

ATIVOS DIGITAIS E BLOCKCHAIN – PROJETO FINAL

DIGITAL EVIDENCE

CAIO TERRA
GABRIEL FERREIRA
JOÃO HENRIQUE CALDEIRA
PEDRO AZAMBUJA

2019.2

AGENDA



- 1 — INTRODUÇÃO
- 2 — PROBLEMA
- 3 — SOLUÇÃO
- 4 — VANTAGENS
- 5 — DESAFIOS
- 6 — DAPP

An aerial, sepia-toned photograph of a dense city skyline, likely New York City, featuring numerous skyscrapers and a bridge in the distance. A semi-transparent white rounded rectangle is centered over the image, containing the word 'INTRODUÇÃO' in a large, bold, black serif font.

INTRODUÇÃO

INTRODUÇÃO

BLOCKCHAIN

É UM ALGORITMO QUE CODIFICA DADOS, CHAMADOS DE BLOCOS E PERMITE ATUALIZAÇÕES NA FORMA DE UMA CADEIA



TODOS OS USUÁRIOS DO SISTEMA BLOCKCHAIN SE TORNAM NÓS DA REDE, O QUE GARANTE A INTEGRIDADE DOS DADOS

AS ATUALIZAÇÕES SÃO COMPARTILHADAS ENTRE OS PARTICIPANTES DO SISTEMA

INTRODUÇÃO

DIGITAL EVIDENCE

É QUALQUER INFORMAÇÃO PROBATÓRIA ARMAZENADA OU TRANSMITIDA EM FORMATO DIGITAL QUE UMA PARTE DE UM CASO JUDICIAL POSSA USAR NO JULGAMENTO.



INTRODUÇÃO

EXEMPLOS DE APLICAÇÕES



VERMONT (2016), ARIZONA
(2017), E OHIO (2018)



SMART CONTRACTS



SUPREMO TRIBUNAL POPULAR
DA CHINA (2018)



ARMAZENAMENTO E AUTENTICAÇÃO DE
EVIDÊNCIAS DIGITAIS



↑ DE EFICIÊNCIA + ↓ CUSTO



PROGRAMA PILOTO



DESAFIOS:
COMPARTILHAMENTO DE EVIDÊNCIAS
GERENCIAMENTO DE IDENTIDADES



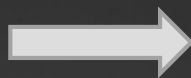
PROBLEMA

PROBLEMA



PROBLEMA

↑ USO DE COMPUTADORES E INTERNET

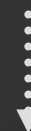


↑ CRIMINALIDADE DIGITAL

PERÍCIA DIGITAL



NÃO HÁ NENHUM TIPO DE PROCEDIMENTO LEGALMENTE PUBLICADO NO
BRASIL REGULAMENTANDO AS ETAPAS



FALTA DE CONHECIMENTO JURÍDICO OU TÉCNICO PODE VIOLAR A
INTEGRIDADE DO MATERIAL QUESTIONADO

PROBLEMA

LEGISLAÇÃO BRASILEIRA

CÓDIGO DE PROCESSO PENAL (CPP), DECRETO DE LEI N.º 3.689, DE 3 DE OUTUBRO DE 1941

“ART. 6º - LOGO QUE TIVER CONHECIMENTO DA PRÁTICA DA INFRAÇÃO PENAL, A AUTORIDADE POLICIAL DEVERÁ:

I - DIRIGIR-SE AO LOCAL, PROVIDENCIANDO PARA QUE **NÃO SE ALTEREM O ESTADO E CONSERVAÇÃO DAS COISAS**, ATÉ A CHEGADA DOS PERITOS CRIMINAIS.”

“ART. 159 - O EXAME DE CORPO DE DELITO E OUTRAS PERÍCIAS SERÃO REALIZADOS POR PERITO OFICIAL, PORTADOR DE **DIPLOMA DE CURSO SUPERIOR**.

§ 1º - NÃO HAVENDO PERITOS OFICIAIS, O EXAME SERÁ REALIZADO (...) PORTADORAS DE DIPLOMA DE CURSO SUPERIOR, (...) TIVEREM **HABILITAÇÃO TÉCNICA RELACIONADA À NATUREZA DO EXAME**.”

PROBLEMA

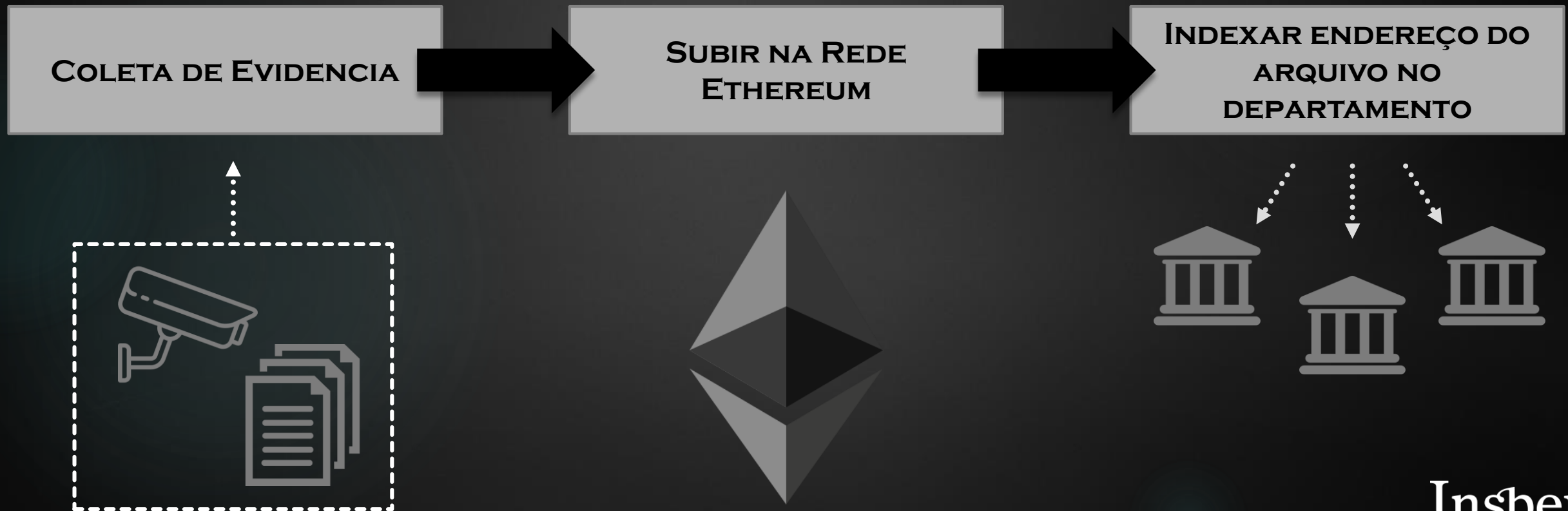




SOLUÇÃO

SOLUÇÃO

O BLOCKCHAIN OFERECE CRIAÇÃO E GERENCIAMENTO DE ATIVOS DE REGISTROS DIGITAIS
CRIPTOGRAFADOS, IMUTÁVEIS E SEGUROS.





VANTAGENS

VANTAGENS



TRANSPARÊNCIA



SEGURANÇA



COMPARTILHAMENTO



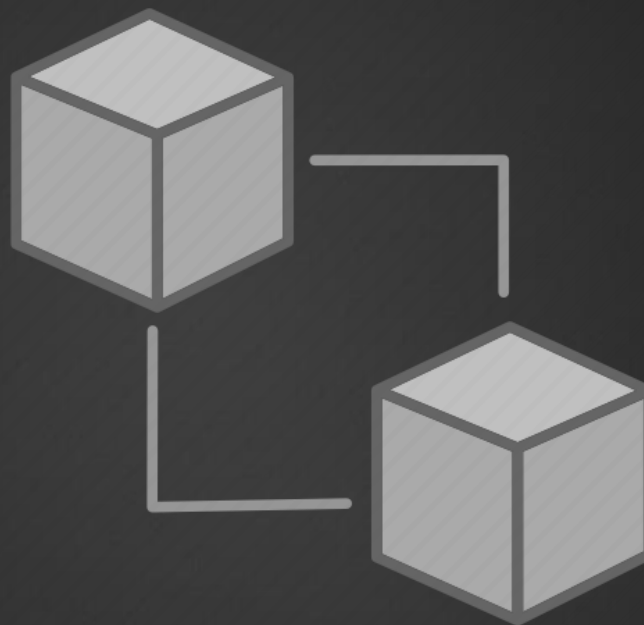
ARMAZENAMENTO

VANTAGENS



TRANSPARÊNCIA

O BLOCKCHAIN GERARIA EFICIÊNCIA PARA AS ENTIDADES E TRANSPARÊNCIA PROCESSUAL PARA OS USUÁRIOS DEVIDO AO FÁCIL ACESSO A INFORMAÇÃO.



A IMUTABILIDADE DOS REGISTROS DIGITAIS ESTÁ INSERIDA NA TECNOLOGIA BLOCKCHAIN. ISSO É ESPECIALMENTE IMPORTANTE EM UMA ERA DE FOTOS E VÍDEOS FALSOS QUE MINAM A CONFIANÇA DO PÚBLICO.



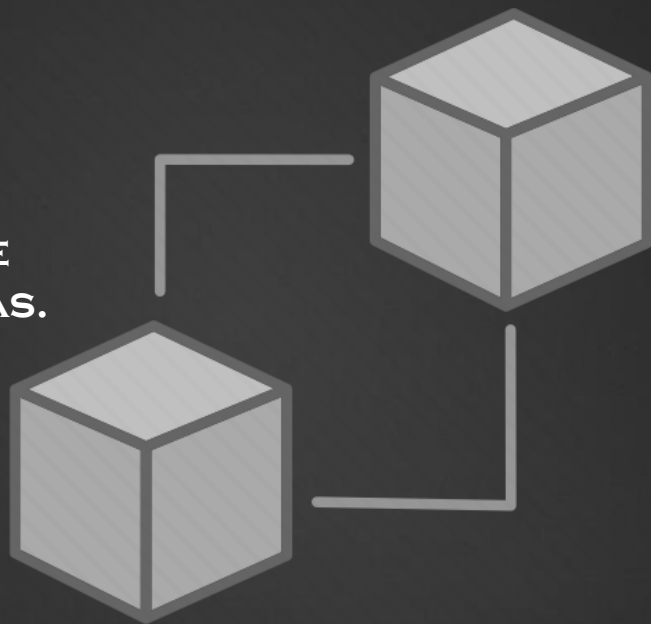
SEGURANÇA

VANTAGENS

OS ATIVOS DIGITAIS PRESENTES NA
BLOCKCHAIN PODEM SER
COMPARTILHADOS DE MANEIRA FÁCIL E
SEGURA ENTRE AS PARTES INTERESSADAS.



COMPARTILHAMENTO



ARMAZENAMENTO

CAPACIDADE DE ARMAZENAMENTO DE
ATIVOS.

A high-contrast, black and white photograph of several sprinters in mid-stride on a running track. The athletes are wearing various athletic gear, including tank tops and shorts. The image is dynamic, with long shadows cast on the track surface. A semi-transparent white rectangular box with rounded corners is centered over the image, containing the word "DESAFIOS" in a bold, black, serif font.

DESAFIOS

DESAFIOS



POR TRATAR-SE DE UMA REDE PEER-TO-PEER (P2P) ONDE SUA DISTRIBUIÇÃO OCORRE EM TODO O BRASIL, PROBLEMAS DE LATÊNCIA E CUSTO DE ARMAZENAGEM PODEM A SER UM PROBLEMA NO FUTURO.



EMBORA A ESTABILIDADE SEJA UMA DAS VANTAGENS DO BLOCKCHAIN, MUDANÇAS REGULATÓRIAS, ESPECIALMENTE LIGADAS A NOVAS LEIS PODEM EXIGIR MUDANÇAS NO CÓDIGO, O QUE OCASIONARIA EM UM HARD FORK, DIVIDINDO A BASE DE DADOS DAS EVIDÊNCIAS.

*SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE)
INTERNET ENGINEERING TASK FORCE (IETF)*



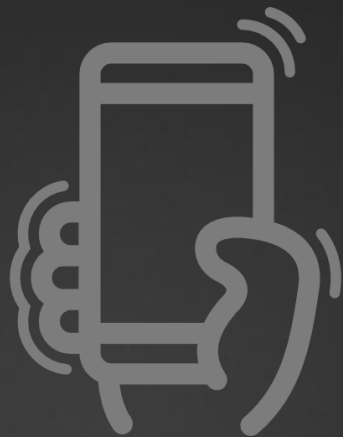
DAPP

Insper

DAPP



ARMAZENA ARQUIVOS
DE FORMA
DISTRIBUÍDA E
IMUTÁVEL – CUSTO DE
ESPAÇO EM DISCO
CONVENCIONAL



A INTERFACE DO USUÁRIO
COM A REDE BLOCKCHAIN É
INTERMEDIADA POR MEIO DE
UM SMART CONTRACT



ENVIA O ENDEREÇO
IPFS DA EVIDÊNCIA
PARA O ENDEREÇO
ETHEREUM QUE
REPRESENTA O
DEPARTAMENTO

SMART CONTRACT

2. Enviar para o departamento:

Endereço Ethereum do departamento: Endereço IPFS:

CRIA UMA TRANSAÇÃO NA BLOCKCHAIN ENTRE DOIS ENDEREÇOS, UM EMISSOR E UM RECEPTOR

ARMAZENA NOS ARGUMENTOS DESSA TRANSAÇÃO O ENDEREÇO IPFS DO ARQUIVO

BAIXO CUSTO POIS ENVOLVE O ARMAZENATO DE APENAS UMA STRING NO BLOCO

SMART CONTRACT


3. Receber Imagens


Receber IPFS


cria uma transação na blockchain, que recebe os dados de outra transação





DEMONSTRAÇÃO


 ACCOUNTS

 BLOCKS

 TRANSACTIONS

 CONTRACTS

 EVENTS

 LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
7

GAS PRICE
20000000000

GAS LIMIT
6721975

HARDFORK
PETERSBURG

NETWORK ID
5777


RPC SERVER
HTTP://127.0.0.1:7545


MINING STATUS
AUTOMINING

WORKSPACE
QUICKSTART

SAVE

SWITCH












MNEMONIC 

HD PATH

royal frost table unique clever position risk shop scale great churn torch

m/44'/60'/0'/0/account_index

ADDRESS 0xfddFEd00ce690E9b4303061d3aCD2157cAb92324	BALANCE 100.00 ETH	TX COUNT 0	INDEX 0	
ADDRESS 0x1Eba2F19955327F676F22C1e1f22710d72cD22C1	BALANCE 100.00 ETH	TX COUNT 3	INDEX 1	
ADDRESS 0x69905b9C3Ae9eFfeA3E37E62948C5779e6825412	BALANCE 100.00 ETH	TX COUNT 4	INDEX 2	
ADDRESS 0xAE6F4b55342Ace01caD4Bf0c52874D856F1bFF03	BALANCE 100.00 ETH	TX COUNT 0	INDEX 3	
ADDRESS 0xB6D3c4368094941f45a6eE494685d3F78888963F	BALANCE 100.00 ETH	TX COUNT 0	INDEX 4	
ADDRESS 0x134b65C069386781EfBed15af50478DFE4e9C544	BALANCE 100.00 ETH	TX COUNT 0	INDEX 5	
ADDRESS 0xE3beeB0df03d2336D70C8E976fEE4a795a894DB8	BALANCE 100.00 ETH	TX COUNT 0	INDEX 6	
ADDRESS 0x0C9bd0EeB1FB519eFc46FD7bD1246240a7d6a64E	BALANCE 100.00 ETH	TX COUNT 0	INDEX 7	



Q&A