Blockchain e **IPFS** para **registro** e **autenticidade** de **certificações**

Maurício Witter

Tópicos

- Transações
- Wallets
- Smart Contracts
- EVM
- Padrões de Contratos
- Mainnet e Testnet

Transações

- Transações públicas
- Chaves públicas e privadas
- Assinatura digital (Private key + ECDSA)
    - Transação é autorizada pelo detentor legítimo correspondente ao endereço do remetente;
    - O remetente disponibiliza publicamente sua chave pública.
    - O destinatário utiliza a chave pública do remetente para verificar a assinatura digital;
    - Prevenção de falsificação (carteiras públicas);
    - Transações legítimas, transparentes e confiáveis.

Wallets

- A carteira é baseada na chave **pública** e **privada**;
- A **chave pública** pode ser **vista por todos**;
- A **chave privada** apenas o **dono** da carteira **possui**;
- **Perder a chave privada** incorre em **perder a carteira** e tudo que tem nela.

Smart Contracts

- Nick Szabo — BitGold (1994-1998)
- Bitcoin
- Ethereum
- EVM (Ethereum Virtual Machine)
- Descentralização
- Elimina a burocracia

Um **contrato inteligente** é uma forma de **descrever a lógica** de um **contrato físico** de forma **digital**.

Esse código possui **propriedades fundamentais** da Blockchain, como **execução autônoma**, operações **irreversíveis**, **imutabilidade** e operações **transparentes** e **auditáveis** em tempo real.

Entre outra aplicações, contratos inteligentes podem **enviar**, **receber** e **armazenar** ativos digitais e **interagir** com **outros** contratos inteligentes ou **qualquer** sistema computacional conectado à internet.

Imaginando a **segurança de um carro**, a estratégia dos **contratos inteligentes** visa aprimorar os métodos de segurança progressivamente. Esses métodos **garantem que apenas o detentor legítimo** do veículo, de acordo com os **termos do contrato**, possua **controle sobre as chaves criptográficas** para operá-lo. Em sua forma mais básica, o veículo só pode ser ativado quando o proprietário legítimo completa um procedimento específico, impedindo roubos.

— Nick Szabo

EVM (Ethereum Virtual Machine)

- Blockchain (**Second-generation**)
- **Máquinas** de **estado programáveis**
- Aplicativos Descentralizados (**dApps**)
- Finanças Descentralizadas (**De-FI**)
- **Solidity** (Turing Complete)
- **Bytecode**

Padrões de Contratos

- **ERC-720**: Token Standard
- **ERC-777**: Decentralized Exchanges Token Standard
- **ERC-721**: Non-Fungible Token Standard
- **ERC-1155**: Multi-Token Standard

Mainnet e Testnet

- **Mainnet** representa a **blockchain real**, onde tudo é fundamentalmente **imutável**.
- **Testnet** é uma rede que **simula** a mainnet, possibilita desenvolvedores e pesquisadores a implantar código **testável**, fazer auditorias e **experimentações**.
    - **Transações** podem ser feitas com **ativos digitais** sem **valor intrínseco** .

Implicações

- Automação e execução confiável
- Descentralização e segurança
- Redução de custos e eficiência
- Disrupção em diversos setores
- Tokenização e novos modelos de negócio
- Desafios Legais e Regulatórios
- Acessibilidade global e inclusão

O que foi feito ?

- **Deploy** do contrato na testnet da Fantom
- Começar a **desenvolver** Plataforma Web
- **Consumir** os Smart Contracts (Parcialmente)

https://testnet.ftmscan.com/address/0x512A67C88DE5e5bF0E01598D197bb3dda860bb17

```
issueCertificate(
      string memory studentName,
      string memory institutionName,
      string memory degree,
      string memory studentEmail,
      string memory cidHash
)


  getCertificateByStudentEmail(string memory studentEmail) returns (
        address institution,
        string memory institutionName,
        string memory studentName,
        string memory degree,
        string memory cidHash,
        uint256 timestamp
  )
```

Próximos passos...

- **Registro** de certificações
- **Testar** contratos
- **Verificar** registro de certificações

Recapitulando

- **Sistema atual** baseado em **confiança** em **instituições**
- **Sistema** proposto **autônomo**, **descentralizado** e **confiável**
- **Smart contracts** são **contratos programáveis digitais**
- **Smart contracts** são **executados** em uma **Blockchain**
- Utiliza **chaves criptográficas** e **assinaturas digitais** seguras

Referências

- Szabo, Nick. Formalizing and Securing Relationships on Public Networks. 1997.
- KHAN, S. et al. Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability. IEEE Access, v. 9, p. 116672–116691, 20 ago. 2021. ISSN 2169-3536.
- XU, X. et al. A taxonomy of blockchain-based systems for architecture design. 2017 IEEE International Conference on Software Architecture (ICSA), p. 243–252, 18 abr. 2017. 8

Dúvidas?

Obrigado!

 @rwietter

 @rwietter

 /in/rwietter

Slides, repositório, proposta e artigo