

Notary

Elisa Malzoni
Raphael Costa
Victor Hugo
Vinicius Bonelli

O que é Notary?

- **Notarization** é o processo de assegurar que as partes de um documento são autênticas e são confiáveis
- No Brasil, cartório.
- Há diversos tipos, dentre eles: Registro Civil, Autenticação de Documentos, Compra de imóveis entre outros
- O processo é dividido em três etapas:
 - Verificação
 - Certificação
 - Registro

Qual o problema?

- Processo altamente burocrático com pouca automatização.
- Necessita de recurso humano para manter o processo.
- Armazenamento de informações rudimentar, a base de livros. Com isso, dificulta buscas futuras.
- Registros são mutáveis.

Por que Blockchain?

- Os recursos e/ou dados são compartilhados entre as partes?
- Sua solução precisa de um intermediário para auditoria?
- Há problemas de confiança entre as partes envolvidas?
- Você abre mão de desempenho computacional?
- Você não precisa de uma solução distribuída?
- Está disposto a pagar mais caro que uma solução tradicional?

Benefícios

- Facilmente auditável
- Contratos imutáveis
- Confiabilidade
- Segurança
- Rapidez

Malefícios

- Não exclui completamente o intermediário
- Certa concentração
- Muitos dados podem demorar para ser processados

Proof of Existence

Prova que um documento/arquivo/media foi criado em um determinado período do tempo.

Armazena uma hash, que identifica o documento criado, e também o timestamp de quando a criação ocorreu.

Proof of Ownership

Autêntica quem é o dono de um determinado documento.

A ideia é armazenar os dados do usuário ou uma assinatura digital ao se criar um contrato. Assim, sempre que houver a necessidade de se consultar a propriedade, basta ter a hash do documento e os dados do usuário estarão junto.

Essa funcionalidade também é um requerimento para implementar a troca de propriedade de documentos.

Document Ownership Transfer

Transferência de propriedade de algum documento para outra pessoa ou entidade.

Modifica os dados do usuário a quem pertence um determinado contrato. É necessário saber qual a hash do documento para fazer a modificação.

Código

Para cumprir as 3 funcionalidades citadas:

- Armazenamos o hash (SHA-256) de um arquivo, associado a uma estrutura Document, que tem como atributo a chave do usuário dono do documento e a data em que foi efetuada (timestamp).

```
struct Document {  
    address signature;  
    uint256 timestamp;  
}  
  
mapping(bytes32 => Document) documents;
```

getDocument

Recebe o hash de um documento e retorna a assinatura do dono e a hora em que foi armazenado.

```
function getDocument(bytes32 docHash) public view returns(address, uint256) {  
    address owner = documents[docHash].signature;  
    uint256 timestamp = documents[docHash].timestamp;  
    return (owner, timestamp);  
}
```

writeDocument

Recebe o Hash de um arquivo e o associa a um Document.

```
function writeDocument(bytes32 docHash) public returns(bool) {  
    require(documents[docHash].timestamp == 0, "Document already exists, to update use updateOwner");  
    documents[docHash].signature = msg.sender;  
    documents[docHash].timestamp = now;  
    return true;  
}
```

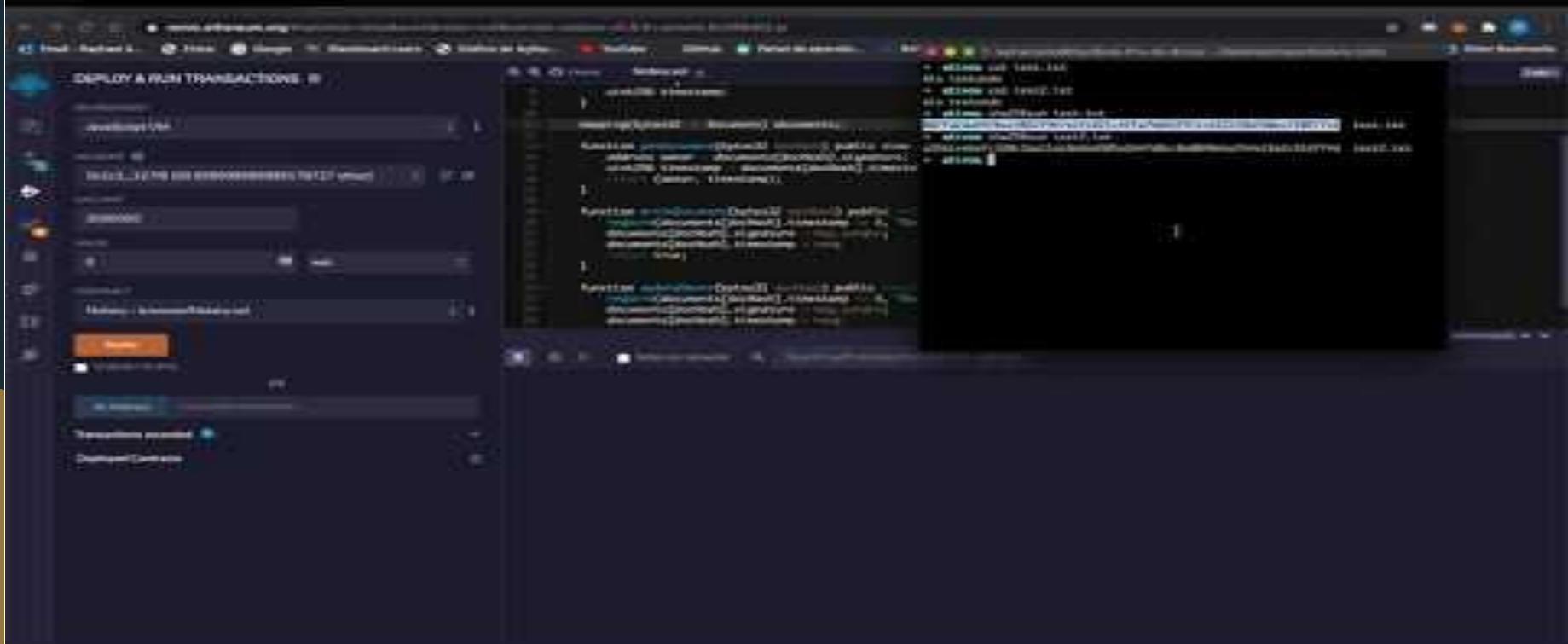
updateOwner

Verifica se existe o documento, se existir, atualiza a chave do dono do documento para o do novo usuário

```
function updateOwner(bytes32 docHash) public returns (bool) {  
    require(documents[docHash].timestamp != 0, "Document doesn't exist, use writeDocument to create new");  
    documents[docHash].signature = msg.sender;  
    documents[docHash].timestamp = now;  
    return true;  
}
```



DEMO



Referências

Explica a funcionalidade de Proof of Existence

<https://medium.com/@kctheservant/notarization-in-blockchain-part-1-a9795f19e28d>

Explica a funcionalidade de Proof of Ownership e detalha como é fácil fazer utilizando smart contracts

<https://medium.com/@kctheservant/notarization-in-blockchain-part-2-1a06d00eb72>

Explica a funcionalidade de Ownership Transfer

<https://medium.com/@kctheservant/notarization-in-blockchain-part-3-ce176c1ac338>