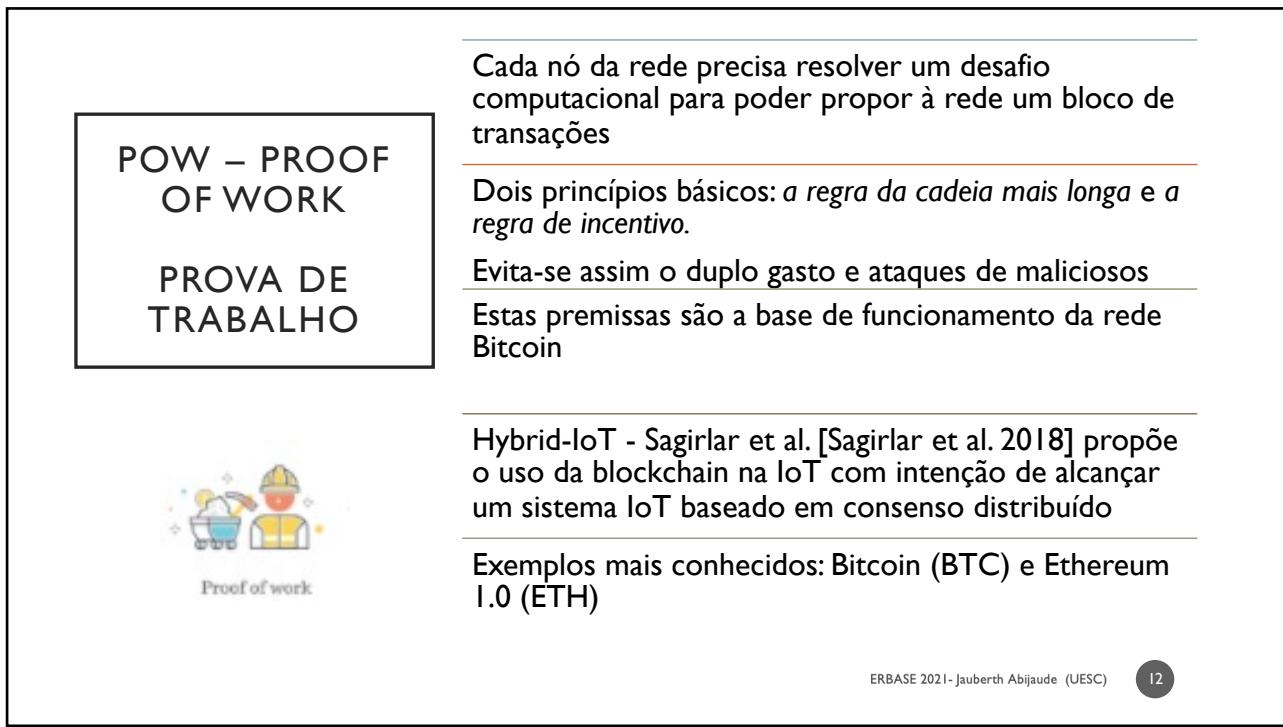
9



10



11



12

**BFT – PROTOCOLOS BYZANTINOS TOLERANTES A FALHAS**

**PBFT – PRACTICAL BYZANTINE FAULT TOLERANCE**

Garante Acordo num sistema onde os processos podem falhar de forma arbitrária: Problema Gerais Bizantinos [Lamport 1982], se qtde falhos é menor que  $1/3$

PBFT é o primeiro algoritmo prático a tolerar falhas bizantinas, considerando ambientes assíncronos

O *BFT-Smart* é oferecido pelo Hyperledger Fabric como camada de acordo e validação

ERBASE 2021- Jauberth Abijaude (UESC)

13

13

**POS – PROOF OF STAKE**

**PROVA DE PARTICIPAÇÃO**



Considera a porcentagem do número total de moedas (ou recursos) que um nó envolvido na competição detém, e eventualmente considera o tempo que o nó leva com o montante de moedas (ou recursos) para estabelecer uma porcentagem de direito de participação no consenso.

Elimina o processo exaustivo de resolução do *puzzle* criptográfico.

Os usuários com mais moedas por um longo período têm maior possibilidade de serem selecionados pelo sistema para gerar o próximo bloco.

Utilizado pelas plataformas Cardano (ADA), Algorand (ALGO) e Ethereum 2.0 (ETH), por exemplo

ERBASE 2021- Jauberth Abijaude (UESC)

14

14

## MODELOS PARA APLICAÇÕES BLOCKCHAIN

### SIDECHAINS

- Permitem ao desenvolvedor anexar recursos à rede principal através de uma cadeia separada
- Permanecem isoladas, e caso algum problema ocorra na sidechain, apenas ela fica comprometida, não interrompendo a cadeia principal.
  - Lisk Restaurante
    - Permite pedir comida online através de uma sidechain com transações personalizadas para restaurantes
  - Loom
    - Rodar DApps e jogos em sidechains conectados à Ethereum
  - Liquid
    - Sidechain comercial que permite a movimentar fundos entre as exchanges.
  - Root Stock
    - Sidechain de código aberto atrelada à rede principal do Bitcoin para a execução de contratos inteligentes.

### CONTRATOS INTELIGENTES

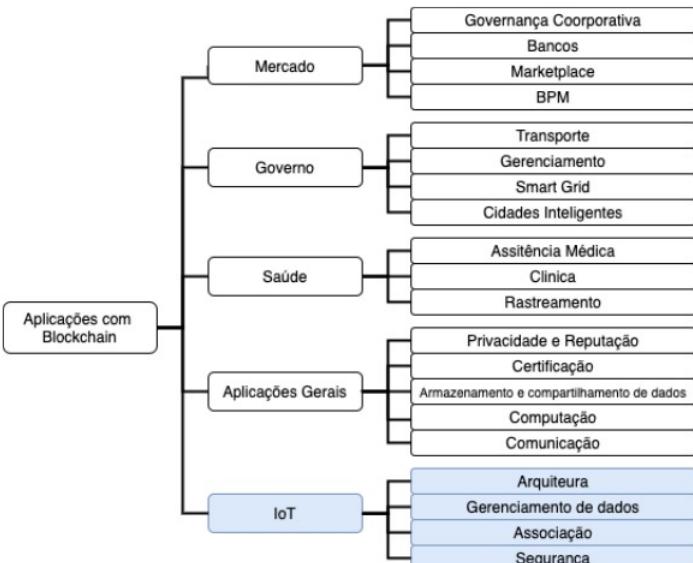
- Programas de computador representando interesses contratuais distintos executados na blockchain.
- Detalhados mais adiante

ERBASE 2021 - Jauberth Abijaude (UESC)

29

29

## APLICAÇÕES BLOCKCHAIN



**Figura 4.8. Classificação de aplicações que usam blockchain. Fonte:[W30 et al. 2019]**

30

## IOT

ERBASE 2021- Jauberth Abijaude (UESC)

31

31

## IOT

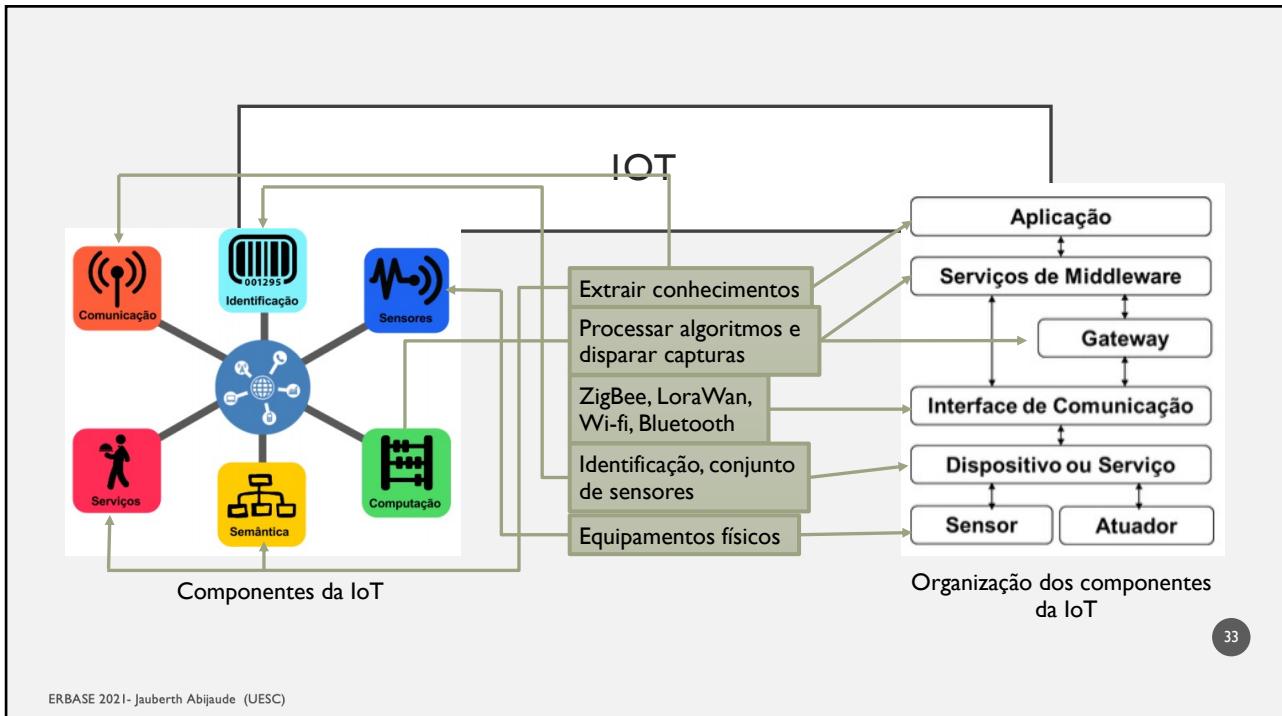
Vamos apresentar neste seção:

- IoT;
- Características
- Arquitetura para IoT
- Arquitetura e aplicações Blockchain e IoT

ERBASE 2021- Jauberth Abijaude (UESC)

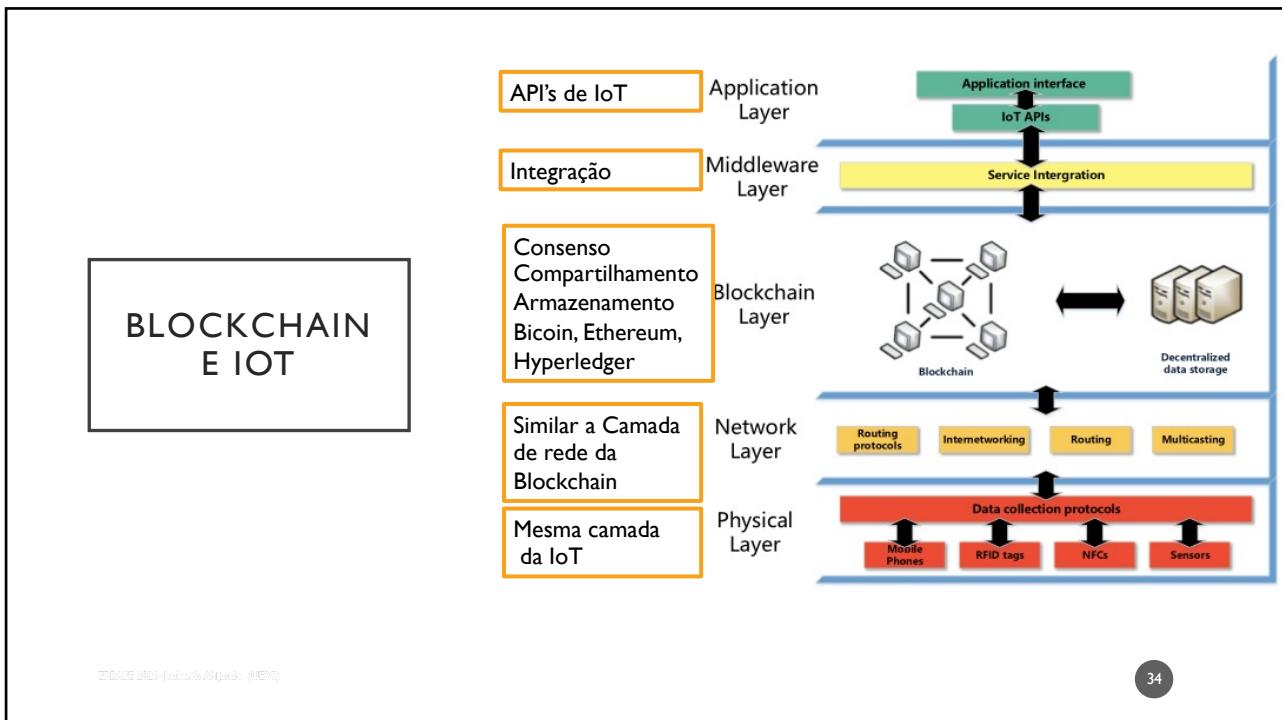
32

32



33

33



34

34

## ARQUITETURAS BLOCKCHAIN IOT

**Tabela 4.1. Arquiteturas de Blockchain-IoT. Fonte [Lao et al. 2020]**

Blockchain-IoT	Aplicação	Middleware	Blockchain	Rede	Física	Classe
Smart Home	Smart Home App	Gerenciamento	Blockchain comercial	P2P	Dispositivos inteligentes	Aplicação específica
LO3 Energy	Energy Shopping	Energy Token	Blockchain pública	Rede de baixa latencia	Painéis solares	Aplicação específica
Slock.it	DApp	Não usa	Ethereum	Rede comercial	Travas eletrônicas	Aplicativo específica
Hybrid-IoT	Aplicação IoT	Plataforma Hybrid-IoT	POW blockchain, BFT blockchain	P2P	Sensores	Aplicativo como serviço
PBIoT	DApp	C	Blockchain	P2P	Dispositivos de IoT	Aplicativo como serviço
JD.COM	JD.com	Blockchain Gateway	BFT blockchain	P2P	Dispositivos de IoT	Aplicativo como serviço
IoT Data Service Framework	Aplicação para Usuários	Framework	Ethereum	P2P	Dispositivos de IoT	Aplicativo como serviço
IoT Chain	Acesso com Autorização	Framework	Ethereum	Rede Comercial	Dispositivos de IoT	Aplicativo como serviço

ERBASE 2021- Jaubert Abijaude (UESC)

35

## APlicações Blockchain e IoT

- Segundo [Lao et al. 2020] as aplicações de blockchain e IoT podem ser categorizadas:

**Pagamentos Digitais**

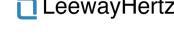
Atualmente blockchains como Bitcoin e Ethereum podem ser utilizadas em smartphones




ethereum

**Serviços de Contratos Inteligentes**

Sistemas de automação e controle com base na IoT, eliminando a terceira parte de confiança [Christidis and Devetsikiotis 2016]

LeewayHertz

**Armazenamento**

Aplicativos de armazenamento de dados que vêm a blockchain como um banco de dados seguro e distribuído



FACTOM

ERBASE 2021- Jaubert Abijaude (UESC)

36

## PLATAFORMA ETHEREUM E CONTRATOS INTELIGENTES

ERBASE 2021- Jauberth Abijaude (UESC)

37

37

## PLATAFORMA ETHEREUM E CONTRATOS INTELIGENTES

- Plataforma Ethereum
  - Redes Ethereum
  - Transações
  - Consenso
- Contratos Inteligentes

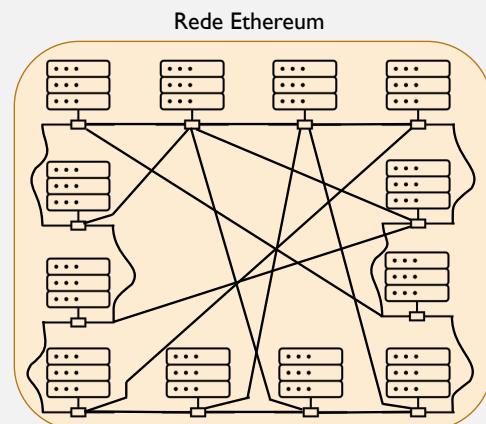
38

38

## REDE ETHEREUM

### Características

- Usada para transferência de dinheiro digital
- Existe mais de uma rede Ethereum
- Executa programas chamados de smart contracts
- Cada nó é uma máquina que possui um cliente Ethereum rodando
- Qualquer um pode rodar um nó – associação de mineradores
- Cada nó pode conter uma cópia completa da blockchain



ERBASE 2021- Jauberth Abijaude (UESC)  
Simpósio Brasileiro de Sistemas de Informação - Minicurso Blockchain, Contratos Inteligentes e Sistemas Web: Teoria e Prática

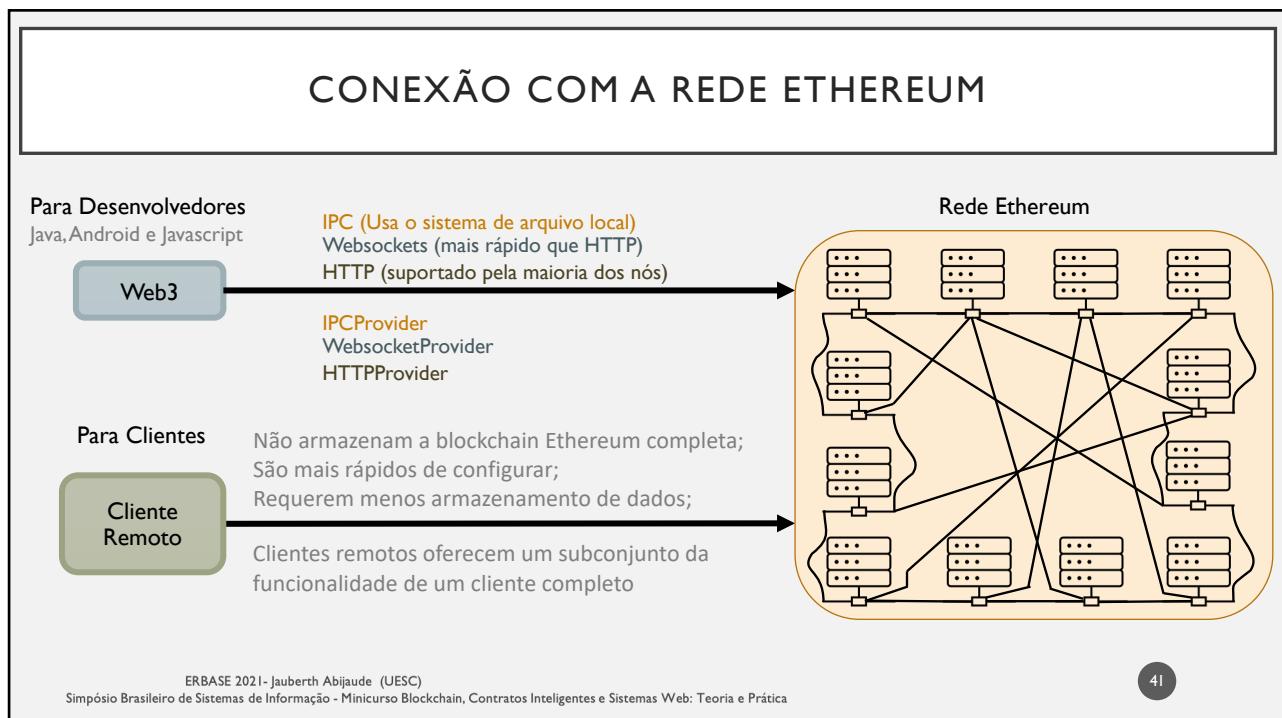
39

## ESTÁGIOS DE DESENVOLVIMENTO

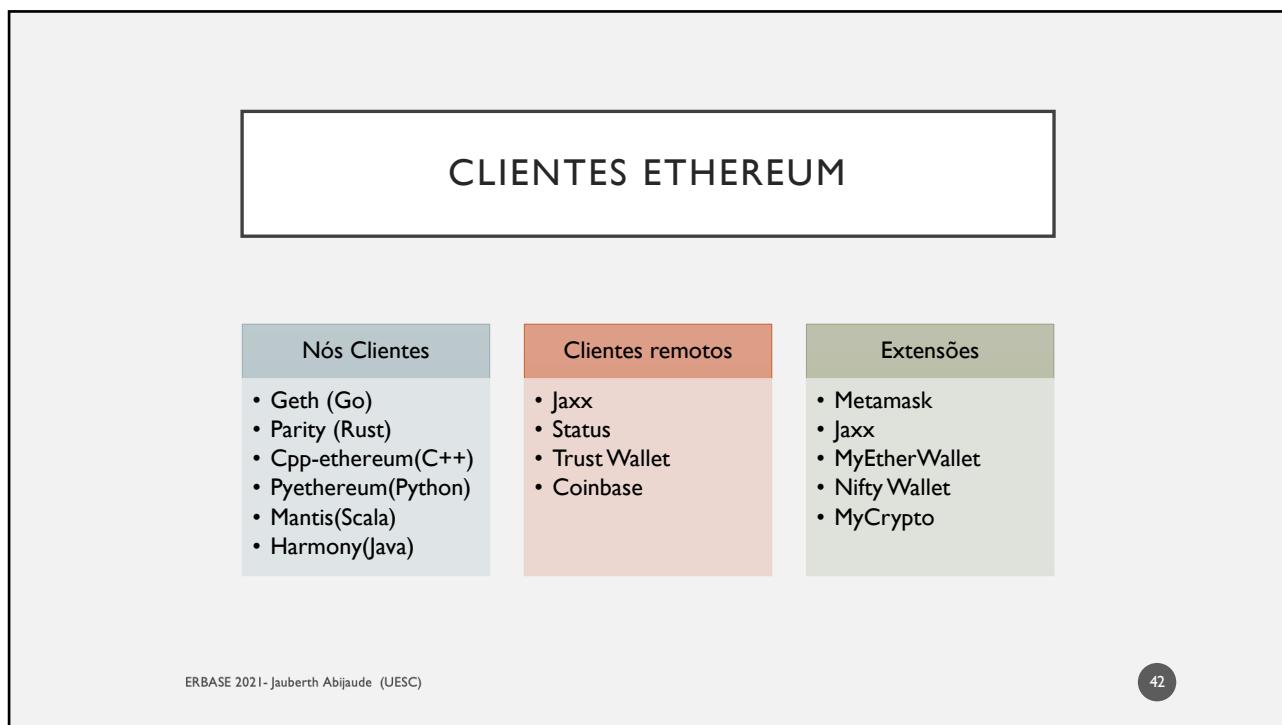
- **Bloco #0 Frontier - O estágio inicial do Ethereum, durando de 30 de julho de 2015 a março de 2016.**
- Bloco #200.000 Ice Age - Um hard fork para introduzir um aumento exponencial de dificuldade, preparando a transição para o PoS.
- Bloco #1.150.000 Homestead - O segundo estágio do Ethereum, lançado em março de 2016.
- **Bloco #1.192.000 DAO - Um hard fork que reembolsou as vítimas do contrato DAO hackeado e fez com que o Ethereum e o Ethereum Classic se dividissem em dois sistemas concorrentes.**
- Bloco #2.463.000 Tangerine Whistle - Uma hard fork para alterar o cálculo do gás para certas operações de E/S e para limpar o estado acumulado de um ataque de negação de serviço (DoS) que explorou o baixo custo do gás dessas operações.
- Bloco #2.675.000 Spurious Dragon - Um hard fork para lidar com mais vetores de ataque DoS e outra limpeza de estado. Além disso, um mecanismo de proteção contra ataques de repetição.
- **Bloco #4.370.000 Byzantium - Recompensas de mineração é reduzida de 5 para 3 ETH.**
- **Bloco #7.280.000 Constantinople – Mudança significativa na rede, entre elas, ajustes para a implementação do POS e ajustes no custo do gas. (2019).**
- Bloco #12.244.000 Berlim - A atualização Berlim otimizou o custo do gás para certas ações de EVM e aumentou o suporte para vários tipos de transação.

ERBASE 2021- Jauberth Abijaude (UESC)

40



41



42

## GASPRICE X GASLIMIT

- O gas não é ether, é uma moeda separada usada para pagamento das transações na rede
- Possui cotação própria em relação ao ether

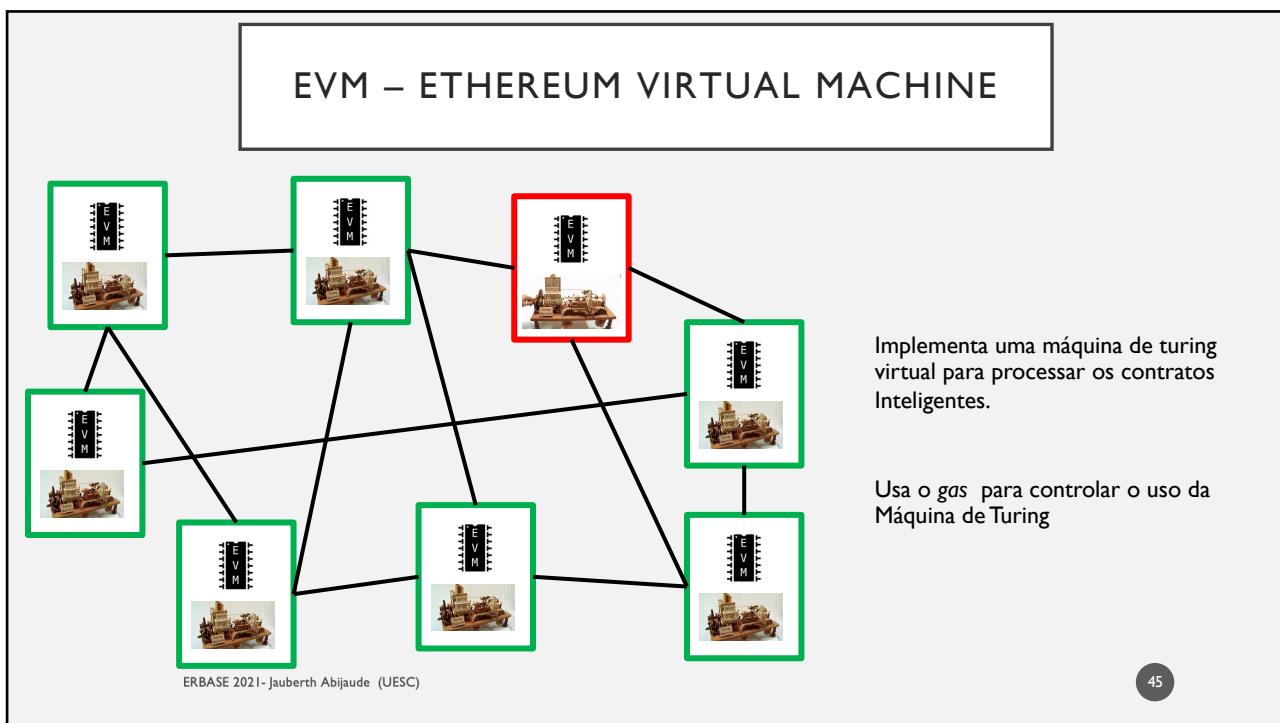
**GasLimit** - indica qual o limite de gas a ser consumido pela transação.

**GasPrice** - permite que o emissor da transação defina o preço que está disposto a pagar para adquirir o gas.

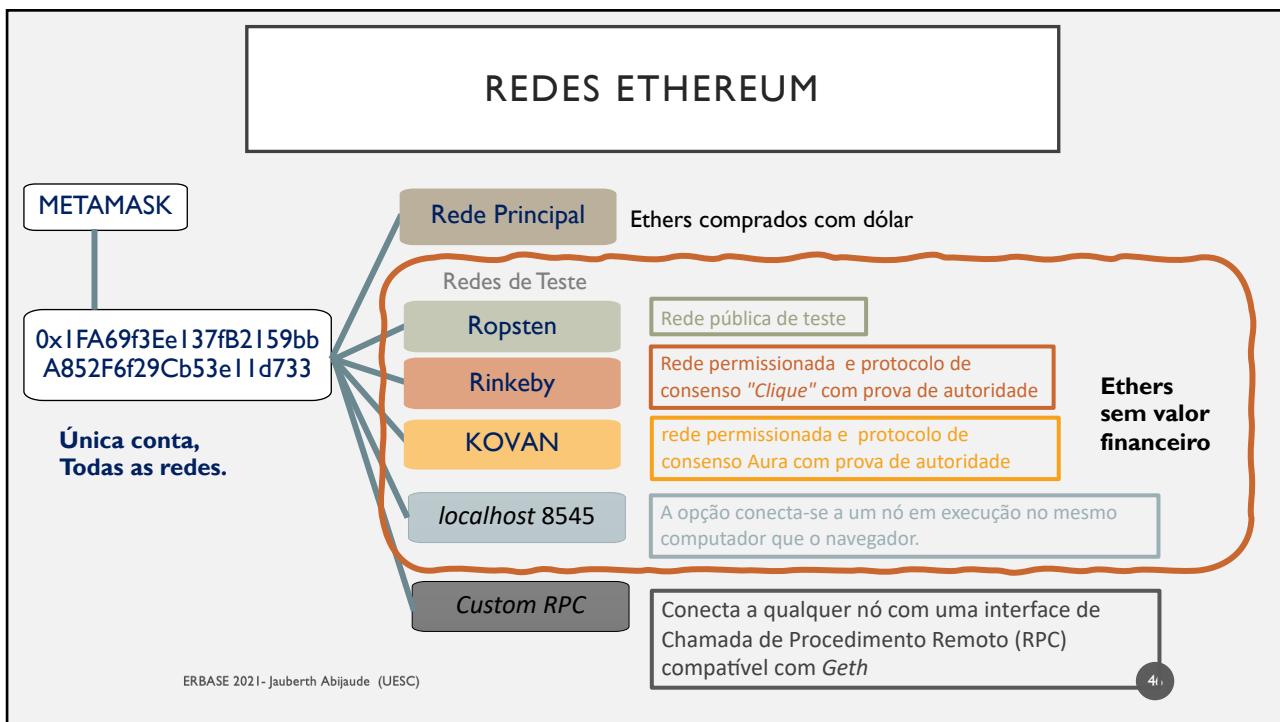
Gas Limit (Units)	21000
Gas Price (GWEI)	7.5
Total	3.000157 ETH

ERBASE 2020 - Jauberth Abijaude (UESC)

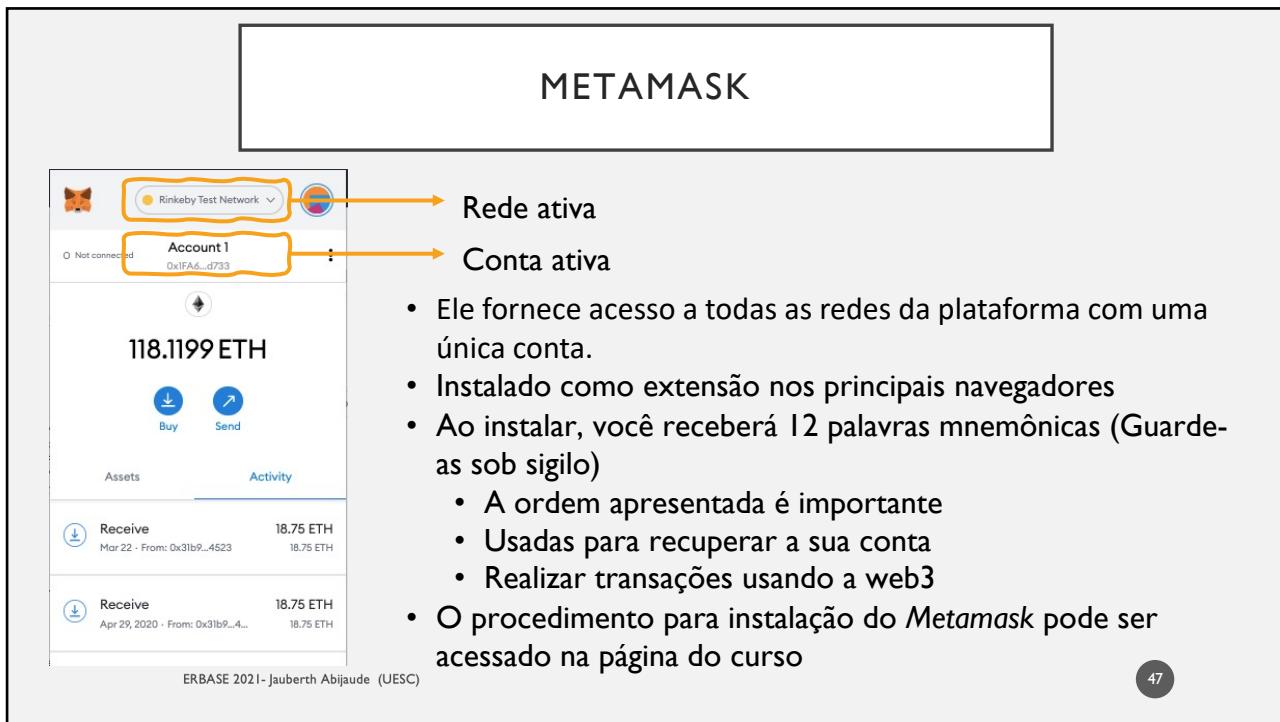
44



45



46



47

## ESTRUTURA DA TRANSAÇÃO

Campo	Descrição
nonce	Número de sequência, emitido pela origem, usado para evitar a reprodução da mensagem
to	Endereço para onde será enviada uma quantidade de ether
value	Quantidade de ether a ser enviada
GasPrice	Valor que será pago por unidade de gas para que a transação seja processada
GasLimit	Quantidade de GAS que esta transação pode consumir
v	Peças criptográficas usadas para a validação do bloco.
r	
s	

Acesse <https://andersbrownworth.com/> para ver um exemplo

ERBASE 2021- Jauberth Abijaude (UESC)

48

48

## DATA E VALUE

Apenas consome gas

```
nonce: 7
to: 0x1FA69f3Ee1378B1159b0A852F6f29Cb53e11d833
value:
gasPrice: 12,3
gasLimit: 30000
data:
```

Indica uma invocação

```
nonce: 7
to: 0x1FA69f3Ee1378B1159b0A852F6f29Cb53e11d833
value:
gasPrice: 12,3
gasLimit: 30000
data: batimentos(80)
```

Indica um pagamento

```
nonce: 7
to: 0x1FA69f3Ee1378B1159b0A852F6f29Cb53e11d833
value: 2,3
gasPrice: 12,3
gasLimit: 30000
data:
```

Indica uma invocação e um pagamento

```
nonce: 7
to: 0x1FA69f3Ee1378B1159b0A852F6f29Cb53e11d833
value: 0,5
gasPrice: 12,3
gasLimit: 30000
data: pag_exame()
```

ERBASE 2021- Jauberth Abijaude (UESC)

51

51

## CONTRATOS INTELIGENTES

Idealizados por Nick Szabo representam "um conjunto de promessas, especificado em formato digital, incluindo protocolos nos quais as partes cumprem estas promessas"

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity >=0.7.4;
3
4 contract Inbox{
5     string public message;
6     constructor(string memory initialMessage){
7         message = initialMessage;
8     }
9     function setMessage(string memory newMessage) public{
10        message = newMessage;
11    }
12    function getMessage() public view returns(string memory){
13        return message;
14    }
15 }
```

Rede Ethereum

52

ERBASE 2021- Jauberth Abijaude (UESC)

52

## CONTRATOS INTELIGENTES

---

CIs são simplesmente programas de computador. A palavra contrato não tem significado legal neste contexto.

---

Eles são imutáveis, por que uma vez implementado em uma rede Ethereum, o código não pode ser alterado nem substituído

---

É preciso prever uma função de autodestruição para apagá-lo

---

São determinísticos, pois o resultado de sua execução é sempre o mesmo para todos os que o executam, conservando-se o contexto no momento da execução.

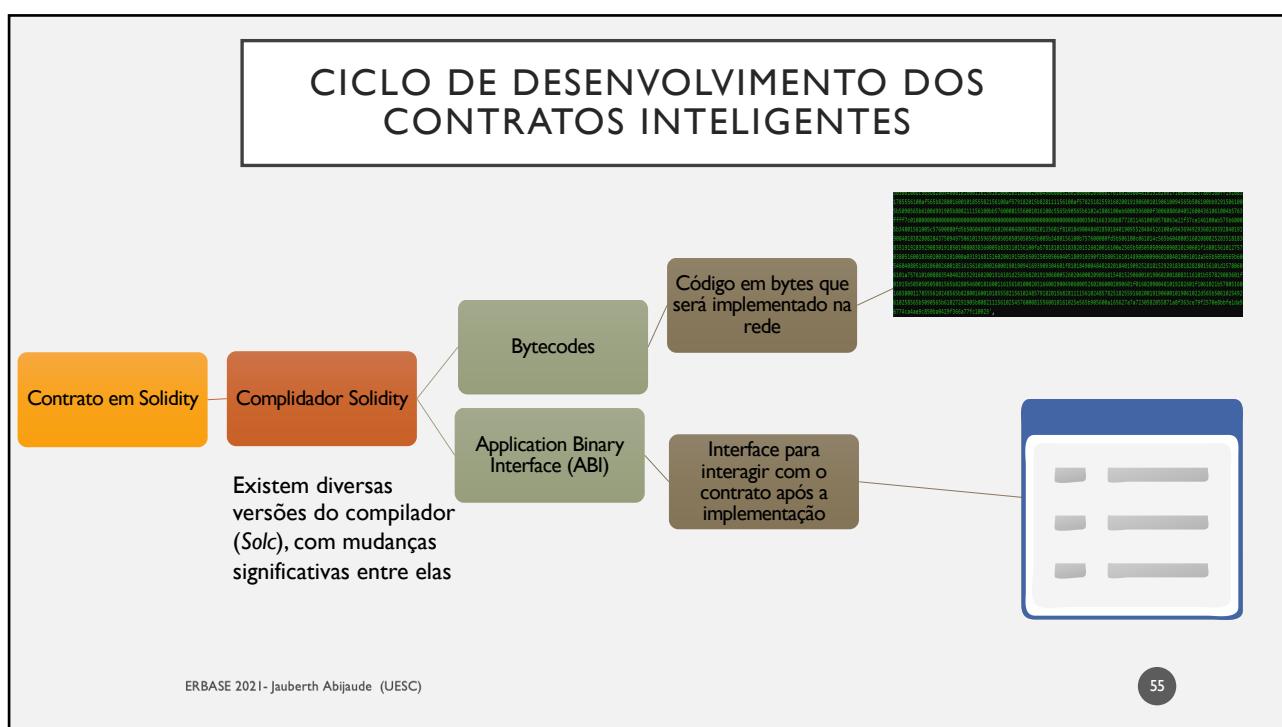
---

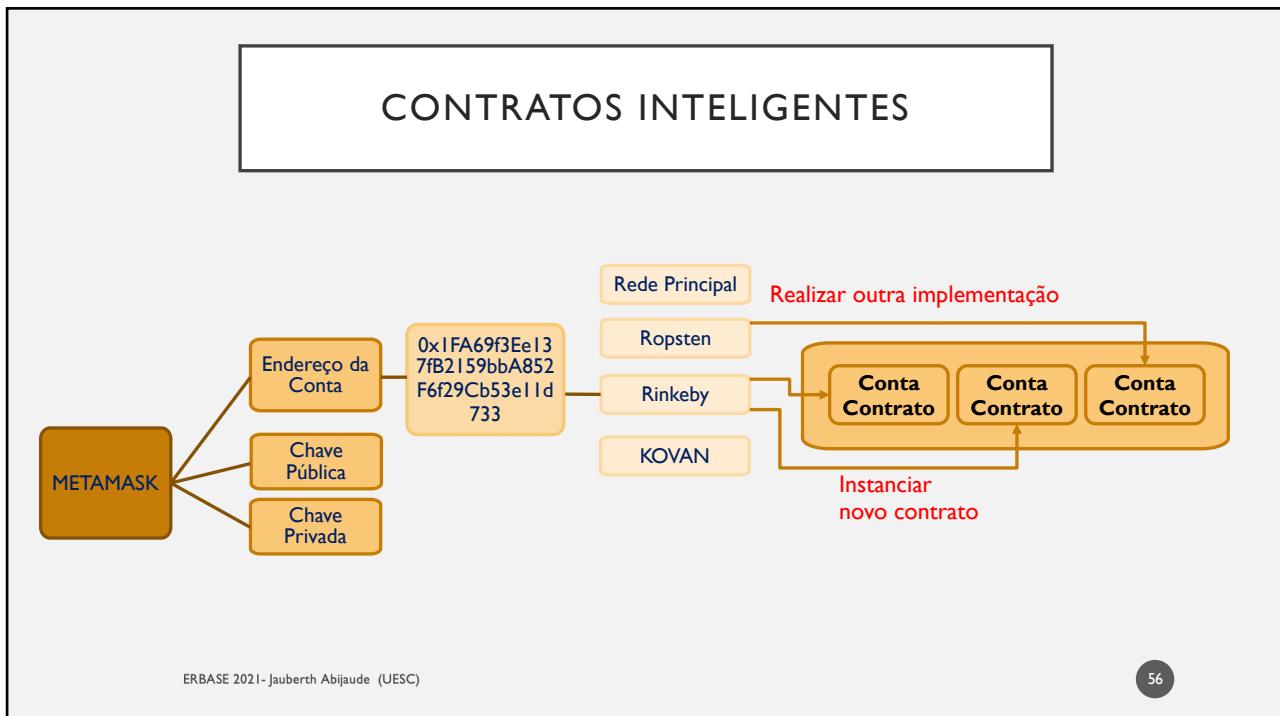
Linguagens de programação: são LLL, Serpent, Vyper, Bambu e Solidity

ERBASE 2021- Jauberth Abijaude (UESC)

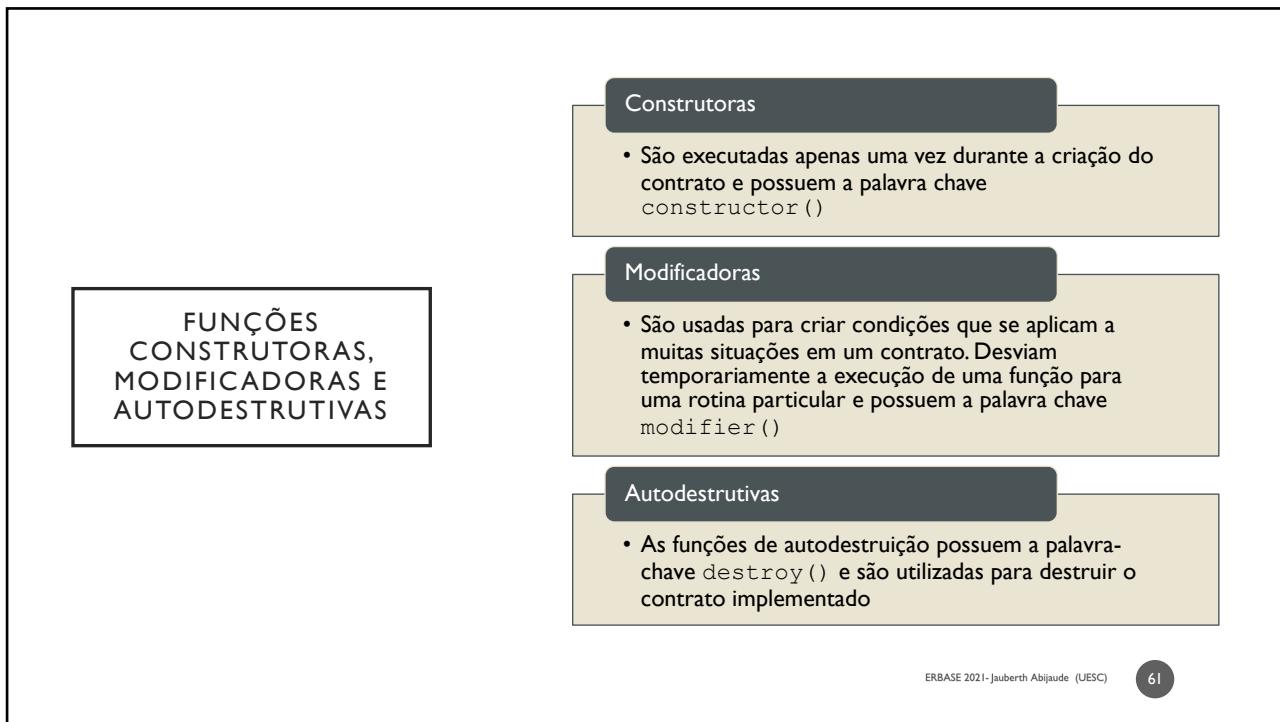
53

53





56



61

## DESENVOLVIMENTO DE CONTRATOS INTELIGENTES

ERBASE 2021- Jauberth Abijaude (UESC)

66

66

## DESENVOLVIMENTO DE CONTRATOS INTELIGENTES

- Ambientes de desenvolvimento
- Construindo um contrato inteligente

67

67

## REMIX X AMBIENTE LOCAL

**REMIX**

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.7.4;
3
4 contract Inbox{
5     string public message;
6     constructor(string memory initialMessage){
7         message = initialMessage;
8     }
9     function setMessage(string memory newMessage) public{
10        message = newMessage;
11    }
12    function getMessage() public view returns(string memory){
13        return message;
14    }
15 }
```

**AMBIENTE LOCAL**

```

graph TD
    Nodejs((Node.js)) --- solc((solc))
    Nodejs --- trufflehdwprovider((truffle-hdwallet-provider))
    Nodejs --- mocha((mocha))
    Nodejs --- ganachecli((ganache-cli))
    Nodejs --- web3((web3))

```

ERBASE 2021- Jauberth Abijaude (UESC)

68

68

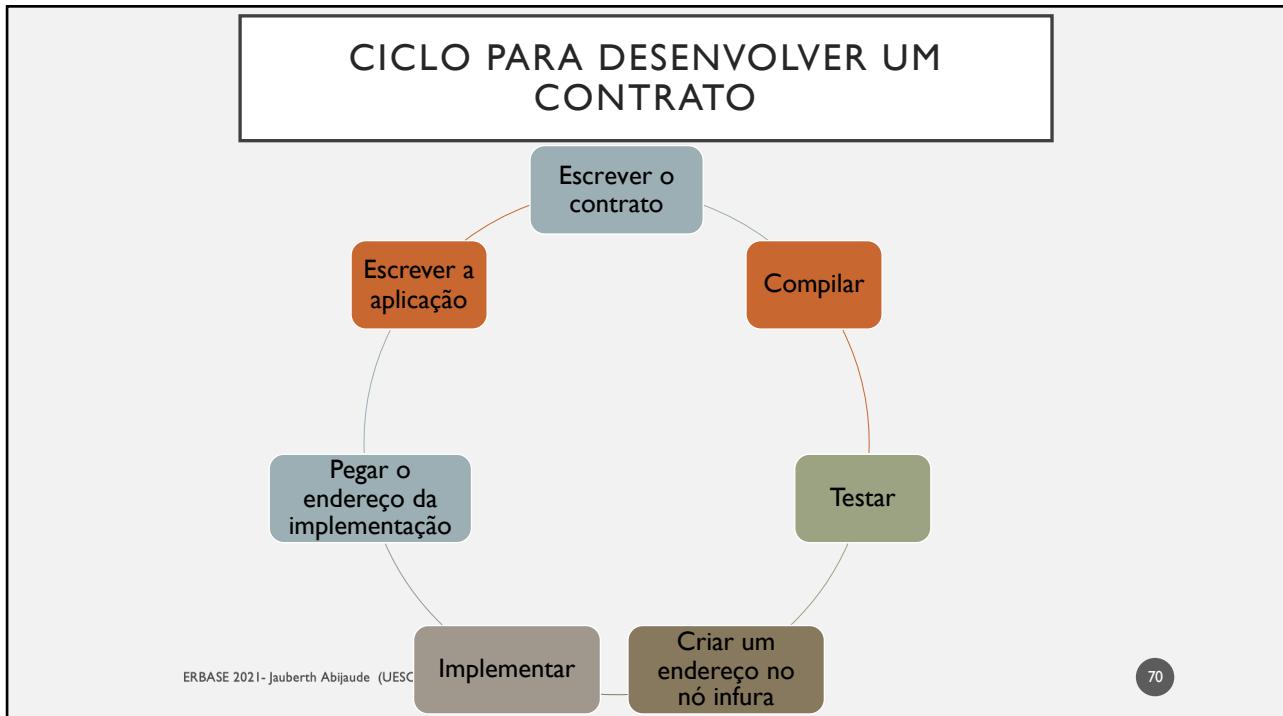
## ACIONANDO UM PROJETO

The screenshot shows the Infura interface for the 'Loteria2' project. On the left, there's a sidebar with 'ETHEREUM' selected, showing 'ETH 2' and 'FIREON' options. The main area has tabs for 'REQUESTS', 'TRANSACTIONS', and 'SETTINGS'. Under 'SETTINGS', there are sections for 'KEYS', 'SECURITY', and 'PER SECOND REQUESTS RATE-LIMITING'. The 'KEYS' section shows a 'PROJECT ID' (2656f044b5b64868b84430a43871f80f) and a 'PROJECT SECRET' (6ea238ea20e44d30872b17a41f6d214d). The 'SECURITY' section includes 'PROJECT SECRET REQUIRED' (unchecked), 'JWT REQUIRED' (unchecked), and fields for 'PER DAY TOTAL REQUESTS' (set to 1000). The 'PER SECOND REQUESTS RATE-LIMITING' section has a field set to 100. At the bottom, there are fields for 'JWT PUBLIC KEY NAME' (Production key) and 'JWT PUBLIC KEY'.

ERBASE 2021-Jauberth Abijaude (UESC)

69

69



70

**PÁGINA DO MINICURSO**

- <https://github.com/lifuesc/erbase2021>
- Códigos, instruções e material complementar
- Sempre em atualização

CONTRIBUTORS 2 FORKS 0 STARS 0 ISSUES 0 OPEN LICENSE MIT

XX ESCOLA REGIONAL DE COMPUTAÇÃO BAHIA - ALAGOAS - SERGIPE

Realizado por:

Patrocínio:

Minicurso 1 - Blockchain e IoT integrados a Sistemas Web

Autores

- Jauberth W. Abijaude (UFBA, UESC)
- Henrique Serra (UESC)
- Péricles de Lima Sobreira (University of Quebec Outaouais, Cégep de Saint-Hyacinthe)
- Fabiola Greve (UFBA)

A Internet das Coisas agrupa dispositivos capazes de capturar informações e interferir no ambiente, de maneira a obter, gerar e enviar dados em larga escala para sistemas de domínios de aplicações diferentes, tais como agricultura, indústria, comércio e governos. Estes sistemas precisam de uma camada de segurança para garantir, dentre outras características, a irrefutabilidade das transações e a integridade dos dados manipulados. Neste sentido, a integração com a blockchain, através dos contratos inteligentes, atenderia a esta necessidade. A blockchain é uma tecnologia disruptiva que oferece uma rede de confiança digital para a realização de transações entre pares, muitas vezes desconhecidos. Este capítulo apresenta pesquisas recentes na fronteira da IoT com a blockchain; apresenta uma classificação da tecnologia de blockchain em camadas e realiza um estudo amplo sobre as estratégias de consenso e aplicações IoT com blockchain. Ao final, fornece um guia com informações que permitam aos interessados a concepção de treinamentos nesta área, contemplando, inclusive, a realização de exercícios práticos.

Índice dos tutoriais

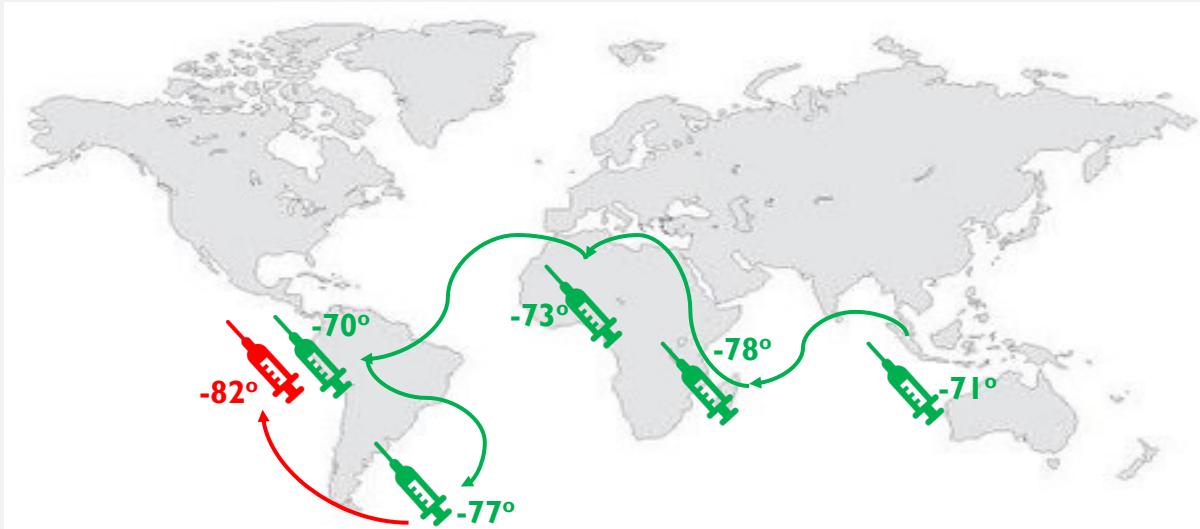
71

## DESENVOLVIMENTO DE DAPPS

ERBASE 2021- Jauberth Abijaude (UESC)

72

72

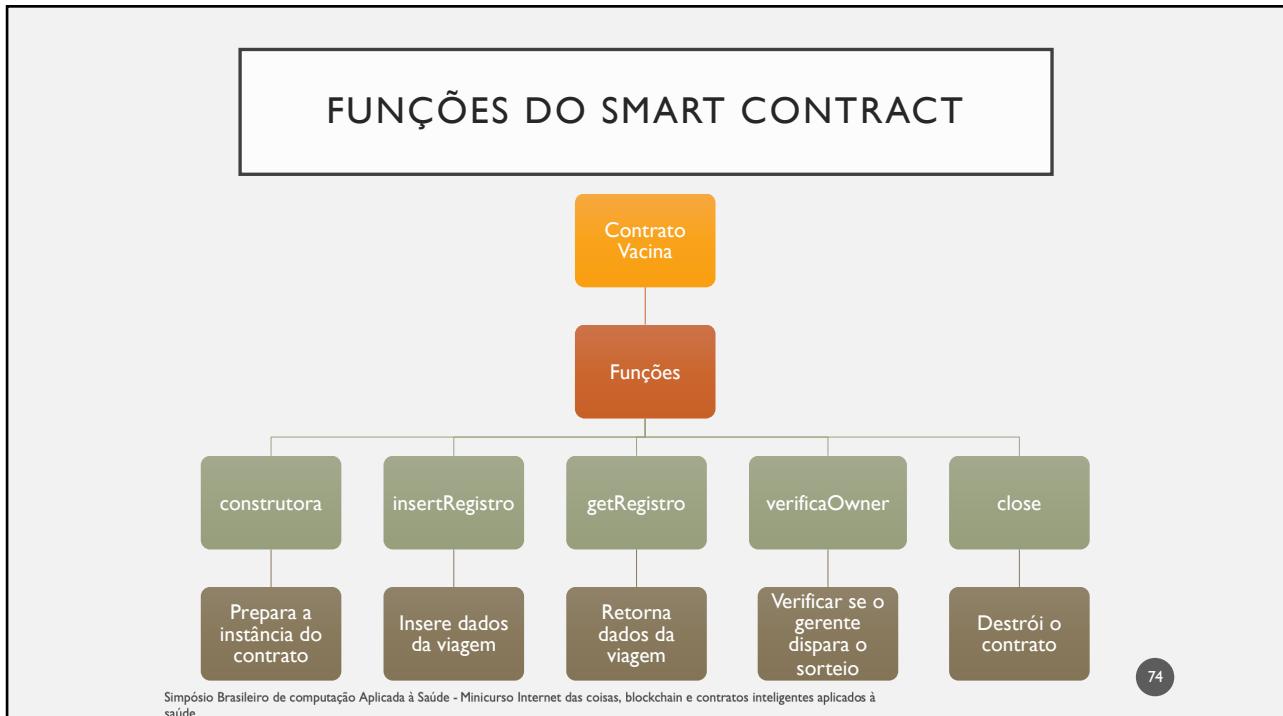


Simpósio Brasileiro de computação Aplicada à Saúde - Minicurso Internet das coisas, blockchain e contratos inteligentes aplicados à saúde

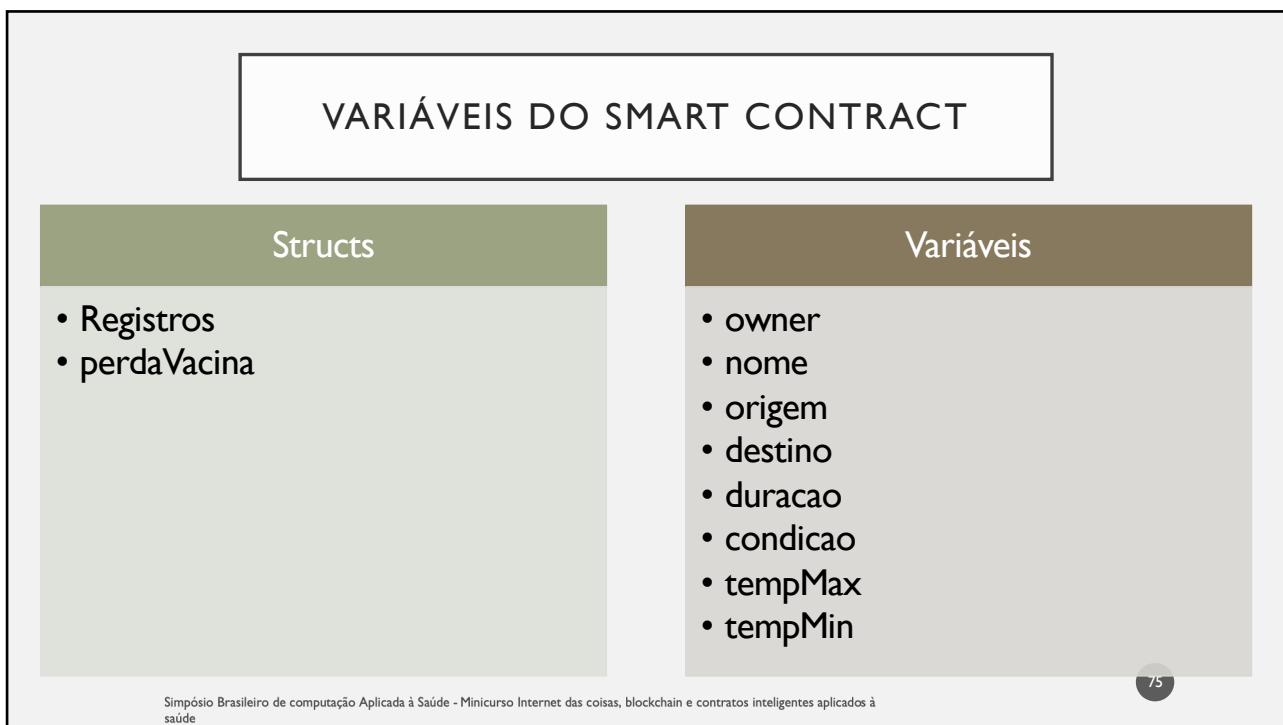
73

73

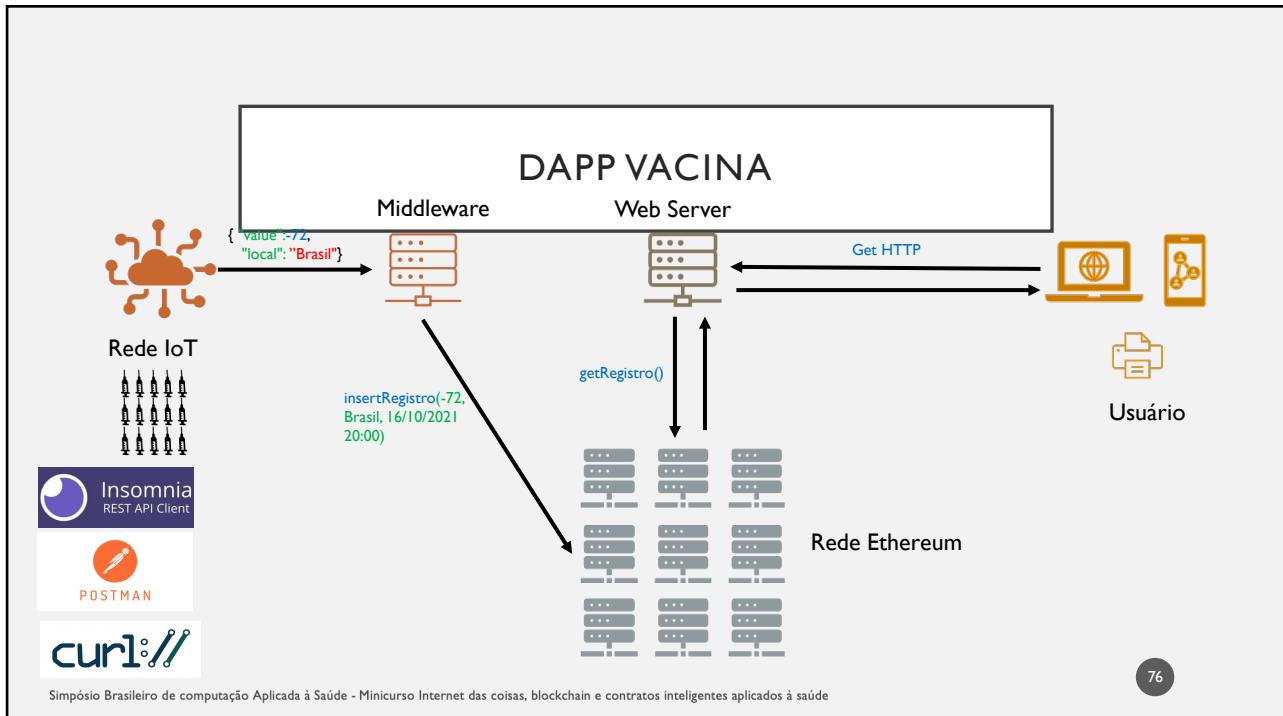
24



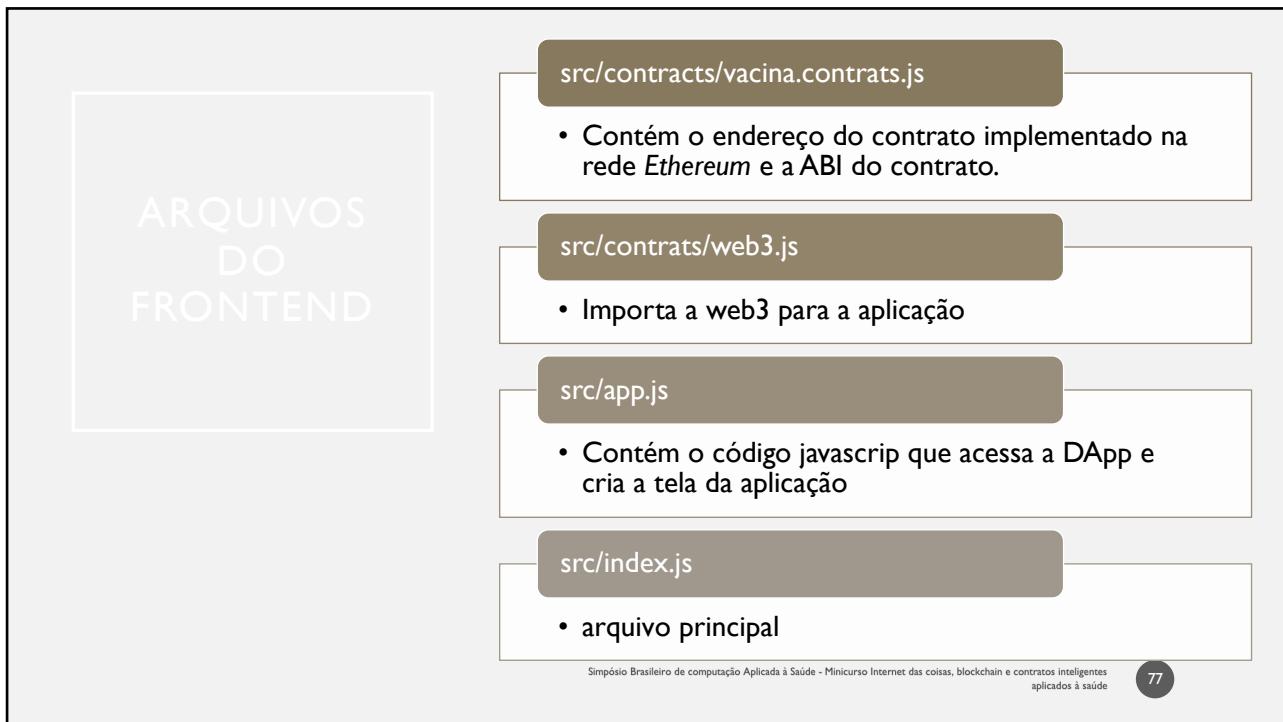
74



75



76



77

## DESAFIOS E PERSPECTIVAS

ERBASE 2021- Jauberth Abijaude (UESC)

78

78

## PERGUNTAS

Dúvidas e mais informações:

**Jauberth Abijaude**  
[jauberth@uesc.br](mailto:jauberth@uesc.br)



ERBASE 2021- Jauberth Abijaude (UESC)

79

79