Blockchain DApps: Construindo uma Aplicação Descentralizada com Ethereum

webminar imasters 2o. Semestre/2018

MICHEL PEREIRA FERNANDES

Chief Engineering do BeyondLabs, centro de inovação da EY

Coordenador de cursos de MBA da FIAP, Mobile Development e Blockchain Technologies[NEW]

Professor dos cursos MBA Fullstack Development e Artificial Intelligence & Machine Learning

br.linkedin.com/in/michelpf/
github.com/michelpf
michelpf@gmail.com
@michelpf

ANTES, POR QUE

?


O MUNDO ESTÁ CADA VEZ MAIS CONECTADO.
MAS CONFIÁVEL?

BANCOS DE DADOS

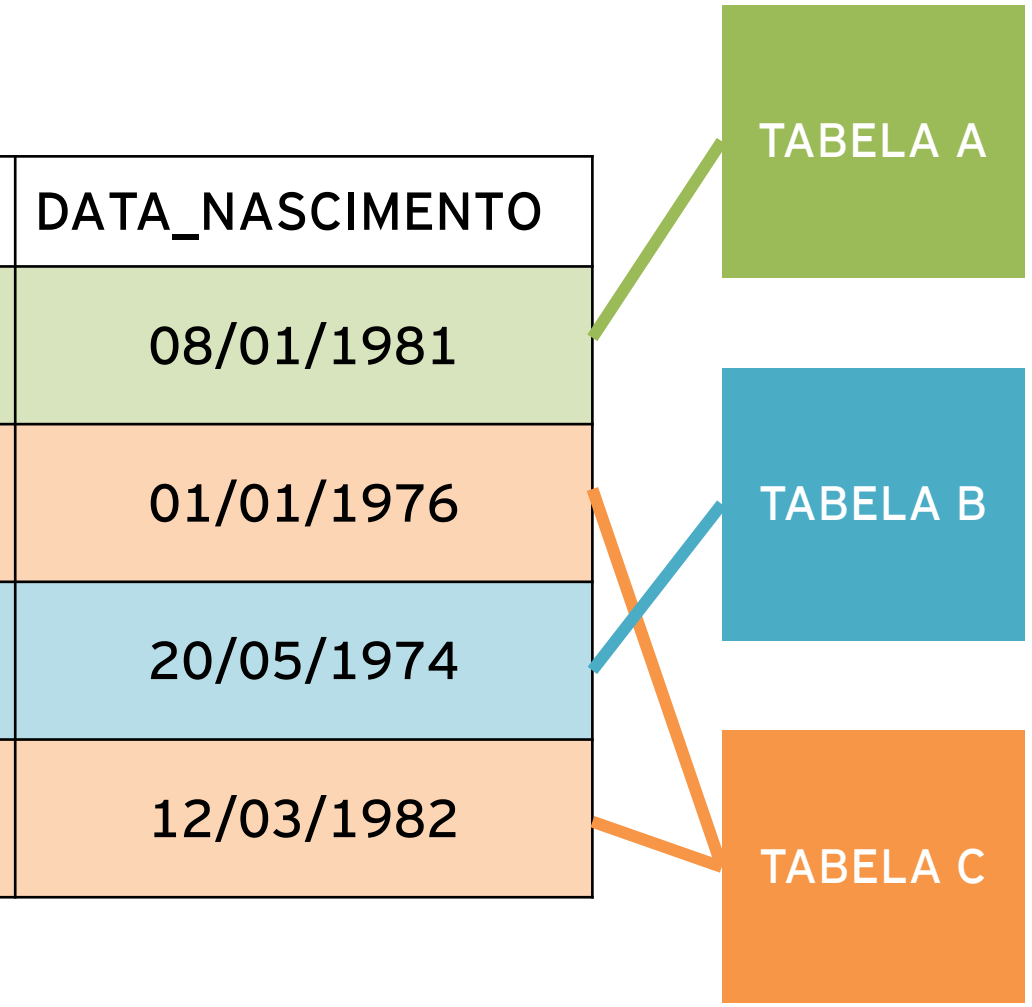
ARMAZENAM QUALQUER TIPO DE INFORMAÇÃO

ESTRUTURADO

ID	PRIMEIRO_NOME	ULTIMO_NOME	DATA_NASCIMENTO
1	MICHEL	FERNANDES	08/01/1981
2	JOÃO	PEDRO	01/01/1976
3	ERNESTO	HENRIQUE	20/05/1974
4	MARIA	DIAS	12/03/1982

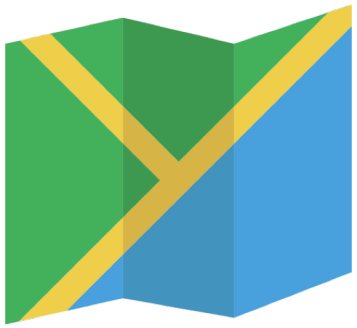
ESTRUTURADO

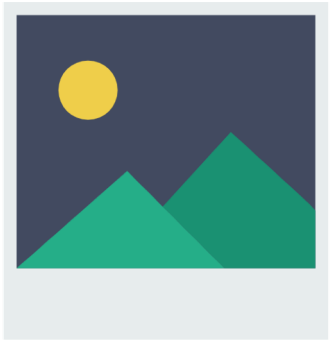
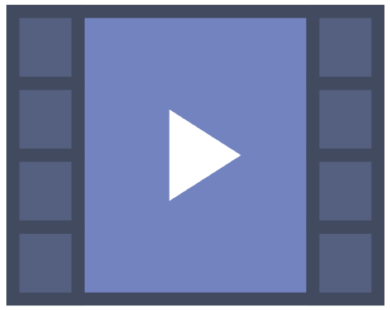
ID	PRIMEIRO_NOME	ULTIMO_NOME	DATA_NASCIMENTO
1	MICHEL	FERNANDES	08/01/1981
2	JOÃO	PEDRO	01/01/1976
3	ERNESTO	HENRIQUE	20/05/1974
4	MARIA	DIAS	12/03/1982



NÃO ESTRUTURADO

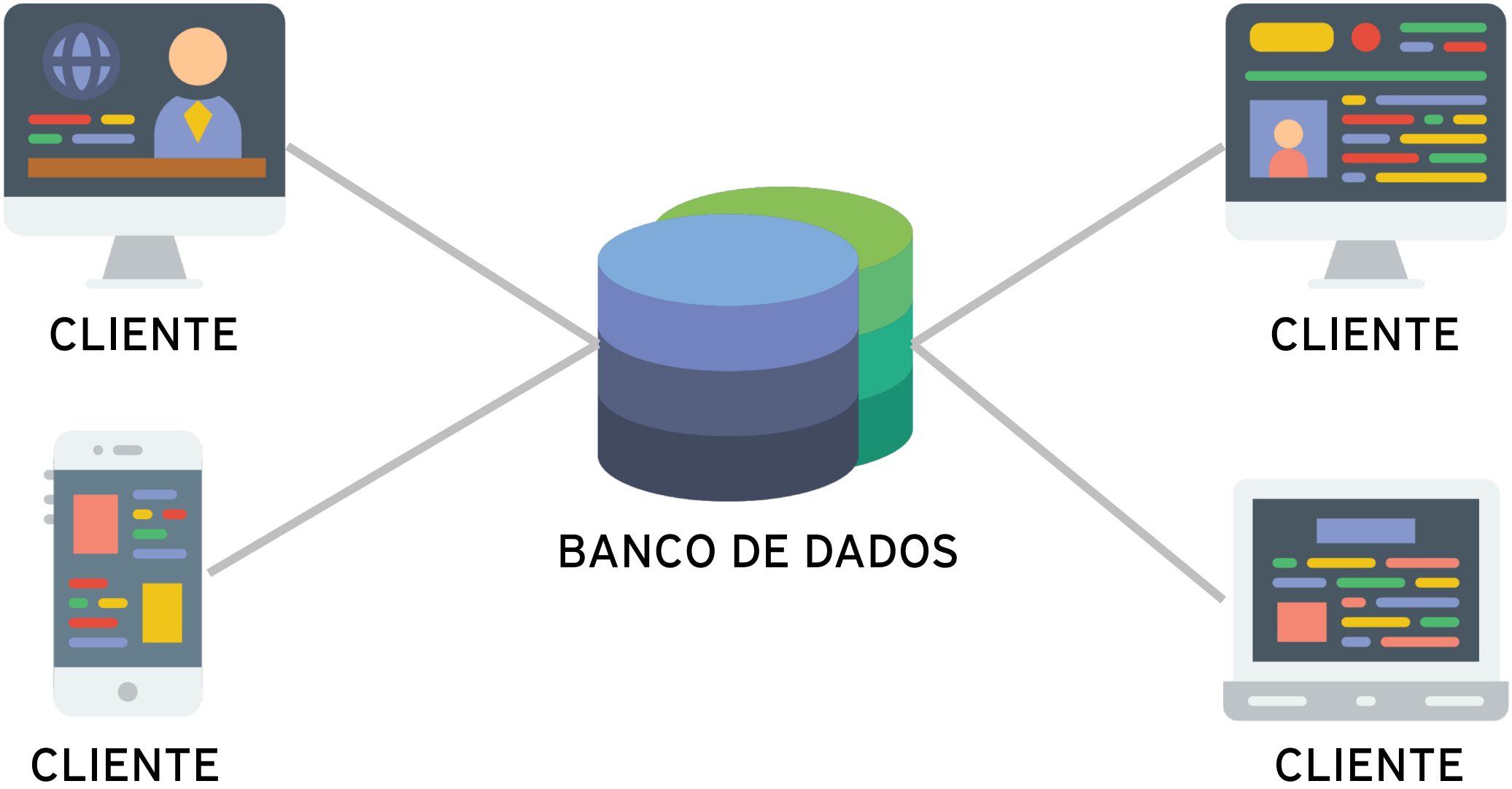
{



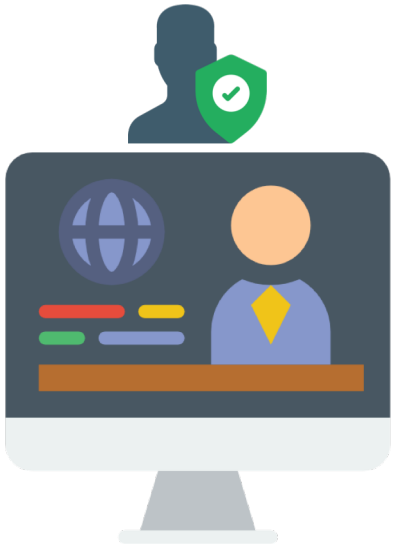

}

TOPOLOGIA CENTRALIZADAS



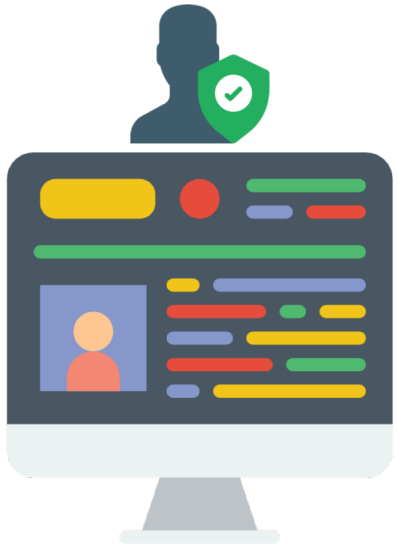
AUTORIDADE CENTRALIZADA

ADMINISTRADOR DO
BANCO DE DADOS

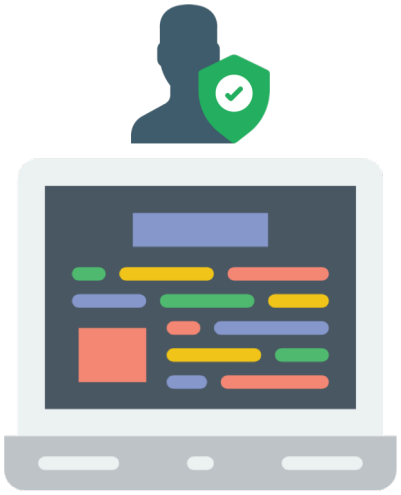


CLIENTE

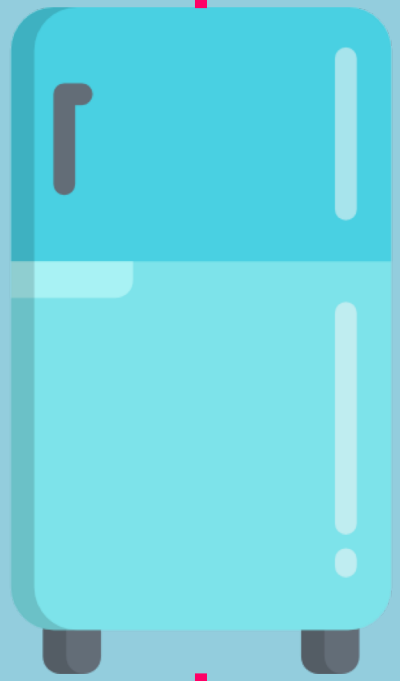
CLIENTE

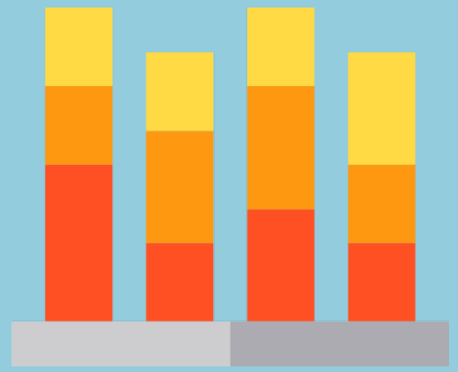


CLIENTE

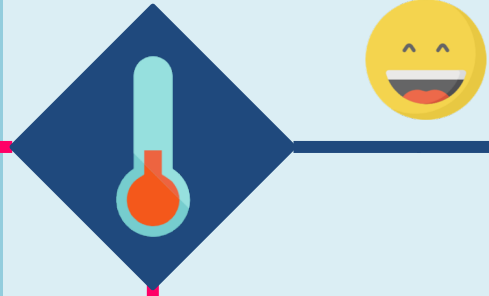


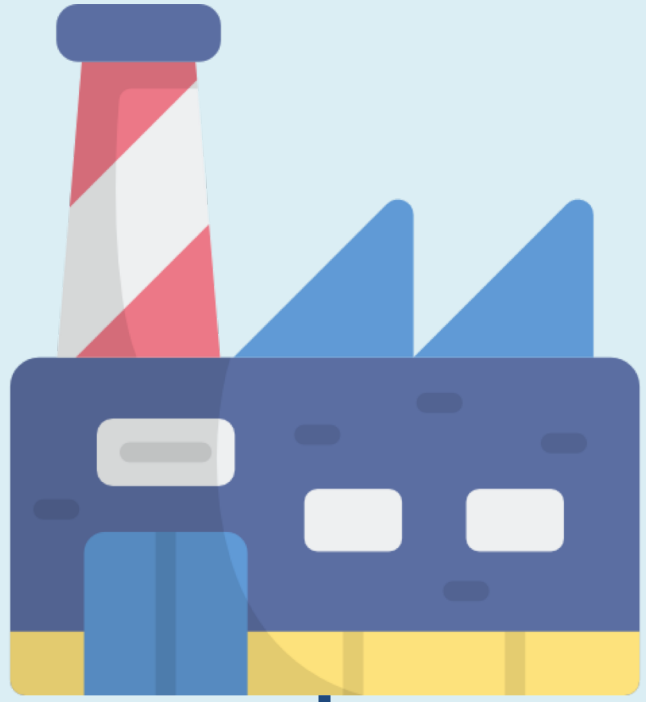
CLIENTE



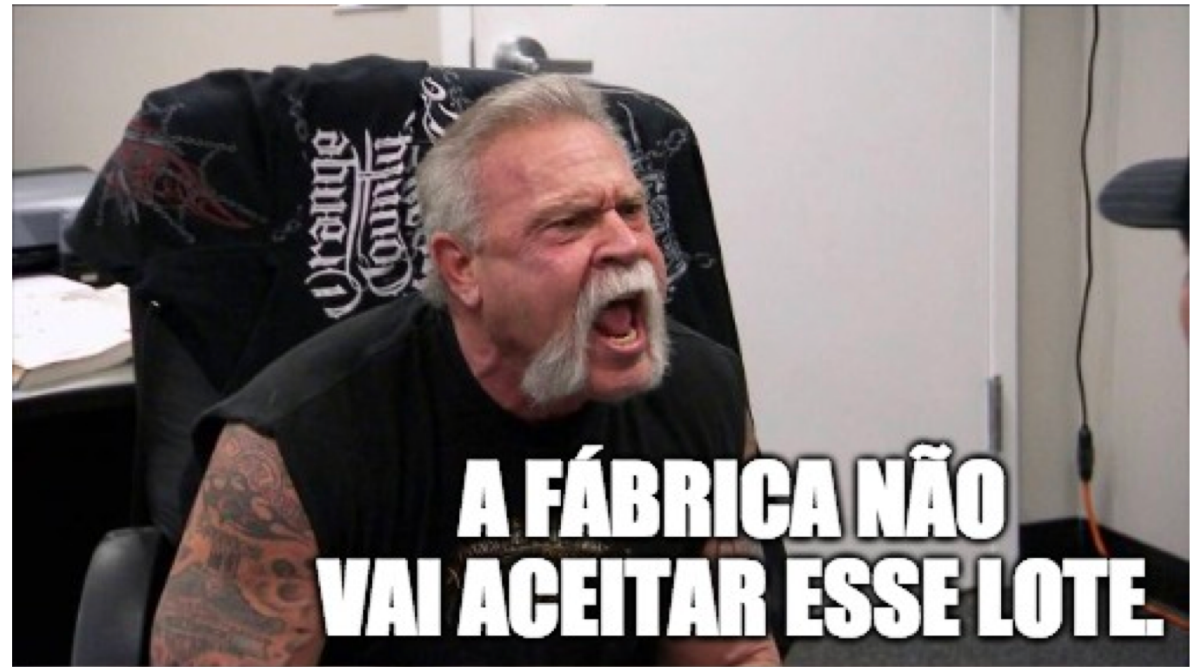


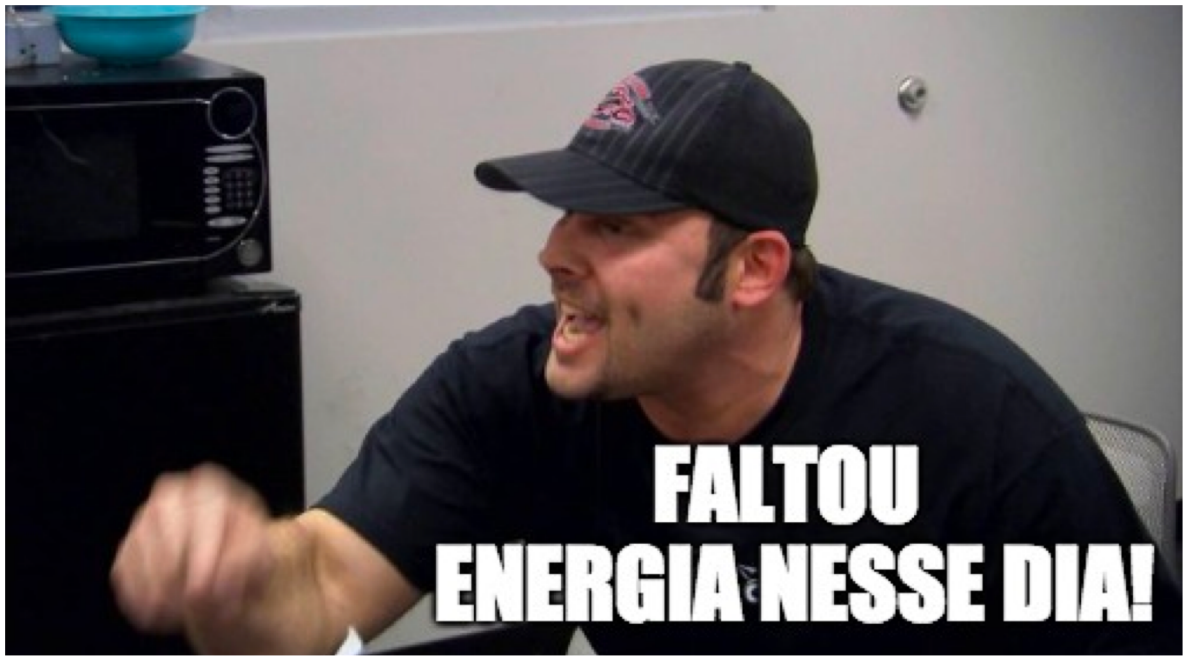
RASTREAMENTO DA TEMPERATURA

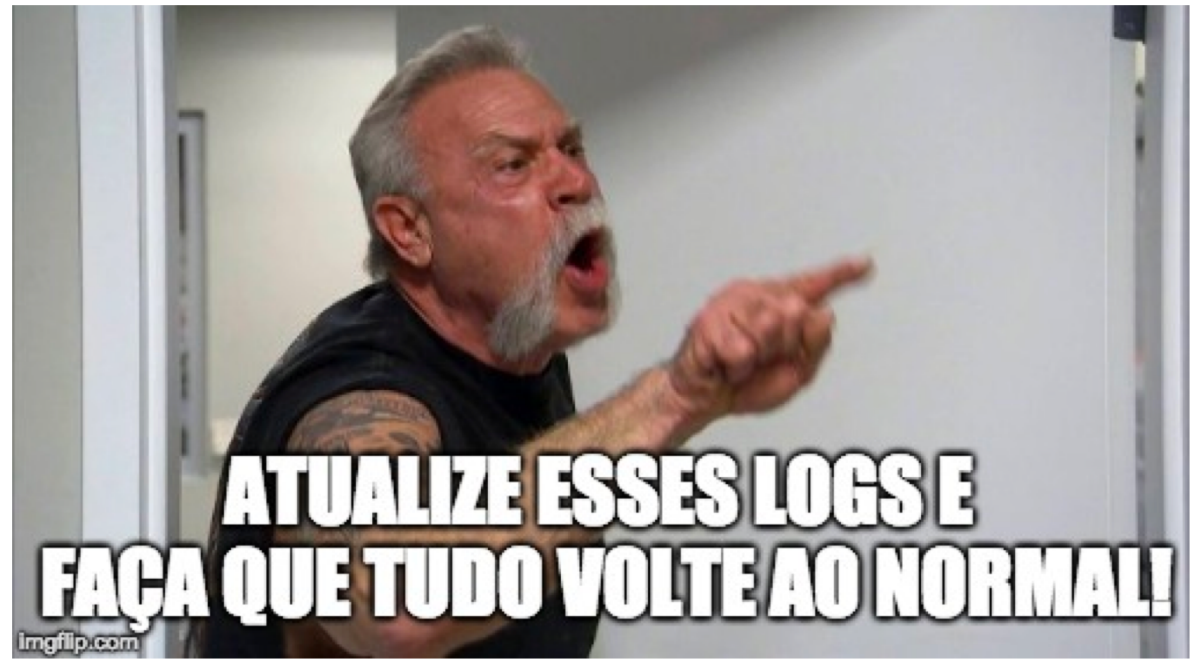


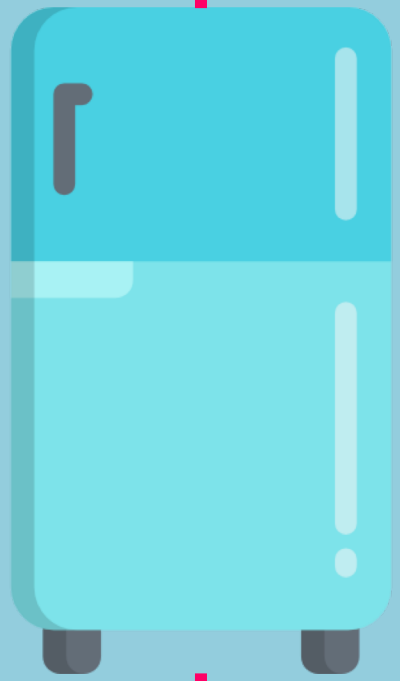


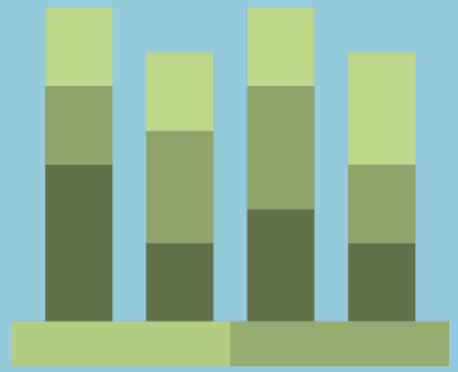

A TEMPERATURA
COMPROMETEU A PRODUÇÃO!


A FÁBRICA NÃO
VAI ACEITAR ESSE LOTE.

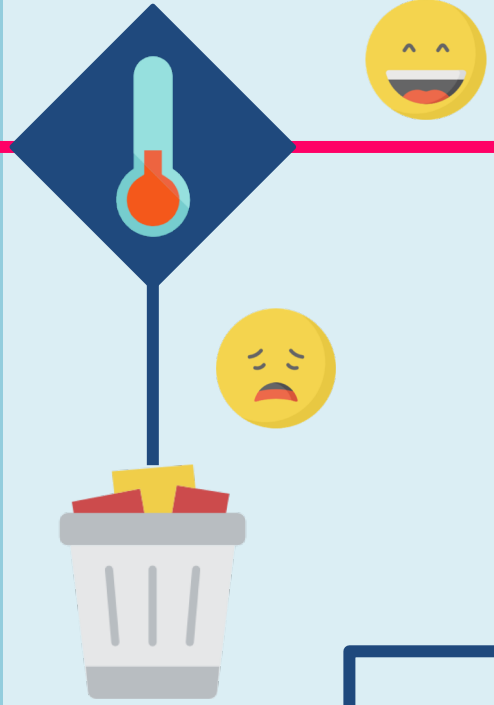

FALTOU
ENERGIA NESSE DIA!

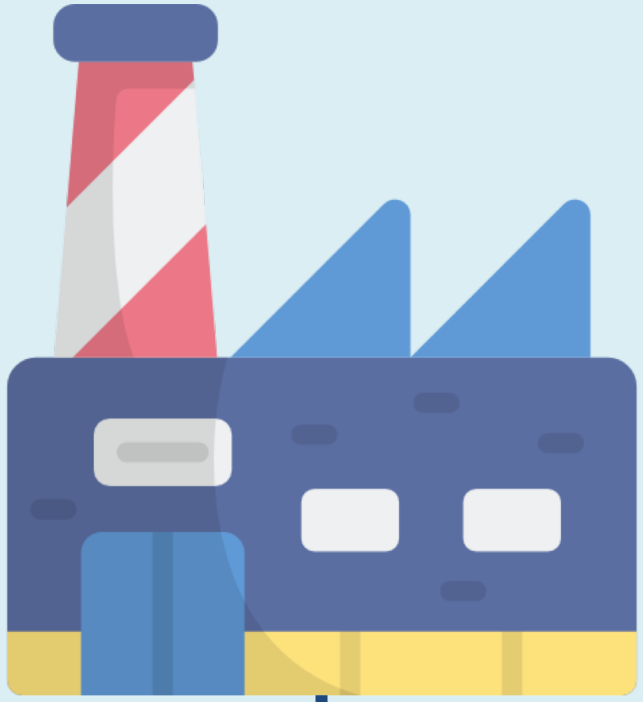

ATUALIZE ESSES LOGS E
FAÇA QUE TUDO VOLTE AO NORMAL!
imgflip.com



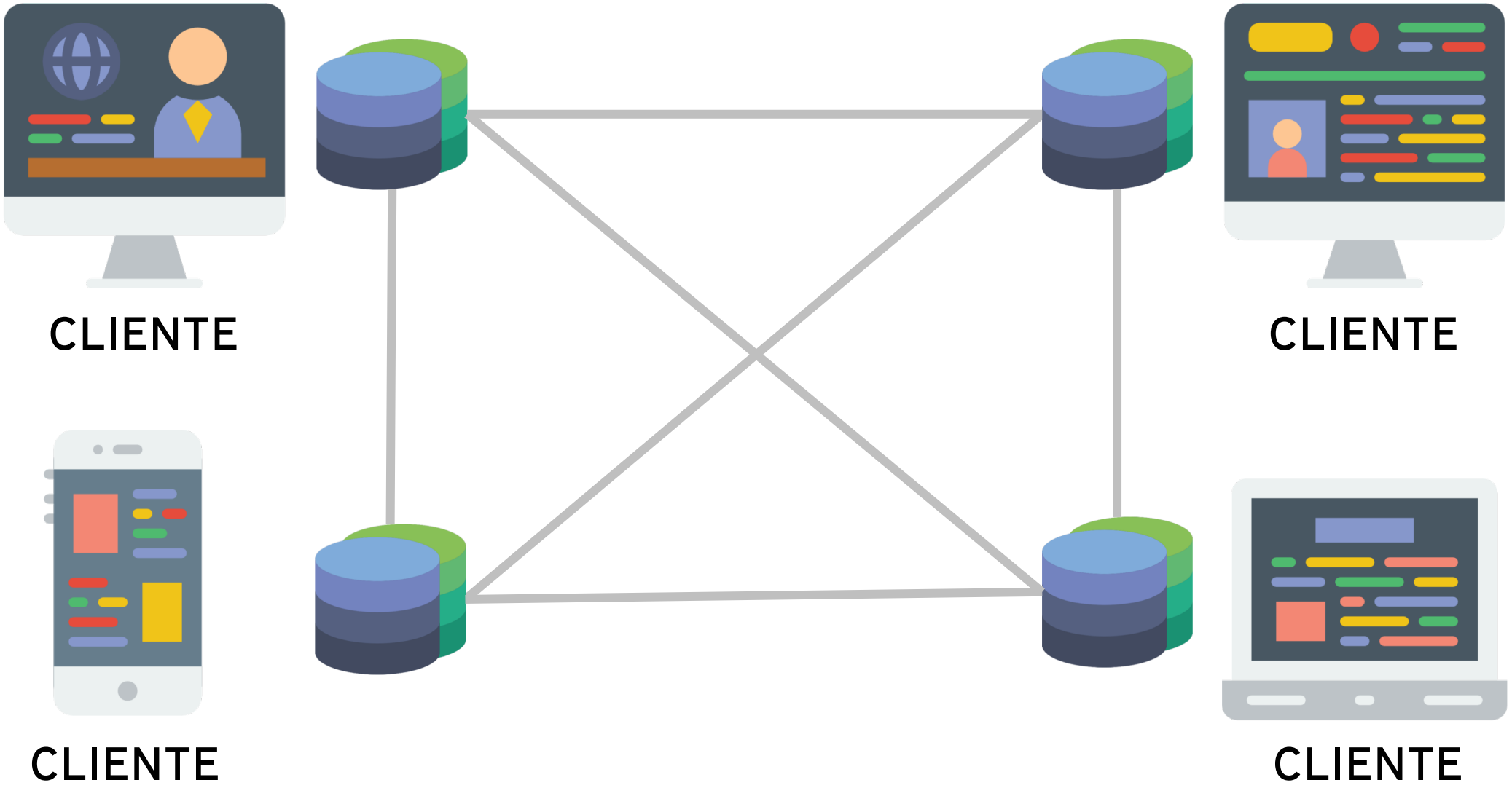


RASTREAMENTO DA TEMPERATURA

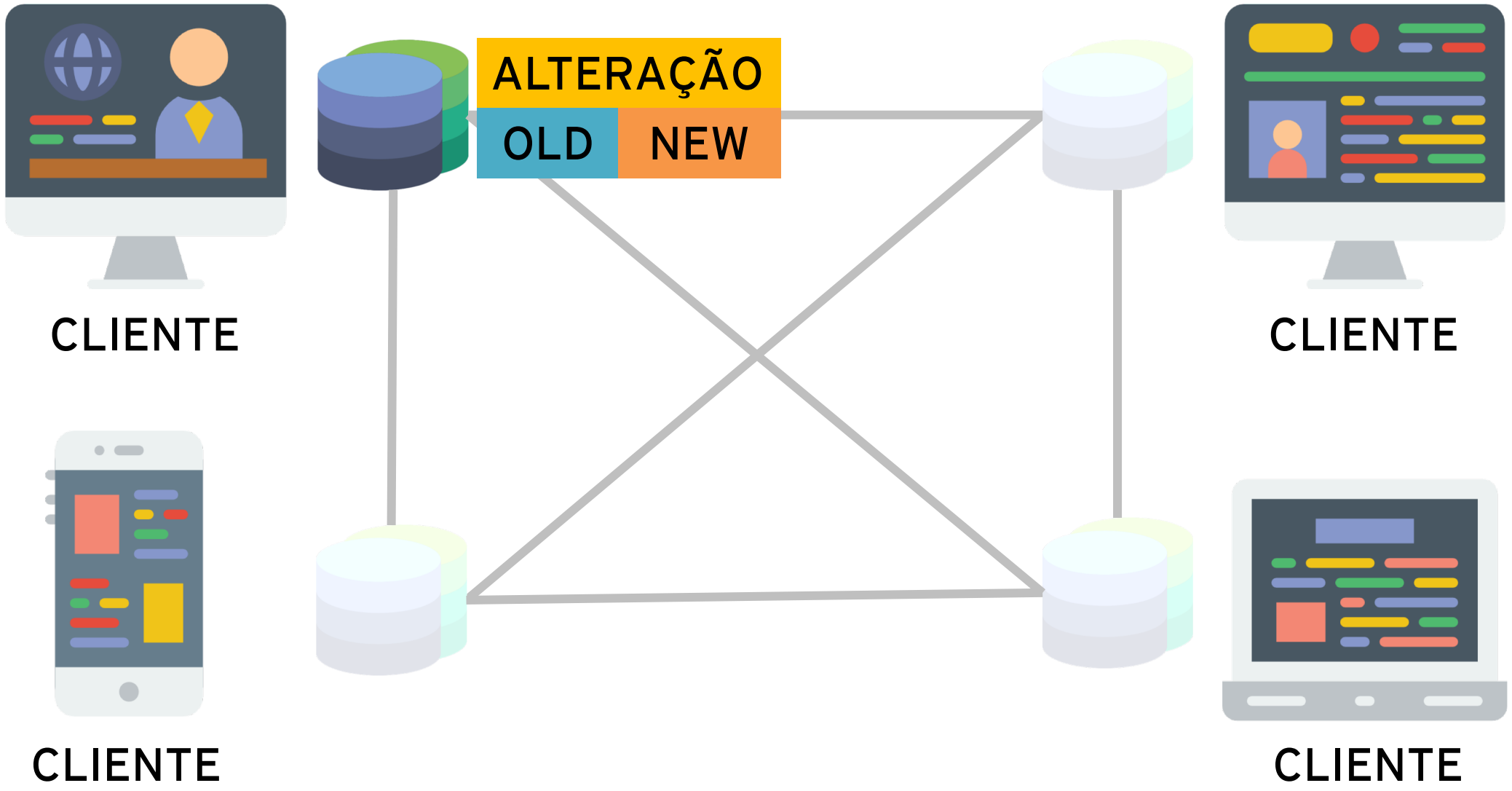




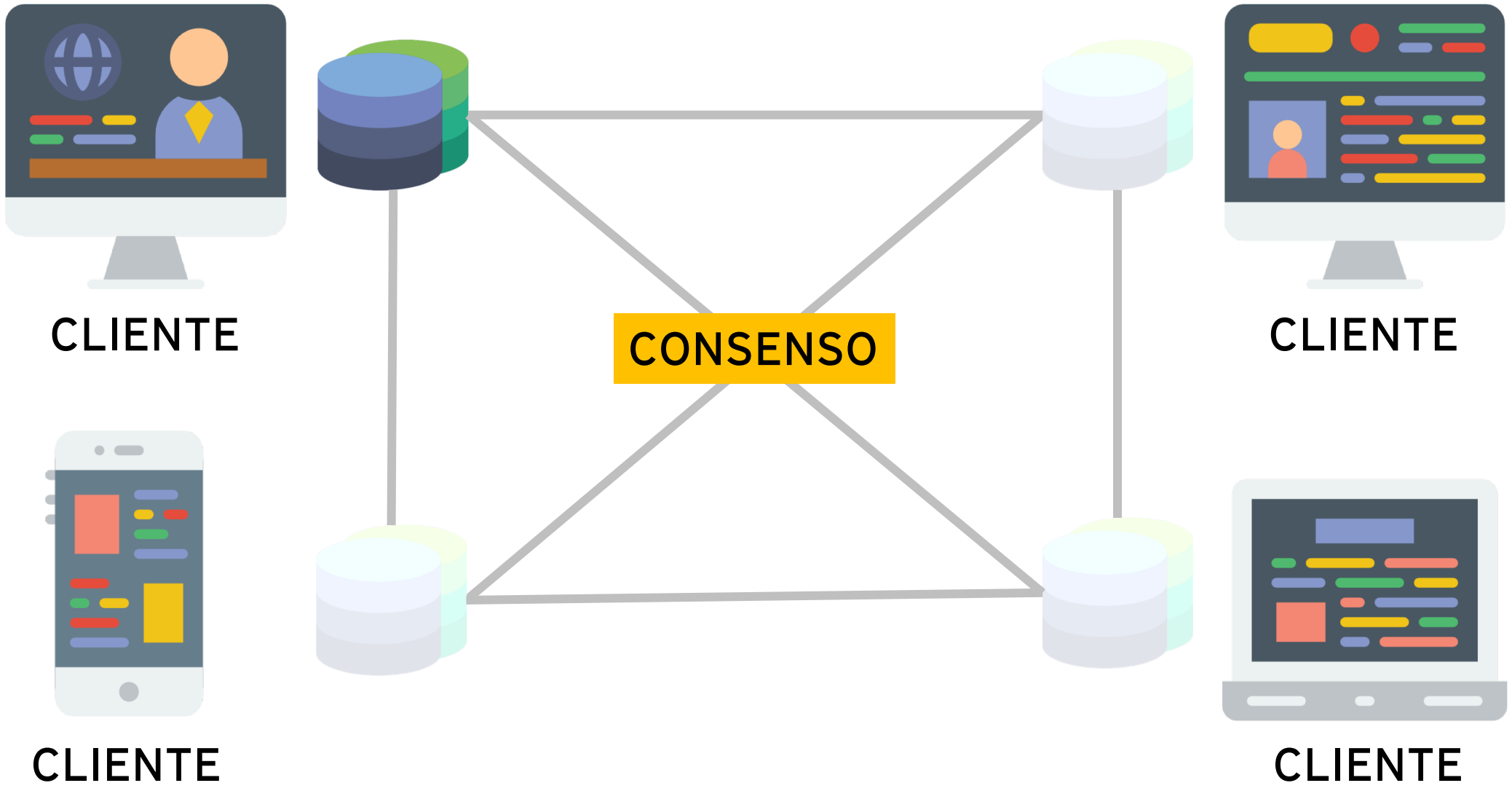
TOPOLOGIA DESCENTRALIZADA



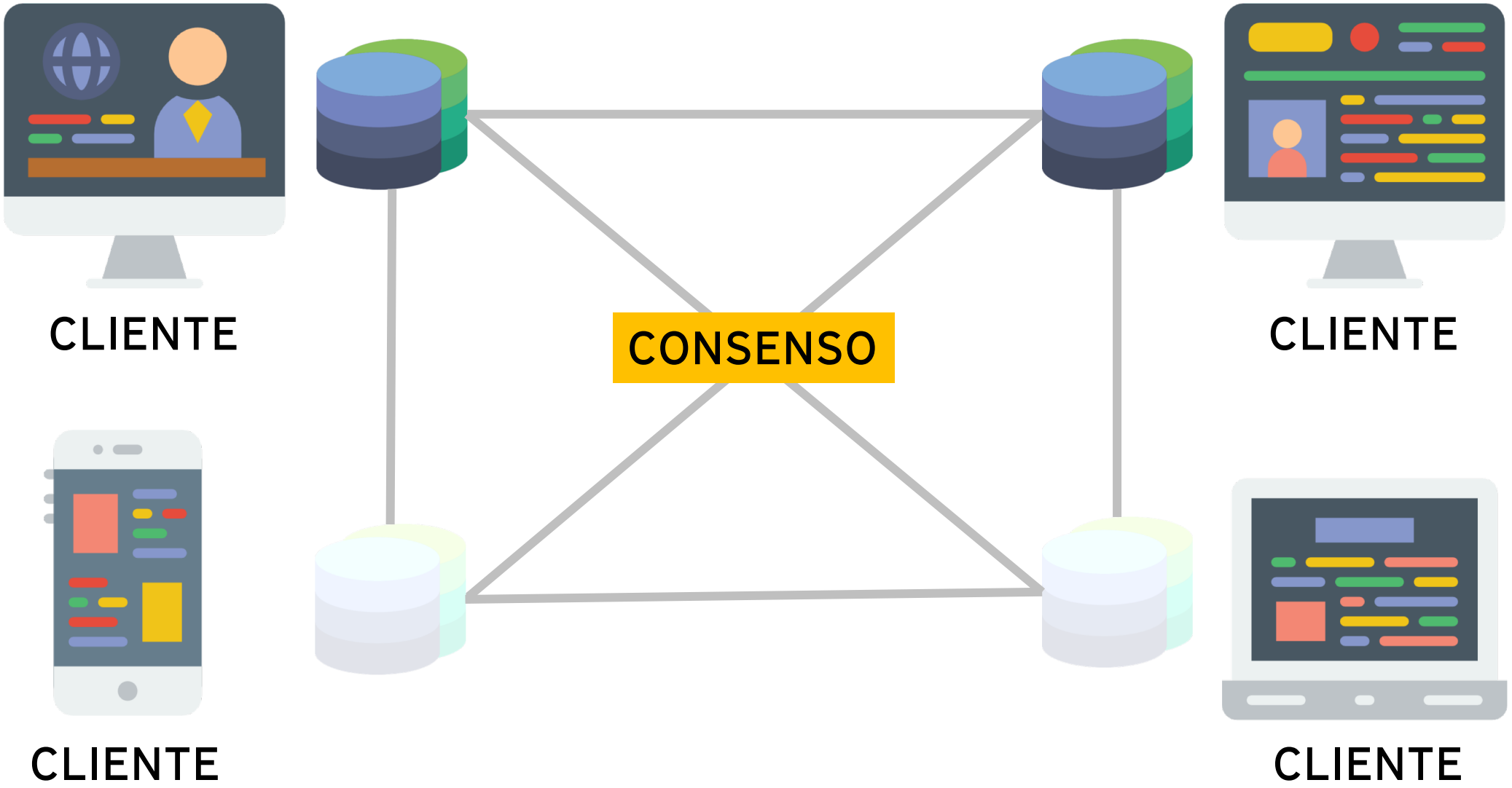
TOPOLOGIA DESCENTRALIZADA



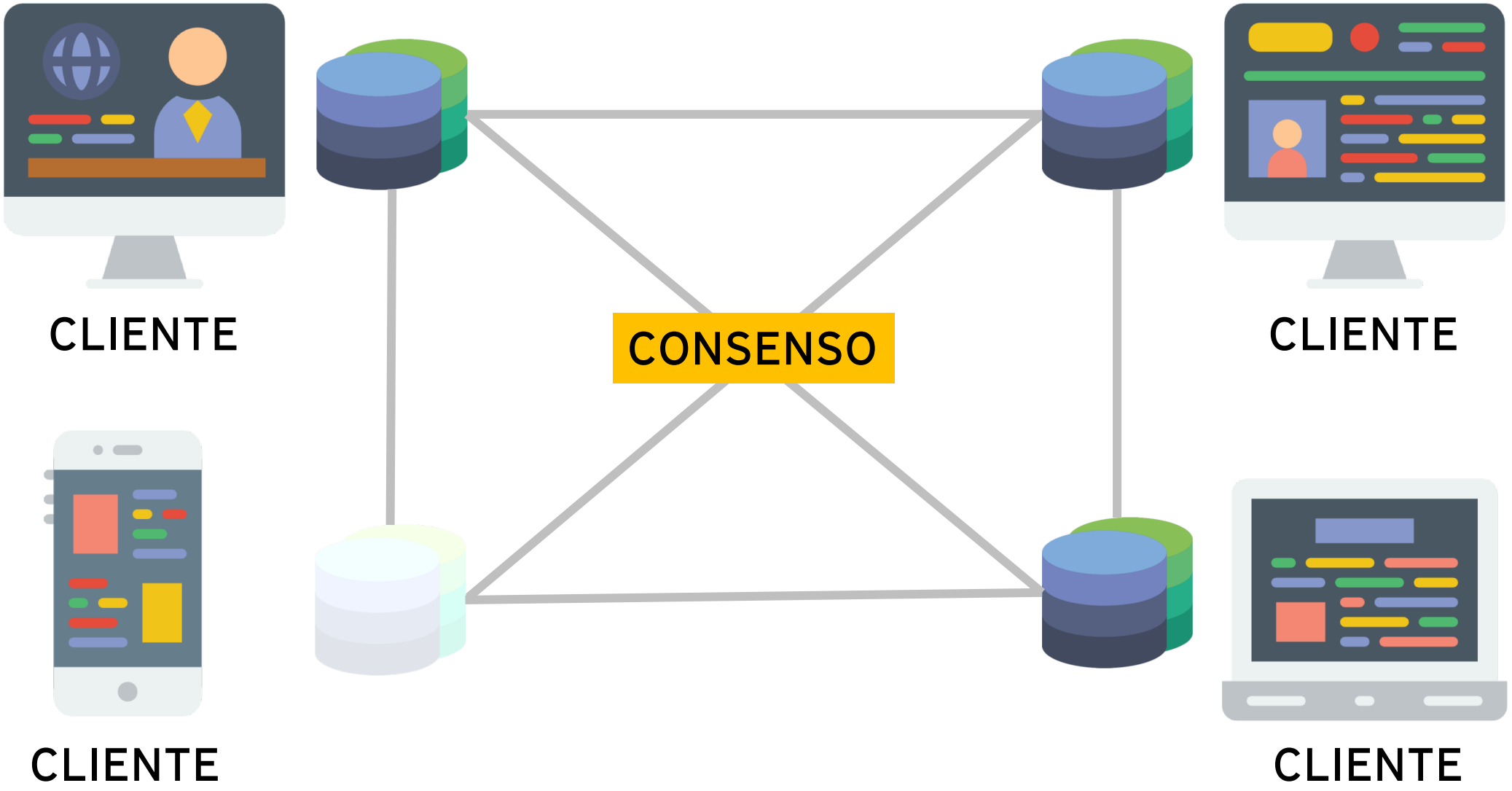
TOPOLOGIA DESCENTRALIZADA



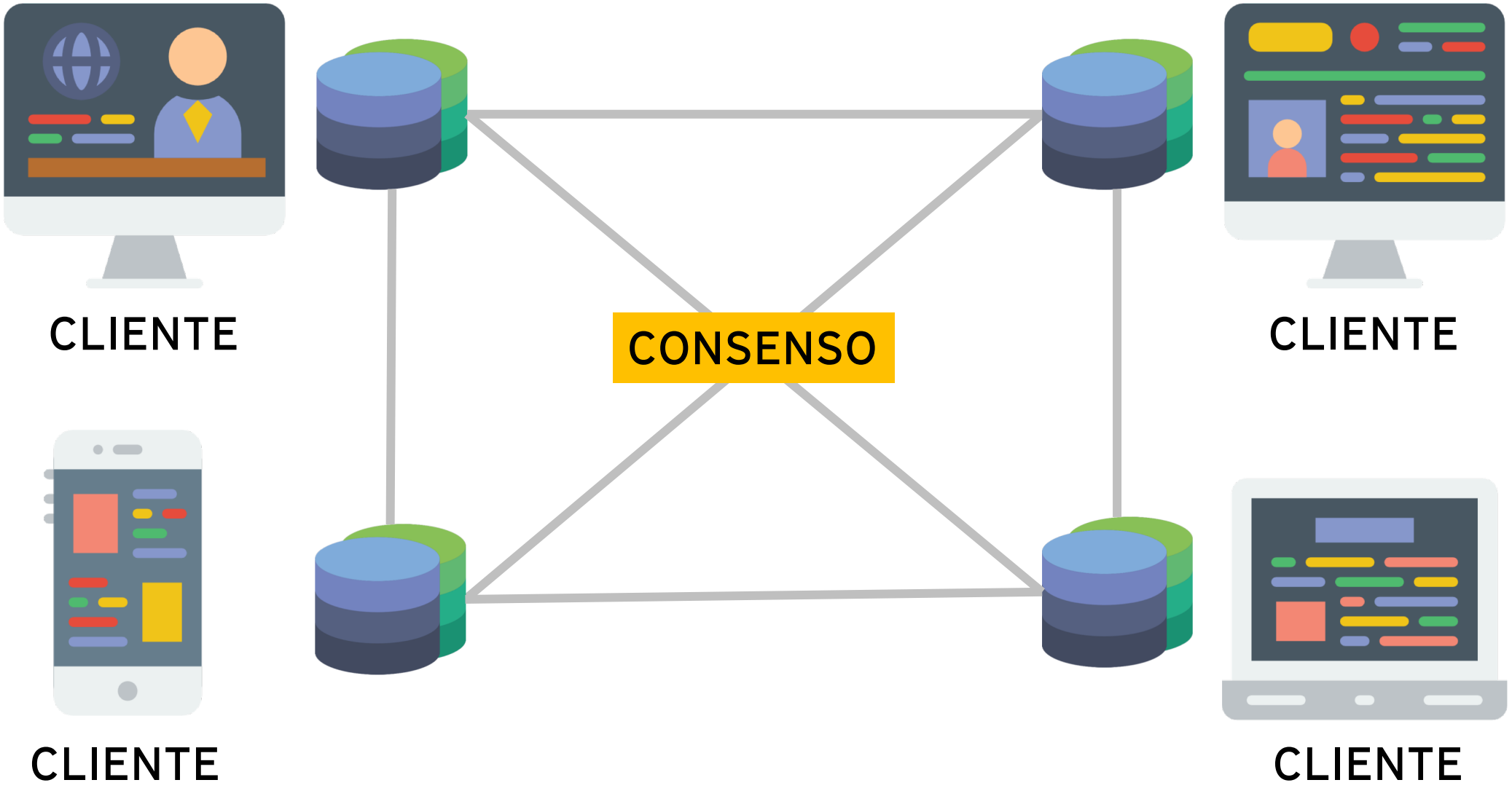
TOPOLOGIA DESCENTRALIZADA



TOPOLOGIA DESCENTRALIZADA



TOPOLOGIA DESCENTRALIZADA



BLOCKCHAIN, UM NOVO BANCO DE DADOS

DESCENTRALIZADO	IMUTÁVEL	PROTOCOLO DE CONFIANÇA
NÃO DEPENDE DE UMA AUTORIDADE CENTRAL	NADA É ALTERÁVEL LIVRO-RAZÃO aka LEDGER	GARANTIA QUE A INFORMAÇÃO É INTEGRA E SEGURA

BLOCKCHAIN, UM NOVO BANCO DE DADOS

DESCENTRALIZADO

IMUTÁVEL

PROTOCOLO DE CONFIANÇA

DISTRIBUTED LEDGER
aka DLT, *DISTRIBUTED LEDGER TECHNOLOGY*

O PROBLEMA DOS GENERAIS BIZANTINOS

https://pt.wikipedia.org/wiki/Problema_dos_dois_generais

ALGUNS ALGORTIMOS DE CONSENSO

PROVA DE TRABALHO
aka *PROVE OF WORK (PoW)*

GERA UMA FUNÇÃO HASH (SHA-256) DE UMA INFORMAÇÃO.
A COMPLEXIDADE DO CÁLCULO TRAZ UM NÍVEL DE CONFIANÇA.

PROVA DE PARTICIPAÇÃO
aka PROVE OF STAKE (PoS)

BLOCOS SERÃO GERADOS POR ENTIDADES CONFIÁVEIS NA REDE, OS QUE POSSUEM MAIOR REPUTAÇÃO POR MEIO DA QUANTIDADE DE MOEDAS.

BITCOIN: A PEER-TO-PEER SYSTEMELECTRONIC CASH

DESCRIÇÃO SOB ASPECTOS TÉCNICOS DO QUE SERIA UMA REDE DE BLOCKCHAIN, UTILIZADA NA IMPLEMENTAÇÃO DO BITCOIN

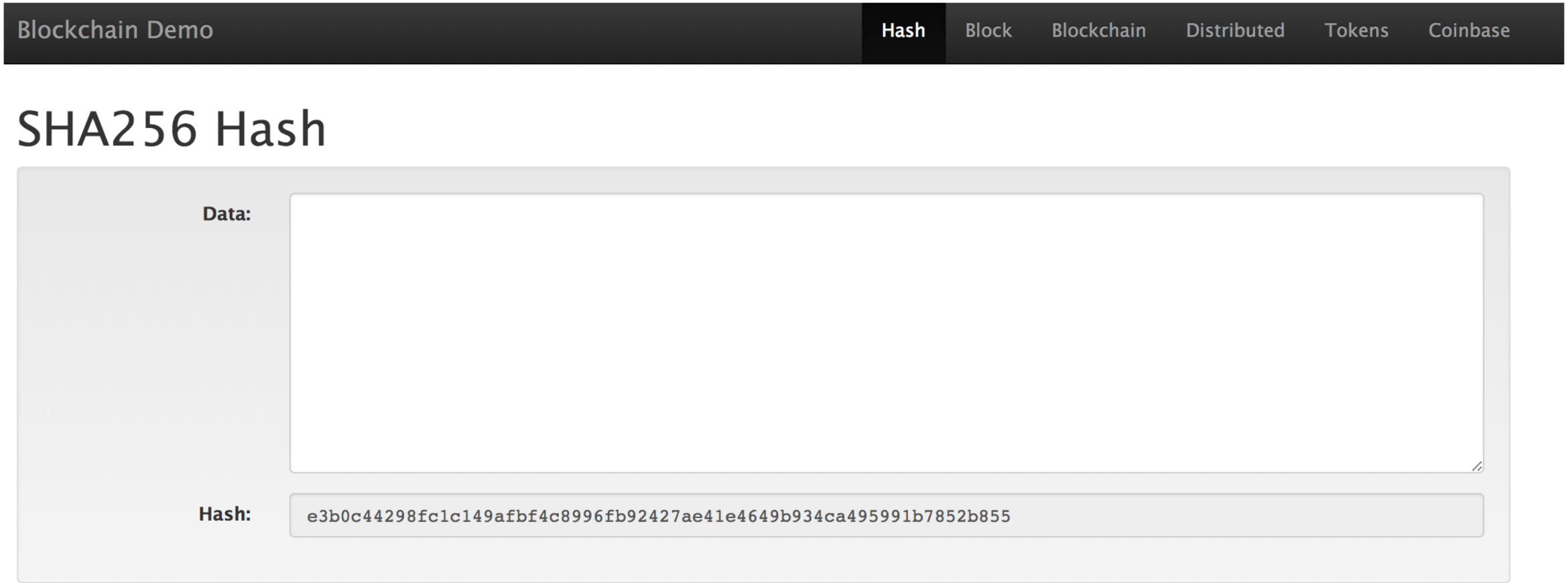
PAPER ORIGINAL

https://bitcoin.org/bitcoin.pdf

PAPER EM PORTUGUÊS

https://cointimes.com.br/whitepaper-do-bitcoin-traduzido

DEMO



https://anders.com/blockchain/

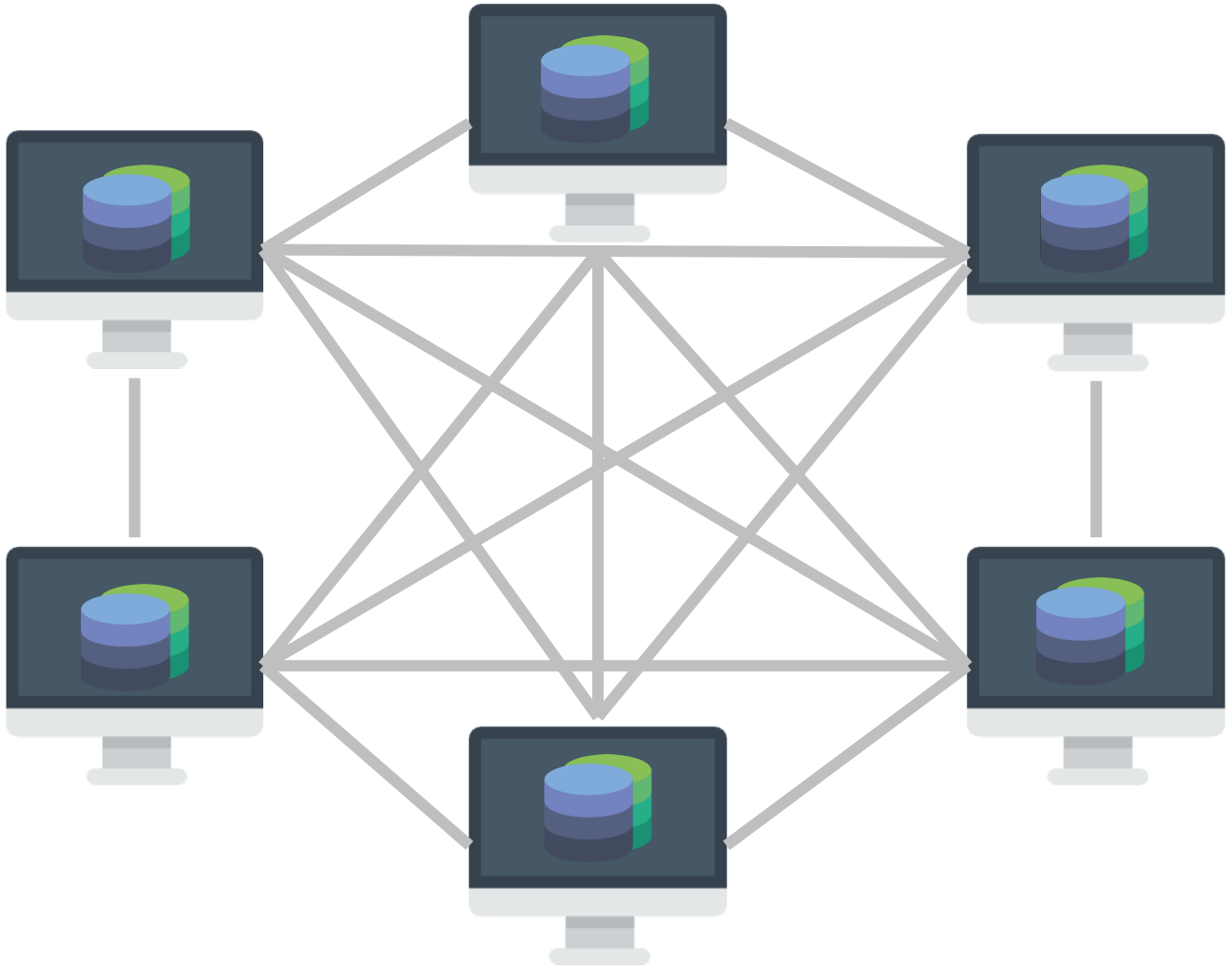
CRIADOR DO ETHEREUM

ESTUDOU PROFUNDAMENTE A PLATAFORMA DO BITCOIN

PROPÔS UMA NOVA PLATAFORMA COM AS SEGUINTES MUDANÇAS:

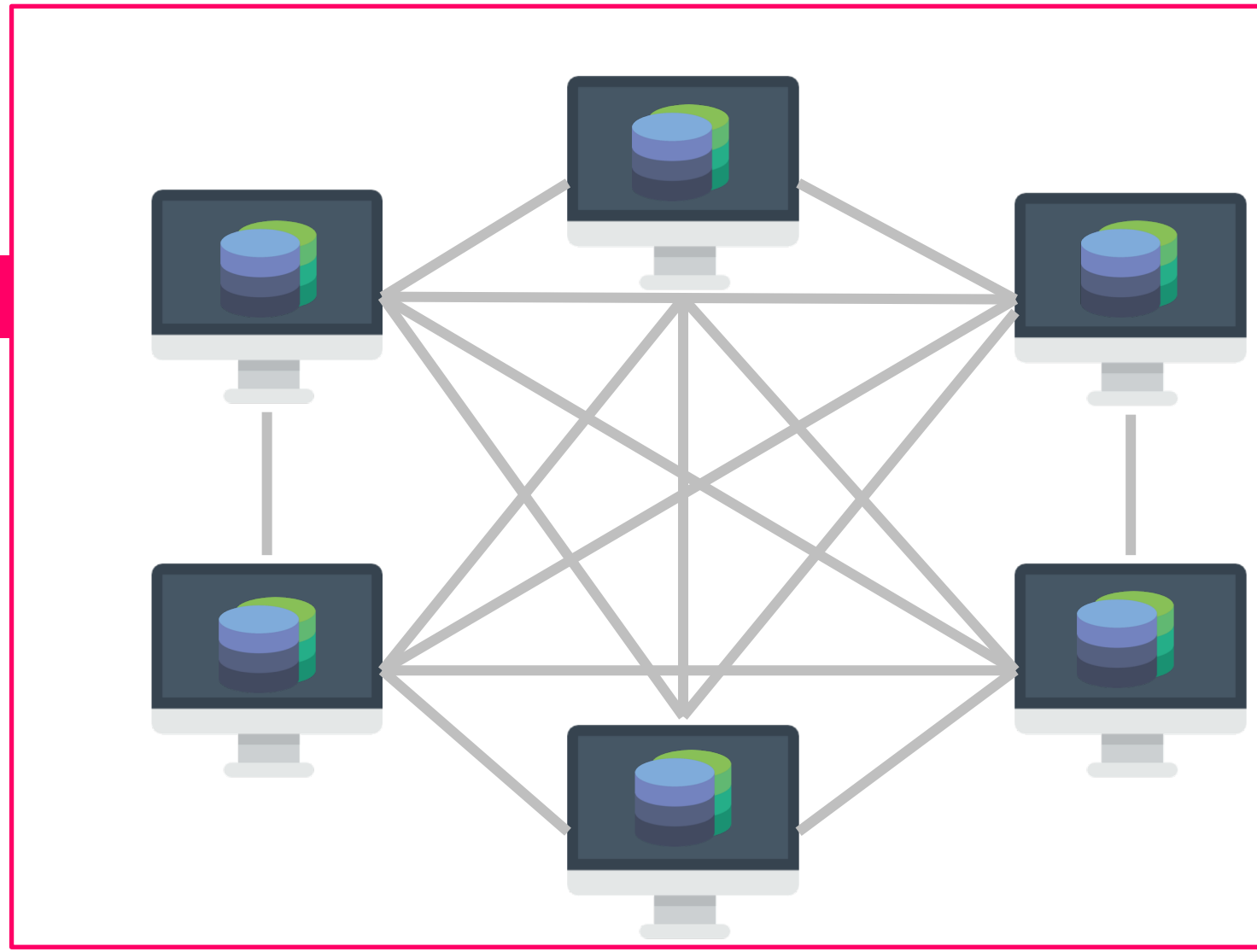
- MOEDA SEM LIMITE
- CONTRATOS INTELIGENTES
- RECOMPENSA FIXA DE PROVA DE TRABALHO
- TRANSAÇÕES MAIS RÁPIDAS QUE O BITCOIN

ETHEREUM BLOCKCHAIN



ETHEREUM BLOCKCHAIN

APPS



USERS

https://web3js.readthedocs.io

https://metamask.io

INSTALANDO O METAMASK

https://metamask.io

METAMASK

Brings Ethereum to your browser

GET CHROME EXTENSION

Chrome Firefox Opera

OR

GET BRAVE BROWSER

WALLET

ENDEREÇO

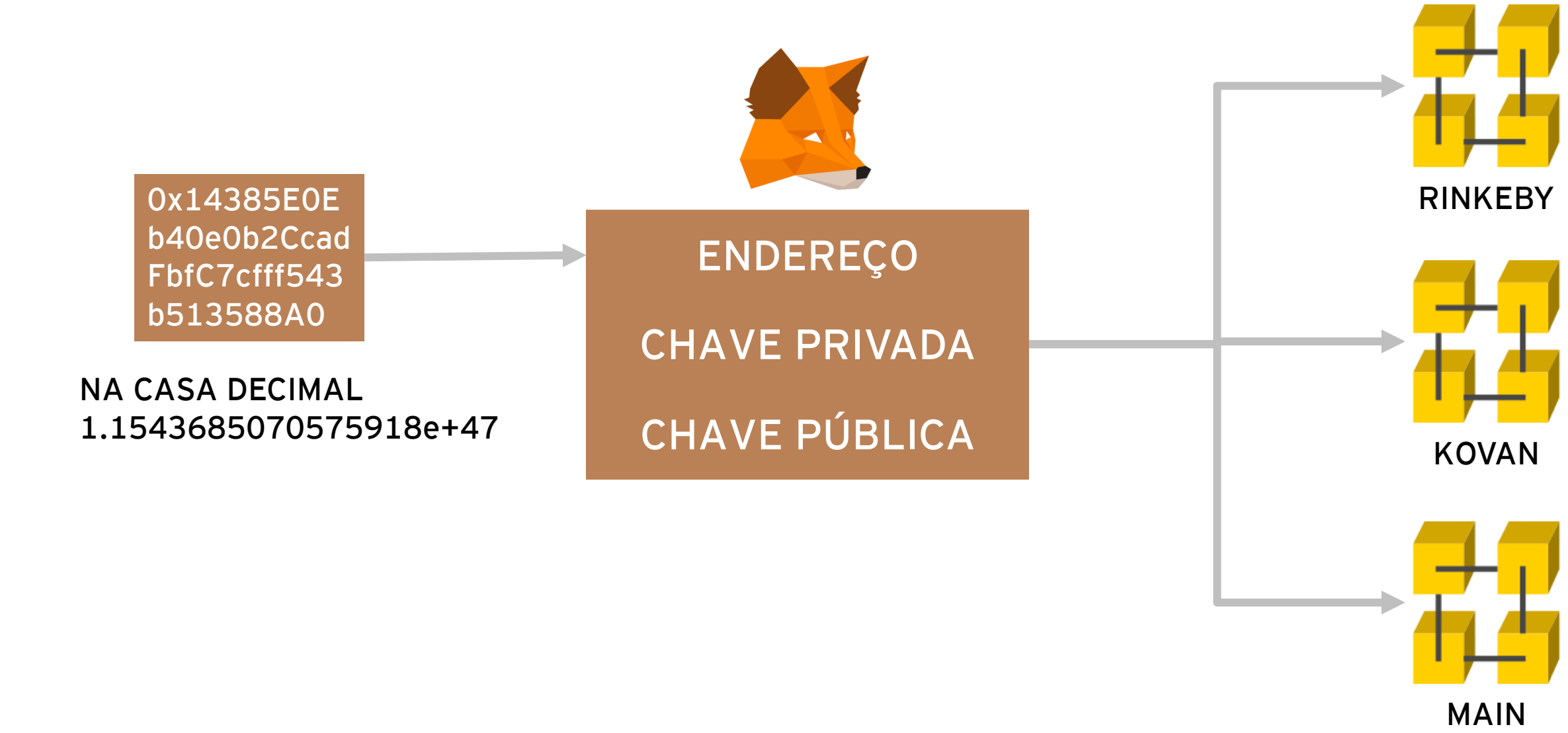
CHAVE PRIVADA

CHAVE PÚBLICA

O METAMASK GERA UM MNEUMÔNICO QUE É CAPAZ DE CRIAR UM CONJUNTO DE ENDEREÇOS, CHAVES PRIVADAS E PÚBLICAS

OS ENDEREÇOS GERADOS PODEM SER UTILIZADOS EM QUAISQUER REDES ETHEREUM (PÚBLICA, PRIVADA OU TESTES)

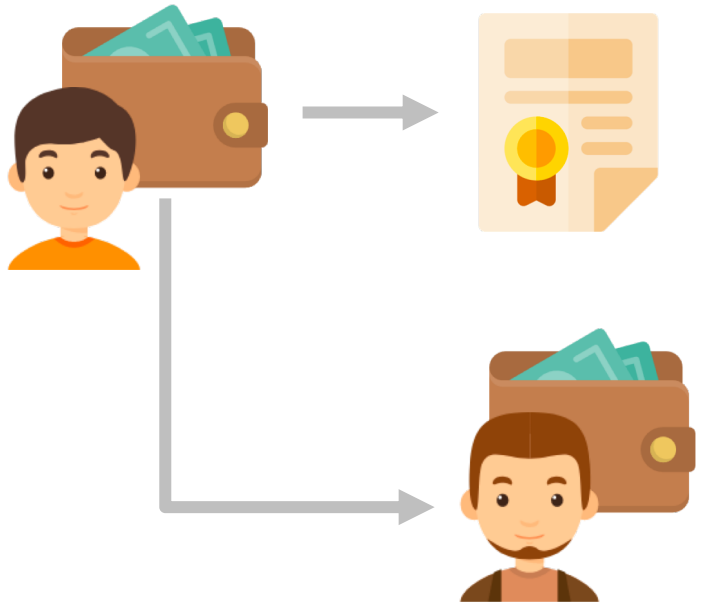
ENDEREÇO DE WALLET



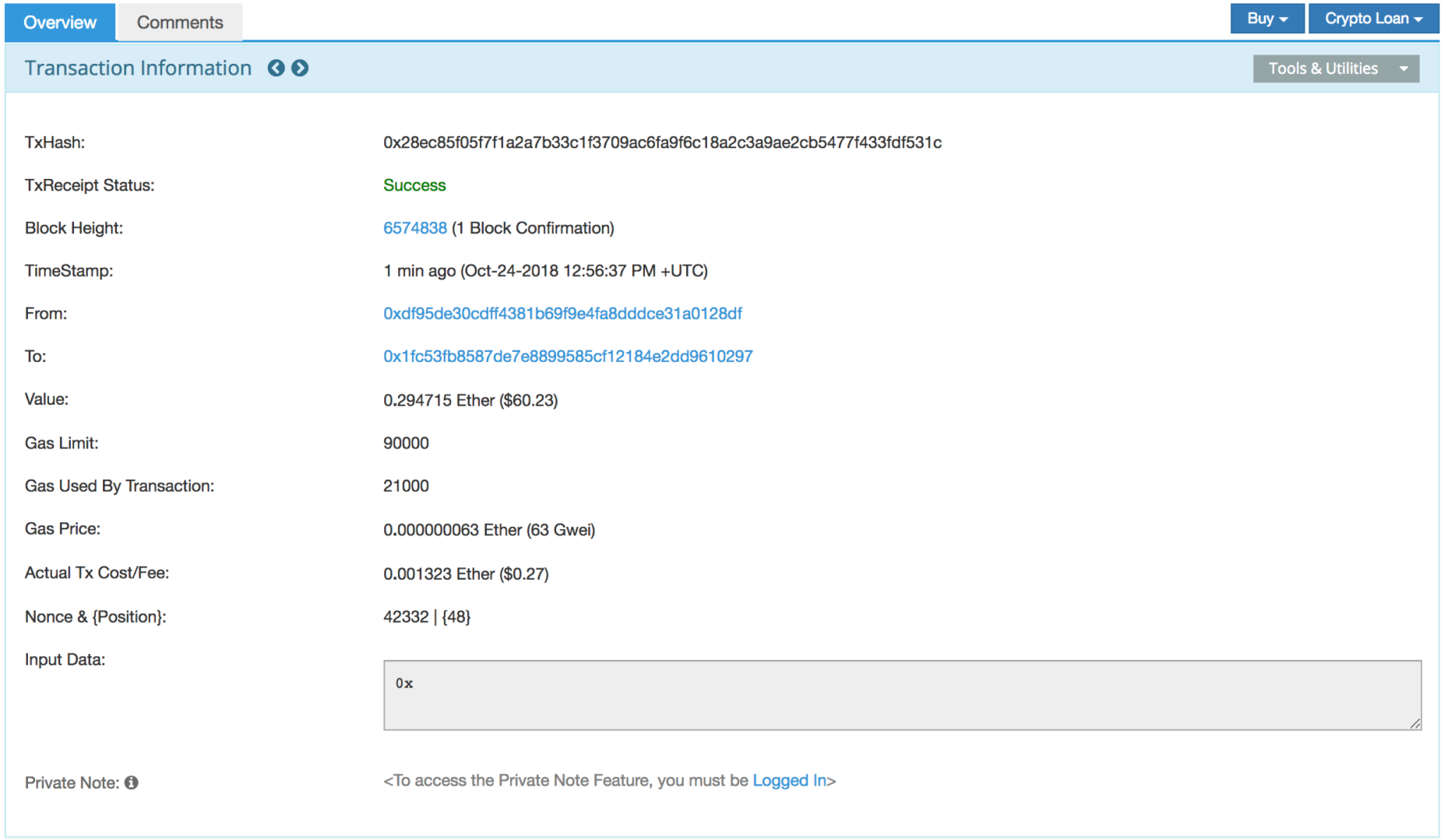
TRANSAÇÃO

TUDO QUE É ARMAZENADO NO BLOCKCHAIN

NONCE	VALOR QUE SATISFAZ A PROVA DE TRABALHO
TO	ENDEREÇO DESTINO (OU CONTRATO)
VALUE	ETHERES A SEREM TRANSFERIDOS
GAS PRICE	FATOR MULTIPLICADOR DISPOSTO A PAGAR PARA A CONFIRMAR A TRANSAÇÃO
GAS LIMIT	VALOR LIMITE DE CONFIRMAÇÃO DA TRANSAÇÃO
V R S	VALORES QUE GERAM O ENDEREÇO DE ORIGEM. SÃO CALCULADOS A PARTIR DA CHAVE PRIMÁRIA DO WALLET DE ORIGEM. *ASSINATURA DIGITAL*



EXEMPLO DE TRANSAÇÃO

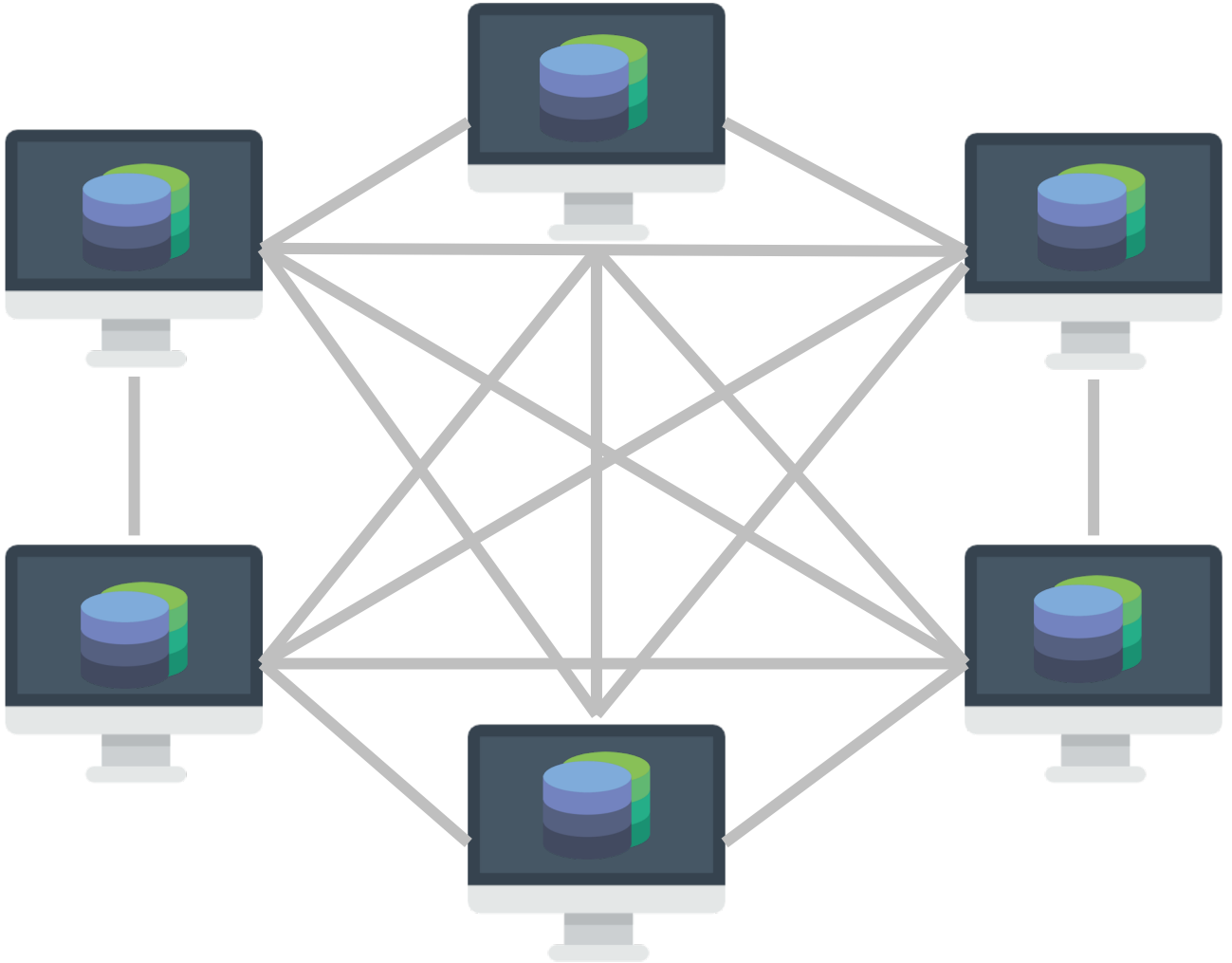


https://goo.gl/voRfCi

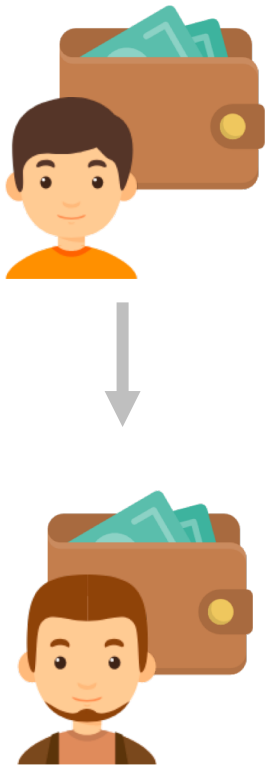
ENVIANDO UMA TRANSAÇÃO

TX

TRANSACTION POOL



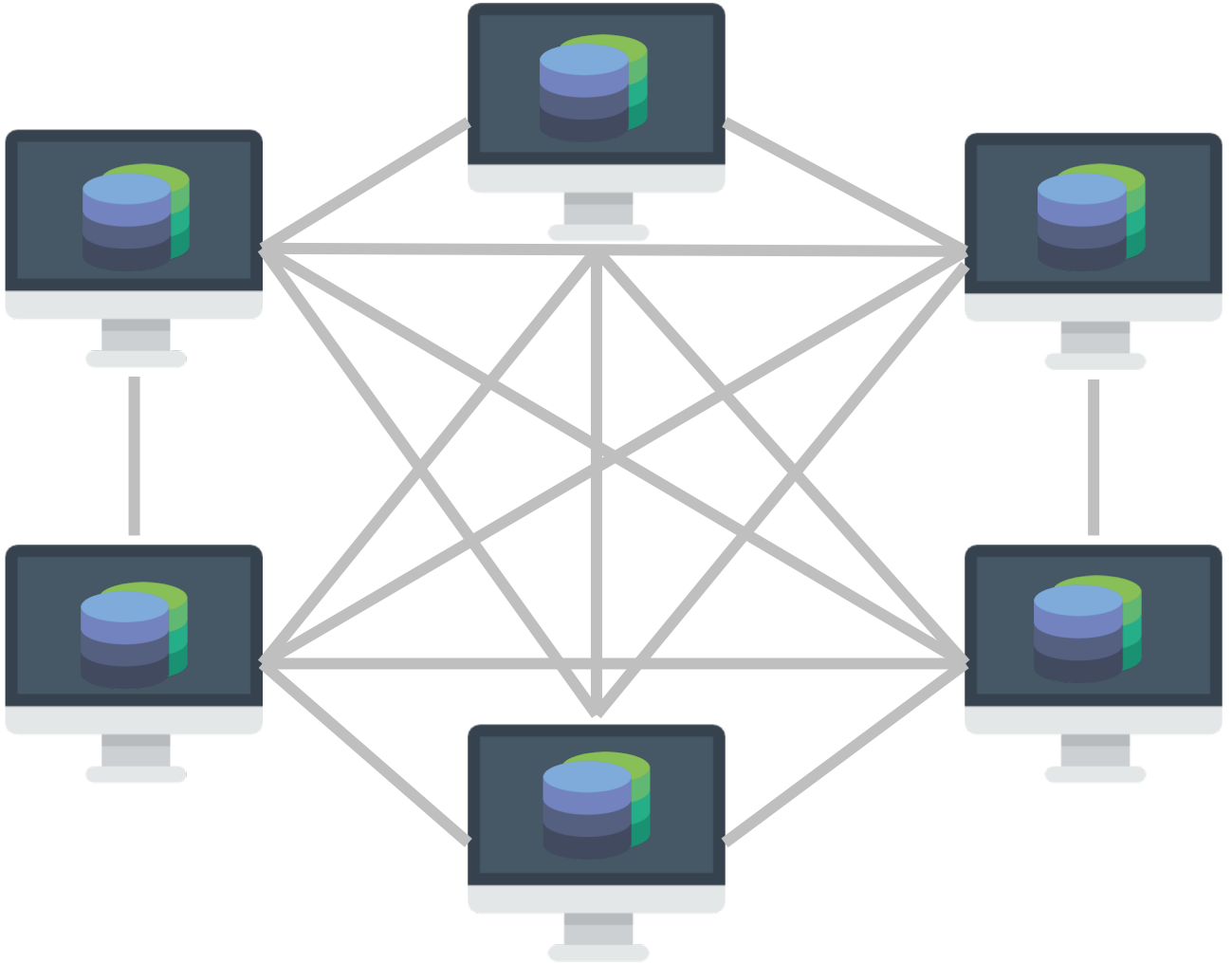
ENVIANDO UMA TRANSAÇÃO



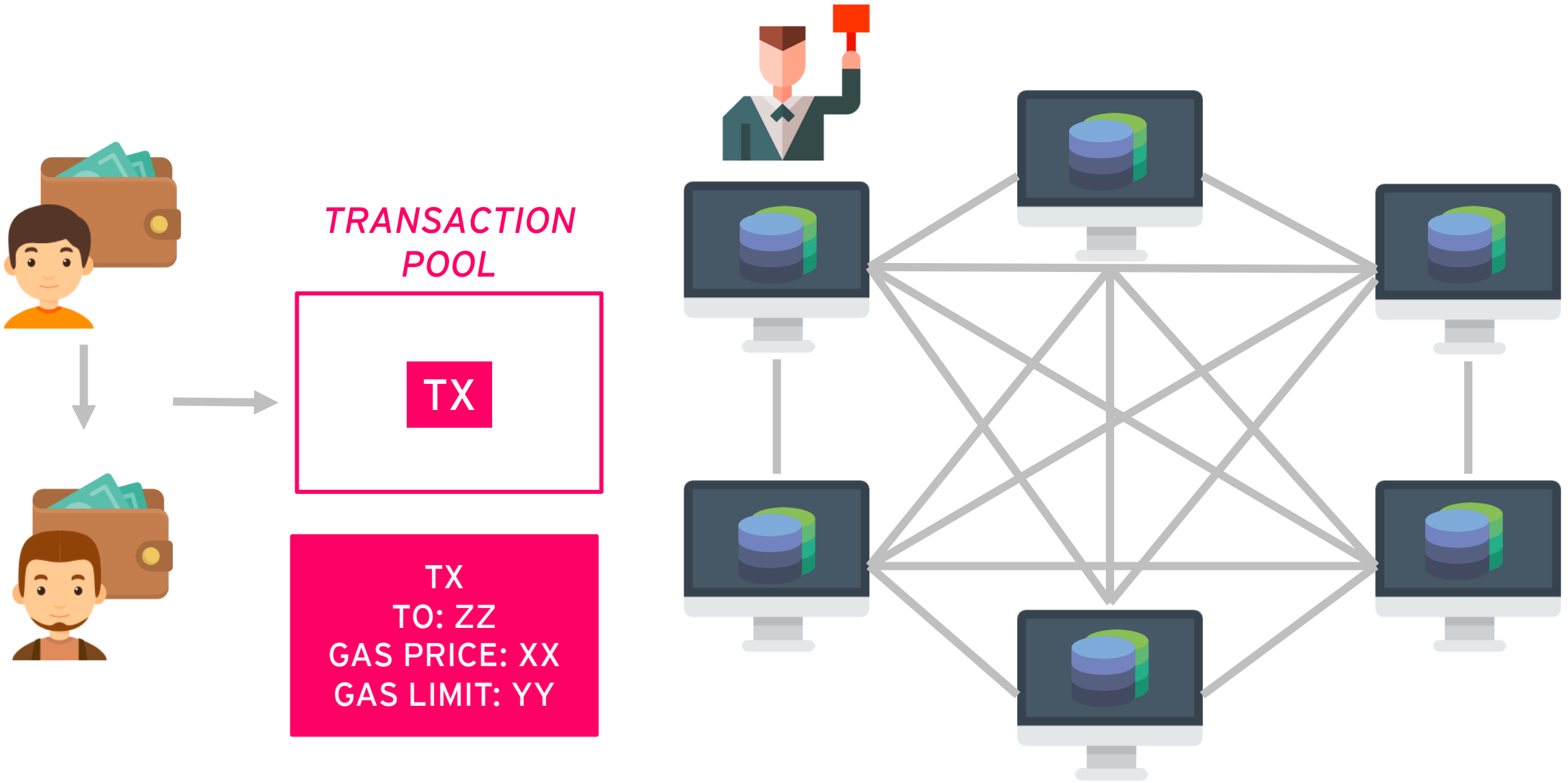
TRANSACTION POOL

TX

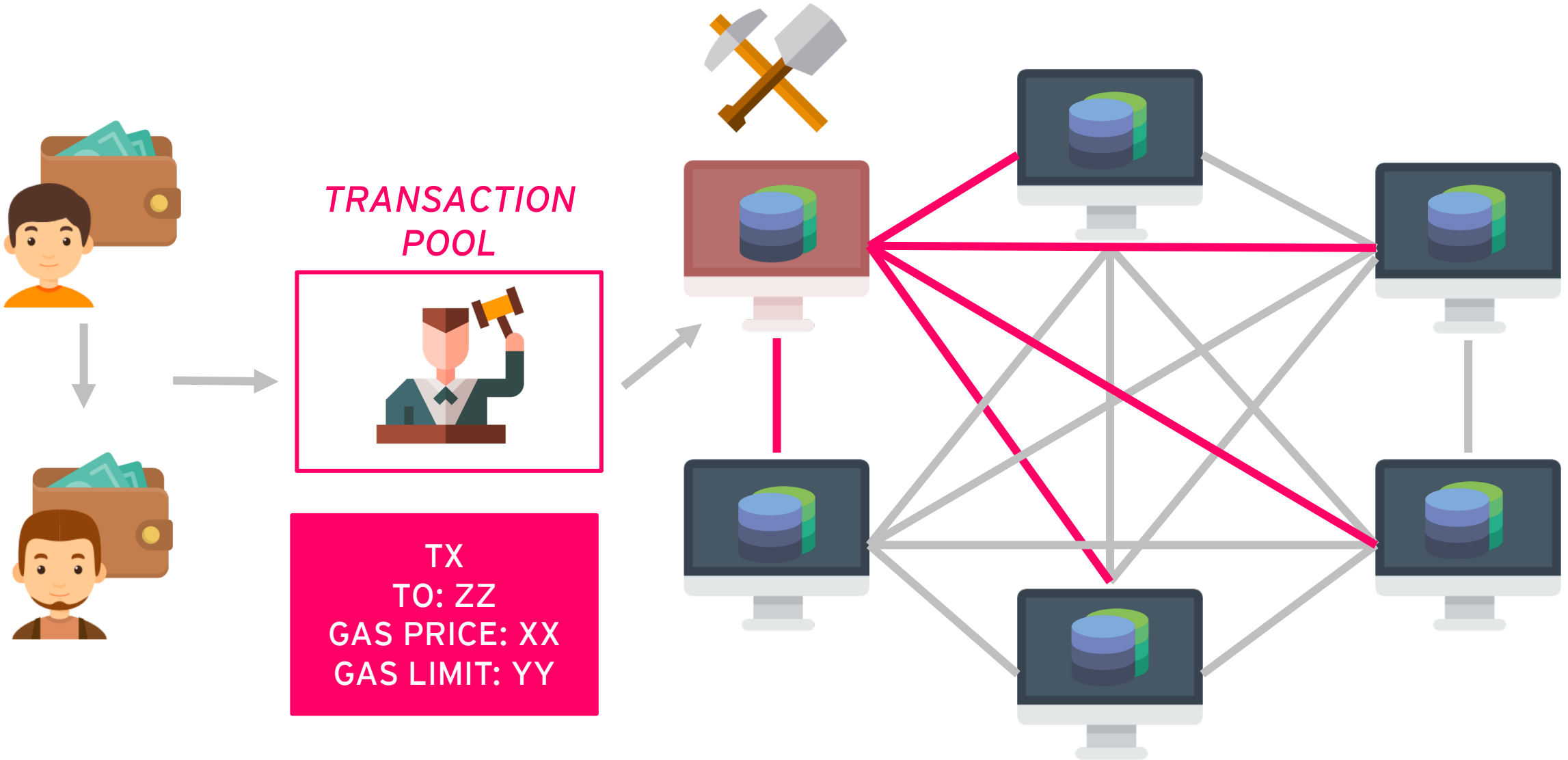
TX
TO: ZZ
GAS PRICE: XX
GAS LIMIT: YY



ENVIANDO UMA TRANSAÇÃO



ENVIANDO UMA TRANSAÇÃO



SMART CONTRACT

https://solidity.readthedocs.io

LINGUAGEM DE SMART CONTRACT É SOLIDITY

SIMILAR AO JAVASCRIPT

FORTEMENTE TIPADO

PARADIGMA ORIENTADO A OBJETOS

CADA DEPLOYMENT DO CONTRATO (*CLASS*) É COMO SE FOSSE UMA INSTÂNCIA

HELLO WORLD CONTRACT

https://remix.ethereum.org/#optimize=true

IDE WEB BASED PARA DESENVOLVIMENTO DE SMART CONTRACTS

INDICADO PARA PEQUENOS TESTES E ENTENDIMENTO BÁSICO DOS CONCEITOS DE SMART CONTRACTS

NÃO É INDICADO PARA APLICAÇÕES PROFISSIONAIS, APESAR DE SER BEM ROBUSTO, POIS DEPENDE DE ACESSO A INTERNET

COMPILAÇÃO

SMART CONTRACT
SOLIDY FILE (.SOL)

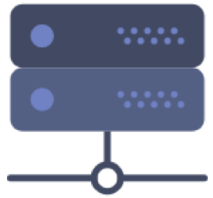
COMPILADOR
SOLIDITY

BYTECODE
NODE DEPLOYMENT

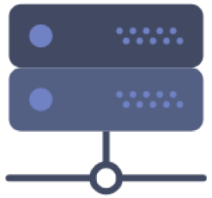
ABI (JS APPS)
APPLICATION BINARY
INTERFACE

DAPP VS APP

FRONT-END



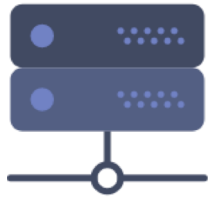
BACK-END



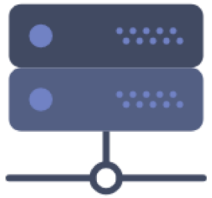
STORAGE

APP

FRONT-END

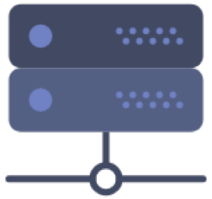


BACK-END



DAPP

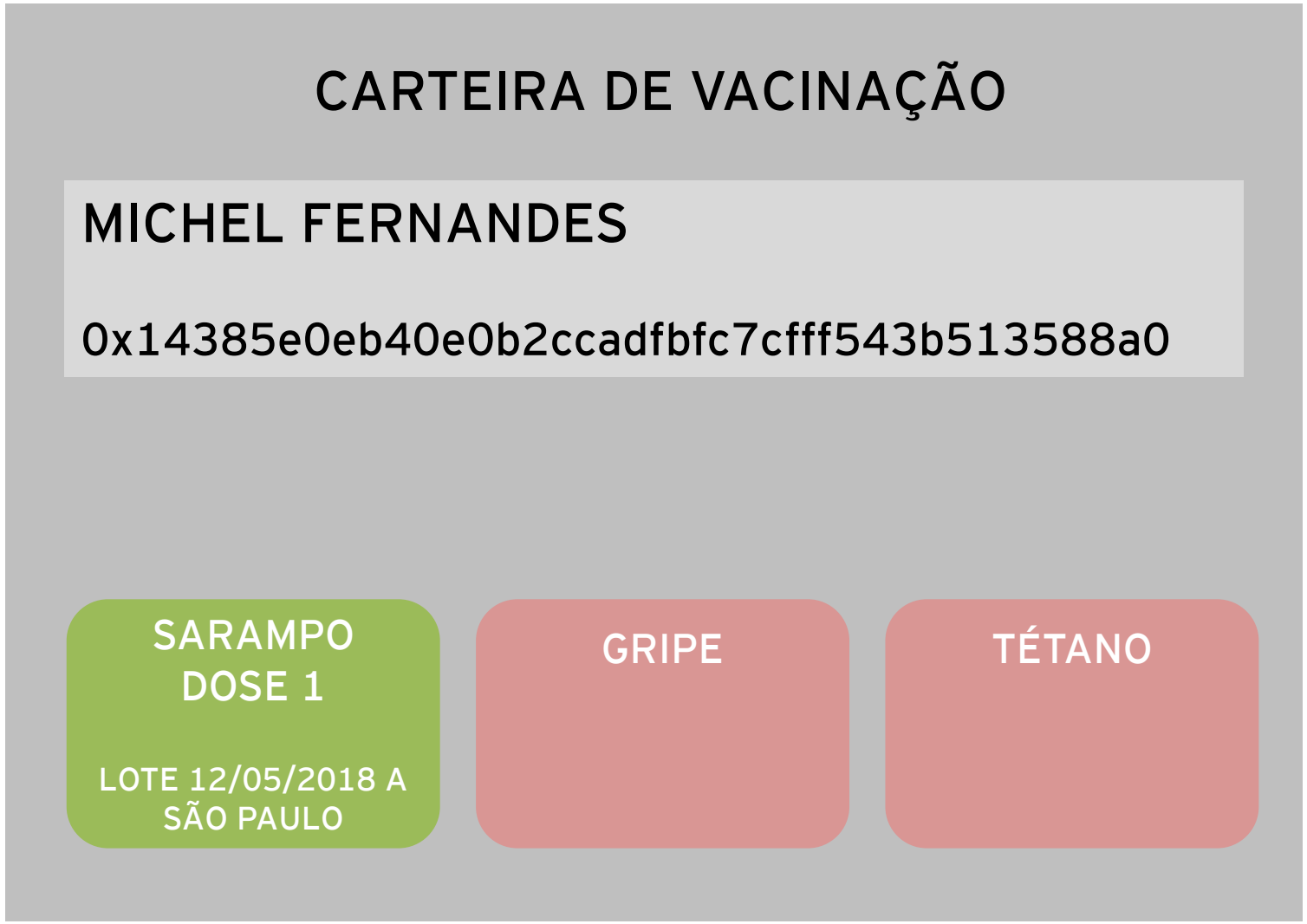
FRONT-END



DAPP

O DESAFIO

CRIAR UMA VERSÃO SIMPLIFICADA DE UMA CARTEIRA DE VACINAÇÃO BASEADA EM BLOCKCHAIN ETHEREUM



FERRAMENTAS

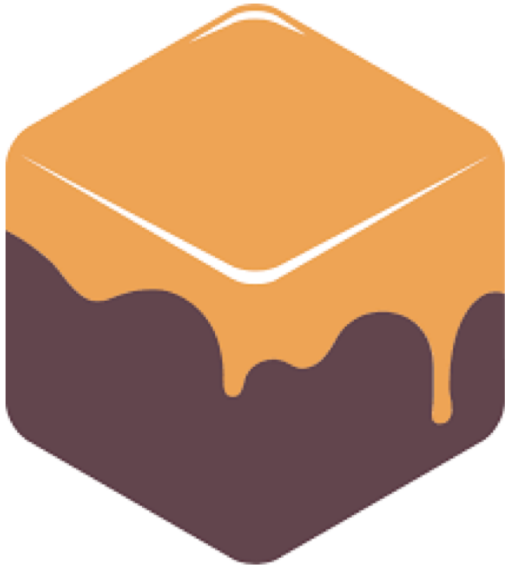
TRUFFLE

DESENVOLVIMENTO, TESTE E DEPLOY DE SMART CONTRACTS

truffleframework.com/truffle

GANACHE

NÓ DE REDE ETHEREUM DE TESTES (EX. TEST RPC)



truffleframework.com/ganache

WEB3

INTERFACE ENTRE SMARTCONTRACT E APP JS

web3js.readthedocs.io

FERRAMENTAS

TRUFFLE

DESENVOLVIMENTO, TESTE E DEPLOY DE SMART CONTRACTS

trufflefframework.com/truffle

GANACHE

NÓ DE REDE ETHEREUM DE TESTES (EX. TEST RPC)

trufflefframework.com/ganache

WEB3

INTERFACE ENTRE SMARTCONTRACT E APP JS

web3js.readthedocs.io

TRUFFLE INIT

DEPOIS DE CRIAR UM DIRETÓRIO DE PROJETO E ENVIAR O COMANDO

truffle init

O TRUFFLE IRÁ CRIAR UMA ESTRUTURA PRONTA DE PROJETO.
OS CONTRATOS DEVERÃO SER EDITADOS NA PASTA contracts.

DEVERÁ SER ACRESCENTADO UM ARQUIVO NA PASTA migrations PARA EXPORTAR CONTRATOS PARA TESTE/DEPLOY.

O ARQUIVO truffle.js, na RAIZ, PRECISA SER EDITADO PARA INCLUIR A REDE DE TESTES DO GANACHE.

TRUFFLE.JS

```
module.exports = {
   migrations_directory: "./migrations",
   networks: {
      development: {
         host: "127.0.0.1",
         port: 8545,
         network_id: "*", // Match any network id
      }
   },
   solc: {
      optimizer: {
         enabled: true,
         runs: 500
      }
   }
};
```

VERIFIQUE SE A PORTA DO GANACHE É A MESMA CONFIGURADA NO TRUFFLE.

SOLC É O COMPILADOR, O VALOR runs É QUANTAS VEZES O COMPILADOR OTIMIZARÁ O CONTRATO

ESTRUTURAS

```
struct Person {
    address personAddress;
    string firstName;
    string lastName;
    bool created;
    mapping(uint => Vaccine)
    vaccines;
}

struct Vaccine {
    uint dose;
    string batch;
    string place;
}
```

MICHEL FERNANDES

0x14385e0eb40e0b2ccadfbfc7cfff543b513588a0

SARAMPO
DOSE 1

LOTE 12/05/2018 A
SÃO PAULO

MÉTODOS

ADICIONAR OU SUBSTITUIR UMA NOVA PESSOA

```
function addPerson(string _firstName, string _lastName) public returns (bool) {

    address _address = msg.sender;
    Person storage person = persons[_address];
    person.firstName = _firstName;
    person.lastName = _lastName;
    person.created = true;

    emit statusEvent(100);
    return true;
}
```

TRANSACTION: ARMAZENA DADOS

MÉTODOS

RETORNAR DADOS DE UMA PESSOA

```
function getPerson() public view returns (string, string) {
    address _address = msg.sender;
    return (persons[_address].firstName, persons[_address].lastName);
}
```

CALL: SOMENTE LEITURA

MÉTODOS

ADICIONAR UMA VACINA A UMA PESSOA

```
unction addVaccine(uint _vaccineId, uint _dose, string _batch, string _place) public
returns(bool)
{
    address _address = msg.sender;

    Vaccine storage vaccine = persons[_address].vaccines[_vaccineId];
    vaccine.dose = _dose;
    vaccine.batch = _batch;
    vaccine.place = _place;
    persons[_address].vaccines[_vaccineId] = vaccine;
    emit statusEvent(101);

    return true;
}
```

TRANSACTION: ARMAZENA DADOS

MÉTODOS

RETORNAR VACINA DE UMA PESSOA

```
function getVaccine(uint _vaccineId) public view returns (uint, string, string) {
address _address = msg.sender;
    return (persons[_address].vaccines[_vaccineId].dose,
    persons[_address].vaccines[_vaccineId].batch,
    persons[_address].vaccines[_vaccineId].place);
}
```

CALL: SOMENTE LEITURA

TESTES

PODEM SER FEITOS COM O MOCHA (JS) OU NO PRÓPRIO SOLIDITY.

```
pragma solidity ^0.4.23;

import "truffle/Assert.sol";
import "truffle/DeployedAddresses.sol";
import "../contracts/VaccineControl.sol";

contract TestVaccineControl {



}
```

FUNÇÕES DE TESTE

TESTES

```
function testAddingNewPerson() public {

    VaccineControl vaccineControl =
    VaccineControl(DeployedAddresses.VaccineControl());

    string memory firstName = "Michel";
    string memory lastName = "Fernandes";
    bool result;
    result = vaccineControl.addPerson(firstName,
    lastName);

    Assert.equal(result, true, "Adding new person.");
}
```

TESTE PARA ADICIONAR NOVA PESSOA

TESTES

```
function testAddingNewVaccine() public {
    VaccineControl vaccineControl =
    VaccineControl(DeployedAddresses.VaccineControl());

    uint idVaccine = 1;
    uint dose = 1;
    string memory batch = "12-2018-ABC";
    string memory place = "Posto de Saúde Santa Maria";
    bool result;
    result = vaccineControl.addVaccine(idVaccine, dose,
    batch, place);

    Assert.equal(result, true, "Adding new vaccine.");
}
```

TESTE PARA ADICIONAR NOVA VACINA

DEPLOY

CONSISTEM EM 3 PASSOS:

truffle compile

VERIFICAÇÃO DE ERROS DE SINTAXE
GERA OS BYTECODES E ABI (JSON)

truffle test

TESTES INTEGRADOS

truffle migrate --reset

MIGRAÇÃO DE CONTRATO

WEB APP

NOSSO WEB APP FOI CONSTRUÍDO DA FORMA MAIS SIMPLES O POSSÍVEL, VISANDO O ENTENDIMENTO DE UM DAPP NO NÍVEL DE FUNDAMENTO.

POR ISSO O STACK ENVOLVIDO FOI SIMPLIFICADO/

O WEB SERVER UTILIZADO FOI O LITE-SERVER DO NPM (NPM INSTALL LITE-SERVER).

O FRONT-END FOI DESENVOLVIDO COM BOOTSTRAP E JQUERY.

ATULAMENTE, O TRUFFLE, COM DRIZZLE OFERECE SUPORTE AO REACT.

Vaccine Registration

Vaccine Card

Account: 0x068cf9e6ded584a05eb68944f3f52be52baf348c

First name

Enter your first name

Last name

Enter your last name

Create or change person identification | Add a vaccine

Measles

MISSING RECORD

Flu

MISSING RECORD

Tetanus

MISSING RECORD

ONDE APRENDER MAIS?

DOCUMENTAÇÃO DO TRUFFLE, ESTUDE DRIZZLE E REACT

OPEN ZEPELLIN (IMPLEMENTAÇÃO DE TOKENS E CONTRATOS PADRONIZADOS, ERC20, ERC70, ETC.)

CURSOS CURTOS (BLOCKCHAIN ACADEMY, UDEMY, ETC.)

FORMAÇÃO MBA (FIAP MBA BLOCKCHAIN DEV & TECH)
www.fiap.com.br/mba/mba-em-blockchain-development-e-technologies/

https://github.com/michelpf/bck-eth-dapp-vaccine-control