Sistemas Distribuídos: uma aplicação baseada em Blockchain e IPFS para registro e autenticidade de diplomas e certificações

Maurício Witter

14 de novembro de 2023

Conteúdo

Lista de Figuras

1 INTRODUÇÃO

A emissão e autenticação de diplomas e certificados estudantis é uma questão crucial no cenário educacional. Diplomas falsos e a dificuldade em verificar a legitimidade desses documentos são alguns dos desafios para serem resolvidos quando fala-se em internet decentralizada, transparente e segura. Nesta proposta, espera-se explorar o potencial da tecnologia Blockchain aliado ao protocolo *InterPlanetary File System* (IPFS) para resolver esse problema, ao criar um sistema global e permitir que as instituições de ensino emitam diplomas de forma segura e transparente.

A tecnologia Blockchain é um Sistema Distribuído bem estabelecido e conta com milhares de aplicações que extrapolam o sistema financeiro e servem para dar maior segurança, transparência e integridade dos dados. Conforme [10], as transações feitas por meio do sistema são armazenadas em blocos, que são então interligados em cadeia e, assim, organizados em ordem cronológica. Mas o maior benefício é que as transações escritas em blocos são imutáveis e transparentes para todos os pares.

1.1 BENEFÍCIOS

- Imutabilidade: a Blockchain é conhecida por sua imutabilidade. Uma vez que os dados são registrados na Blockchain, eles não podem ser alterados sem a concordância da maioria dos participantes da rede. Isso ajuda a garantir a autenticidade dos registros e diplomas.

- Rastreabilidade: os registros de diplomas podem ser rastreados na Blockchain, o que permite verificar se um diploma foi emitido pela universidade legítima.

- Armazenamento distribuído: o uso do IPFS para armazenar os arquivos PDF dos diplomas ajuda a descentralizar o armazenamento e evita a dependência de um único ponto de falha.

1.2 LIMITAÇÕES

- Entrada de dados falsos: mesmo com o sistema de Blockchain e IPFS, a entrada de dados falsos (nomes, CPFs, etc.) ainda é uma possibilidade se não houver verificações rigorosas durante o processo de emissão.

- Ataques externos: enquanto a Blockchain é resistente a alterações internas, ataques externos à infraestrutura, como um ataque ao servidor do back-end, podem comprometer a integridade dos registros antes de serem armazenados na Blockchain.

- Armazenamento distribuído: o uso do IPFS para armazenar os arquivos PDF dos diplomas ajuda a descentralizar o armazenamento e evita a dependência de um único ponto de falha.

2 OBJETIVOS GERAIS E ESPECÍFICOS

O objetivo geral deste trabalho é desenvolver uma aplicação que aproveite da tecnologia Blockchain para desenvolver um sistema distribuído e decentralizado para autenticar diplomas e certificados estudantis.

2.1 OBJETIVOS ESPECÍFICOS

- Implementar um contrato inteligente na Blockchain Fantom que registre os detalhes dos diplomas, incluindo metadados e hashes dos documentos.
- Integrar a aplicação com o protocolo IPFS para armazenar os dados brutos dos diplomas de forma imutável e descentralizada.
- Criar uma interface de usuário amigável que permita que as instituições de ensino enviem os diplomas para autenticação.
- Testar e avaliar a aplicação em termos de segurança, eficiência e usabilidade.

3 REVISÃO BIBLIOGRÁFICA

A literatura revela algumas abordagens de utilização de Blockchain com IPFS e outras formas de autenticar e gerenciar diplomas e certificados estudantis. SOUZA, CARNEIRO E COUTINHO, propõe uma aplicação para geração e validação de diplomas digitais através do uso da tecnologia Blockchain da *Ethereum* para a geração de *non-fungible tokens* (NFT's), que representam os documentos criados. Eles estariam distribuídos globalmente através do protocolo IPFS.

Segundo a Lei de Diretrizes e Bases da Educacão (LDB, Lei 9394/1996), as instituições de ensino superior (IES) são responsáveis pela emissão, registro e manutenção dos registros dos diplomas por ela emitidos. A Portaria No. 1.095/2018 do Ministério da Educação (MEC) estabelece que os registros dos diplomas podem ser realizados por meios f ́ısicos ou eletr ̂onicos, atendendo o que preconiza a Lei No. 8159/91 e a Norma Técnica 391/2013, do MEC (SOUZA, CARNEIRO E COUTINHO).

Em 2018, o MEC instituiu através da Portaria No. 330/2018 a criação do diploma digital para instituições federais de ensino com o objetivo de modernizar o fluxo processual para emissão e registro de diploma de graduação (SOUZA, CARNEIRO E COUTINHO).

BARROSO tem uma proposta parecida, mas utiliza Blockchain Solana, devido aos altos custos de trnasação da Blockchain Ethereum. Também inclui a validação do emissor (IES) certificado pelo ICP Brasil.

Outras soluções para tal problemática são BC Diploma e Block Certs

A solução proposta difere parcialmente das outras pois tem como objetivo utilizar a Blockchain Fantom para criar *smart contracts*, com isso haverá menores taxas de transação e mais velocidade para submeter a criação do diploma/certificação.

Alguns desafios, para o reconhecimento do MEC, o membro de uma Instituição de ensino qualificada pelo Ministério da Educação (MEC) precisa estar em posse de um certificado

digital emitido pela ICP Brasil e ser responsável por usar o sistema para assinar digitalmente e emitir os diplomas (BARROSO). Ou seja, afim de provar que uma instituição emissora de um documento´e de fato quem ela diz ser, ou seja, autenticar instituições emissoras de diplomas na rede (SOUZA, CARNEIRO E COUTINHO).

4 METODOLOGIA

Primeiramente, será feita uma revisão bibliográfica a cerca das tecnologias apresentadas afim de obter maior compreensão sobre o projeto. Em seguida será feito o desenvolvimento prático para, de fato, construir o sistema distribuído abordando tais tecnologias.

4.1 FERRAMENTAS

- Blockchain: Fantom
- Contratos Inteligentes: Solidity
- Armazenamento de Dados: IPFS
- Interface de Usuário: Next
- Backend: Node
- Gerenciamento de Estado: Zustand
- Biblioteca Web3: web3.js

4.1.1 Blockchain

A Blockchain surgiu como uma tecnologia para registos de transações descentralizadas seguras com amplas aplicações em sistemas financeiros, cadeias de abastecimento, saúde entre outras. Entretanto, um sistema distribuído a prova de falhas era um problema em aberto e altamente complexo de se resolver. Foi então que surgiu os algoritmos de prova de consenso, com base na tolerância a falhas bizantinas, abordada em sistemas de bases de dados distribuídas, nos quais até um terço dos nós participantes podem estar comprometidos (LAMPORT apud CHOI Sang-Min, et al., 2018). Os algoritmos de consenso garantem a integridade das transações entre participantes numa rede distribuída. Assim, foi proposto um grande número de algoritmos de consenso. Entre os principais, por exemplo, estão o protocolo de consenso Proof of Work (PoW) de Nakamoto na Blockchain Bitcoin. Outras Blockchains como a Fantom utilizam o protocolo de consenso Proof Of Stake (PoS).

A tecnologia Blockchain possui Blocos (Block) e Cadeias (Chain). Um bloco é formado por um conjunto de transações que acontecem na rede. A cadeia é onde os blocos são interligados de forma que o próximo bloco contenha o hash do bloco anterior. Ou seja, mesmo uma pequena alteração no bloco anterior pode alterar seu hash e quebrar toda a cadeia, desta forma, qualquer um que tentar fazer uma alteração em um ou mais blocos, terá que alterar em todos os blocos anteriores (ROSSETTO e GOMES, 2022).

O PoW é o algoritmo de consenso usado na Blockchain do Bitcoin. Os participantes (mineradores) resolvem problemas computacionais complexos para adicionar blocos à Blockchain. Isso requer um consumo significativo de energia, mas é considerado seguro e resistente a ataques.

O PoS é um algoritmo de consenso alternativo que não envolve a resolução de problemas computacionais. Em vez disso, os participantes são escolhidos para criar blocos com base na quantidade de ativos que possuem e estão dispostos a "apostar"como garantia. O PoS é mais eficiente em termos de energia, mas ainda garante segurança.

4.1.2 Fantom

A Fantom é uma plataforma de contratos inteligentes, descentralizada, de código aberto, rápida e de alto rendimento para ativos digitais e dApps.

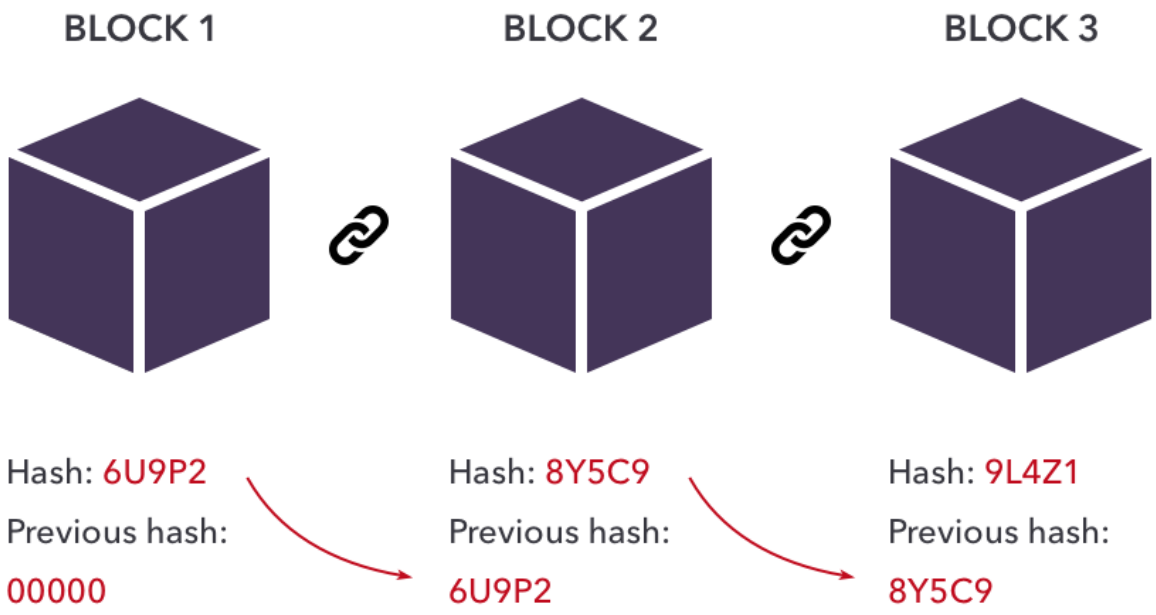
A Fantom, por outro lado, utiliza o *Lachesis* como algoritmo de consenso de rede. O protocolo *Lachesis* utiliza um mecanismo de consenso chamado *Directed Acyclic Graph* (DAG) conforme 2, que é uma estrutura de dados que não depende de mineradores ou validadores específicos para criar blocos. Em vez disso, os participantes da rede são responsáveis por validar as transações e adicionar blocos ao DAG.

No Lachesis, cada validador possui seu próprio DAG local e cria blocos de transações recebidas, que são adicionados ao seu DAG. Os validadores trocam esses blocos de forma assíncrona, espalhando informações pela rede. Uma vez que a maioria dos validadores concorda com um bloco, ele é adicionado a rede principal da Fantom contendo todas as transações de consenso finais (FANTOM).

Fantom utiliza grande parte da Máquina Virtual Ethereum (EVM) no backend. Os contratos inteligentes são escritos em *Solidity* e podem funcionar no Fantom da mesma forma que no Ethereum (FANTOM).

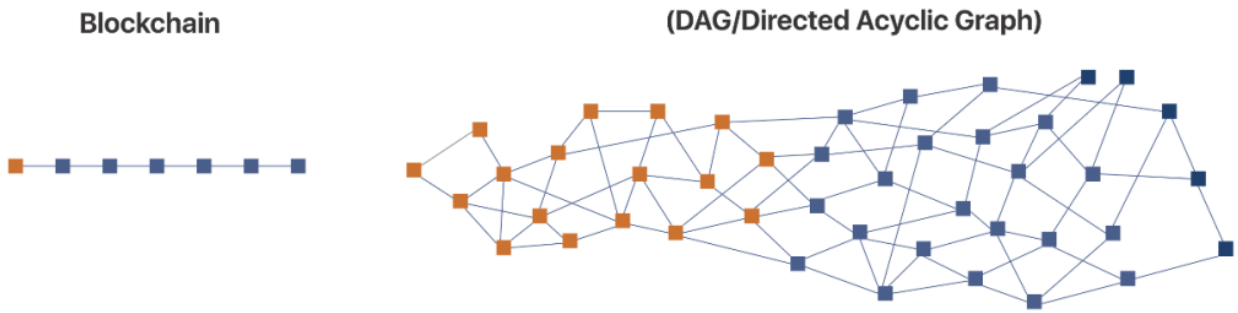
Um contrato inteligente é um "agente autônomo"armazenado na Blockchain, codificado como parte de uma transação de "criação"que introduz um contrato na Blockchain. Uma vez criado, é identificado por um endereço *hash*. O estado de um contrato consiste em duas partes principais: um armazenamento privado e a quantidade de moedas virtuais que ele detém. O código do contrato pode manipular variáveis como nos programas imperativos tradicionais. O código de um contrato da executável na Máquina Virtual da Ethereum (EVM) está em uma linguagem de bytecode. Os usuários definem contratos usando linguagens de programação de alto nível, por exemplo, Solidity, que são então compiladas no código EVM. Para invocar um contrato no endereço , os usuários enviam uma transação para o endereço do contrato. Uma transação normalmente inclui: pagamento (para o contrato) pela execução e/ou registro ou invocação de dados (LUU, et al., 2016).

Figura 1: Organização de blocos e cadeias na tecnologia Blockchain.



Fonte: HAPSE, 2022.

Figura 2: Linear Vs. Lachesis Directed Acyclic Graph



Fonte: Fantom Foundation.

4.1.3 Solidity

Solidity 3 é uma linguagem de alto nível orientada a objetos para implementação de contratos inteligentes na Máquina Virtual da Ethereum (EVM) e de Blockchains baseadas na EVM. Solidity possui tipagem estática, suporta herança, bibliotecas e tipos complexos.

Figura 3: Exemplo de código com estado em Solidity.

```
pragma solidity >=0.4.16 <0.9.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Fonte: Solidity.

4.1.4 IPFS (InterPlanetary File System)

IPFS é um sistema descentralizado e distribuído para armazenar e compartilhar qualquer tipo de conteúdo, independente do seu tamanho (por exemplo, texto, imagens, vídeos, PDFs) em uma rede ponto a ponto (Peer-to-Peer). Foi projetado para resolver algumas das limitações e ineficiências do modelo tradicional cliente-servidor para compartilhamento e armazenamento de arquivos.

Entre suas principais características estão a descentralização, o IPFS opera em uma rede ponto a ponto, o que significa que não há servidor central ou autoridade que armazene e controle os dados. Em vez disso, o conteúdo é distribuído por vários nós (computadores) na rede. Esta descentralização aumenta a resiliência e reduz o risco de censura ou pontos únicos de falha.

Os dados são endereçados usando Identificadores de Conteúdo (CIDs), que são hashes criptográficos gerados com base no próprio conteúdo. Ou seja, o endereço do conteúdo está diretamente vinculado ao seu conteúdo. Ao solicitar um conteúdo por seu CID, o conteúdo recebido será exatamente o mesmo. A alteração de um único *bit* do conteúdo por algum nó da rede faz com que o hash do conteúdo seja alterado e deixa de apontar para o conteúdo original, isso garante a segurança e integridade do conteúdo.

O IPFS, usa uma tabela hash distribuída (DHT) para ajudar a localizar conteúdo na rede. Quando alguém solicita um conteúdo, a rede ajuda a encaminhá-lo para a cópia mais próxima

desse conteúdo, reduzindo a latência e melhorando a velocidade de download. Além disso, o conteúdo pode ser acessado offline caso o nó tenha uma cópia local.

Devido ao endereçamento de conteúdo, o IPFS *desduplica* automaticamente os dados. Se os mesmos dados forem adicionados várias vezes, eles serão armazenados apenas uma vez na rede. Isso reduz os requisitos de armazenamento e o uso de largura de banda.

O IPFS ganhou popularidade em vários casos de uso, incluindo aplicativos descentralizados (dApps), entrega de conteúdo e arquivamento de dados, devido ao seu sistema de endereçamento de conteúdo descentralizado, imutável e eficiente. O IPFS é frequentemente usado em conjunto com a tecnologia Blockchain para várias aplicações, como armazenamento descentralizado, endereçamento de conteúdo e garantia de disponibilidade de dados mesmo quando o servidor de hospedagem está inativo.

5 CONCLUSÃO

A aplicação proposta oferece uma solução para a autenticação de diplomas e certificados usando Blockchain. Ao registrar dados na Blockchain e armazenar documentos brutos no IPFS, pode-se garantir a imutabilidade, a verificabilidade e a integridade dos registros.

À medida que o mundo avança em direção a um ambiente mais digitalizado e decentralizado, essa aplicação pode desempenhar um papel fundamental na validação confiável de credenciais educacionais.

A implementação proposta pode aumentar a confiança na autenticidade dos diplomas emitidos. No entanto, ela não é a prova de falhas, faz-se necessário realizar testes rigorosos, além da compreensão profunda das tecnologias utilizadas.

REFERÊNCIAS

[1] CHOI, S. M., PARK, J., NGUYEN, Q., CRONJE, A. *FANTOM: A Scalable Framework for Asynchronous Distributed Systems*. FANTOM Lab; FANTOM Foundation. 25, out. 2018. Disponível em <https://arxiv.org/abs/1810.10360>. Acesso em: 02 de set. 2023.

[2] HAPSE S.. *Blockchain 101: The Simplest Guide You Will Ever Read*. Velotio. 2022. Disponível em <https://www.velotio.com/engineering-blog/introduction-to-blockchain-and-how-bitcoin-works>. Acesso em: 02 de set. 2023.

[3] LUU L., CHU H. D, OLICKEL H., SAXENA P., HOBOR A.. **Making Smart Contracts Smarter**. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. Association for Computing Machinery, New York, NY, USA, 254–269. 2016. Disponível em <https://doi.org/10.1145/2976749.2978309>. Acesso em: 02 de set. 2023.

[4] ROSSETTO M. de G. A., GOMES O. de M.. Uma aplicação baseada em blockchain para registro de composições musicais. 2022. Disponível em <https://painel.passofundo.ifsul.edu.br/uploads/arq/20220729090836189628993 8.pdf>. Acesso em: 27 de ago. 2023.

[5] FANTOM. *Developer Documentation*. Disponível em <https://docs.fantom.foundation/>. Acesso em: 02 de set. 2023.

[6] SOLIDITY. *Introduction to Smart Contracts*. Disponível em <https://docs.soliditylang.org/en/v0.8.21/introduction-to-smart-contracts.html>. Acesso em: 02 de set. 2023.

[7] SOUZA, B. E., CARNEIRO E., COUTINHO A.. Geração e Validacão de Diplomas e Certificados utilizando Blockchain Pública. 2021. Disponível em <https://sol.sbc.org.br/index.php/wblockchain/article/view/17128/16966>. Acesso em: 01 de set. 2023.

[8] BARROSO L. R.. Emissão e validação de diplomas digitais usando a tecnologia Blockchain. 2023. Disponível em <https://repositorio.ufc.br/bitstream/riufc/73078/1/2023_tcc_rlbarroso.pdf>. Acesso em: 01 de set. 2023.

[9] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State. Blockchain-Based, Decentralized Access Control for IPFS. 2022. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1499-1506, doi: 10.1109/Cybermatics_2018.2018.00253. Disponível em <https://ieeexplore.ieee.org/document/8726493>. Acesso em: 25 de set. 2023.

[10] Q. Zhou, H. Huang, Z. Zheng, J. Bian. Solutions to Scalability of Blockchain: A Survey. 2023. IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218. Disponível em <https://ieeexplore.ieee.org/document/8962150>. Acesso em: 25 de set. 2023.

[11] P. Zheng, Z. Jiang, J. Wu, Z. Zheng. Blockchain-Based Decentralized Application: A Survey. 2023. IEEE Open Journal of the Computer Society, vol. 4, pp. 121-133,

2023, doi: 10.1109/OJCS.2023.3251854. Disponível em <https://ieeexplore.ieee.org/document/10068327>. Acesso em: 25 de set. 2023.

[12] S. Kravenkit, C. So-In. Zheng. Blockchain-Based Traceability System for Product Recall. IEEE Access, vol. 10, pp. 95132-95150, 2022, doi: 10.1109/ACCESS.2022.3204750. Disponível em <https://ieeexplore.ieee.org/document/9878306>. Acesso em: 25 de set. 2023.

[13] Dennis Trautwein, Aravindh Raman, Gareth Tyson, Ignacio Castro, Will Scott, Moritz Schubotz, Bela Gipp, Yiannis Psaras. Design and evaluation of IPFS: a storage layer for the decentralized web. 2022. Proceedings of the ACM SIGCOMM 2022 Conference (SIGCOMM '22). Association for Computing Machinery, New York, NY, USA, 739–752. https://doi.org/10.1145/3544216.3544232. Disponível em <https://dl.acm.org/-doi/10.1145/3544216.3544232>. Acesso em: 25 de set. 2023.