Geração e Validação de Diplomas e Certificados utilizando Blockchain Pública

Emerson de Brito Souza[1], **Elisângela Carneiro**[1], **Antonio Coutinho**[1]

[1]Departamento de Tecnologia – Universidade Estadual de Feira de Santana (UEFS)
Caixa Postal 15.064 – 91.501-970 – Feira de Santana – BA – Brasil

ebsouza@ecomp.uefs.br,{eocarneiro,acoutinho}@uefs.br

Abstract. *This article proposes a system for generating and validating diplomas and certificates where the documents are reliable and easily verifiable. The Ethereum public blockchain network combined with a distributed file network using the InterPlanetary File System protocol and open source tools was used. The model shows that the deployment of the system is feasible, encompassing properties of off-chain and on-chain systems for the proposed architecture.*

Resumo. *Este artigo propõe um sistema para a geração e validação de diplomas e certificados onde os documentos sejam confiáveis e facilmente verificáveis. Para isso foi utilizada a rede blockchain pública da Ethereum aliada com uma rede de arquivos distribuída usando o protocolo InterPlanetary File System e ferramentas de código aberto. O modelo mostra que a realização do sistema é viável, englobando propriedades de sistemas off-chain e on-chain para a arquitetura proposta.*

1. Introdução

Os diplomas e certificados são documentos oficiais categorizados como documentos arquivísticos, concedidos por uma instituição de ensino que declara que o portador cumpriu as exigências necessárias para obtenção de um grau ou título e estar apto para exercer determinada atividade. Estes documentos possuem devida importância para o portador, bem como para a sociedade. Por causa do seu valor, frequentemente estes documentos são alvos de pessoas mal-intencionadas que querem obter de maneira ilegal o status e os benefícios de um diploma (ou certificado).

A falsificação de diplomas não é um problema recente e enfrentado apenas pelo Brasil. No entanto, esta questão tem atraído atenção tanto das instituições de ensino, quanto de organizações internacionais e empregadores. Em 2018, a Operação Nota Zero realizada pela Polícia do Rio de Janeiro, detectou que cerca de 350 mil diplomas foram falsificados em cinco anos[1]. A falsificação de informações prestadas em currículos de profissionais que diziam possuir títulos acadêmicos demonstram quão custosa é a verificação da veracidade das informações contidas nos currículos[2].

Atualmente, a validação de créditos acadêmicos e a emissão de certificados de grau acadêmico no sistema educacional brasileiro ocorrem de forma semi ou totalmente

[1]Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2018/09/24/policia-do-rio-faz-operacao-de-combate-a-emissao-de-diplomas-escolares-falsos.ghtml>. Acesso em: 10 set. 2020.

[2]Disponível em: <https://brasil.elpais.com/brasil/2020-06-26/ministro-da-educacao-foi-reprovado-em-tese-e-nao-tem-o-doutorado-que-divulgava/no-curriculo.html>. Acesso em: 10 set. 2020.

não informatizada, facilitando a ocorrência de fraudes. Segundo a Lei de Diretrizes e Bases da Educação (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 físicos ou eletrônicos, atendendo o que preconiza a Lei No. 8159/91 e a Norma Técnica 391/2013, do MEC.

O Governo Federal vem traçando políticas que promovam a digitalização de documentos e automatização das tarefas para combater as falsificações. 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 [MEC 2018]. No ano seguinte, através da Portaria No. 554/2019, o MEC estabeleceu os termos e o prazo (ano de 2021) para a implementação do diploma digital pelas IES públicas e privadas do sistema federal de ensino.

A geração de certificados e diplomas exige confiança no órgão emissor. Muitas vezes, esse processo é burocrático e custoso devido à fragmentação de uma organização em diversos setores, sendo também suscetível à diferentes fraudes. A substituição do processo de emissão dos documentos físicos por um sistema computacional seguro torna o processo mais rápido e confiável. Com os avanços da tecnologia blockchain [Greve et al. 2018] e o emprego dos contratos inteligentes (*smart contracts*) [Szabo 1997] é possível a criação e validação de diplomas digitais de forma segura, imutável, descentralizada, rastreável, eliminando fraudes através de uma solução robusta e confiável.

Este trabalho apresenta a proposta de uma aplicação para a geração e validação de diplomas digitais através do uso da tecnologia blockchain pública da *Ethereum* [Buterin 2013] para geração de *non-fungible tokens* (NFT's) [Ethereum 2021] que representam os documentos criados no sistema. O conteúdo dos diplomas e certificados é armazenado em um sistema de arquivos distribuído globalmente através do protocolo *InterPlanetary File System* (IPFS) [IPFS 2021]. Os usuários do sistema poderão interagir com a rede blockchain por meio de uma aplicação *web* convencional através da Internet. O sistema tem a finalidade de prover confiabilidade, transparência, imutabilidade e facilidade de verificação dos dados dos diplomas e certificados registrados na blockchain.

2. Trabalhos relacionados

Em 2016, o Massachusetts Institute of Technology (MIT) desenvolveu um padrão aberto chamado de Blockcerts para a geração e validação de certificados utilizando a tecnologia blockchain do Bitcoin. Os documentos digitais são registrados na blockchain e são assinados criptograficamente, tornando-os invioláveis e compartilháveis [MIT 2016].

Um estudo preliminar sobre o uso combinado das tecnologias blockchain, certificação digital e preservação digital para criação de uma plataforma especializada em autenticação e preservação de documentos digitais é apresentado por [Costa et al. 2018]. Como prova de conceito, foi construído um serviço público escalável e agnóstico para registro e verificação digital da autenticidade de documentos acadêmicos.

A proposta de solução apresenta por [Palma et al. 2019] delega a responsabilidade da emissão de diplomas de graduação para os contratos inteligentes. As universidades registram os eventos acadêmicos dos alunos como transações na blockchain *Ethereum* e um

contrato inteligente emite diplomas de graduação ao identificar que os alunos cumpriram todos os requisitos para a obtenção do título.

A Rede Nacional de Ensino e Pesquisa (RNP) em parceria com o MEC vem desenvolvendo o diploma digital através do uso da tecnologia blockchain, que promete modernizar os processos de emissão de documentos e dispensar a emissão e arquivamento de documentos de papel. A solução proposta é baseada no estudo realizado por [Costa et al. 2018]. Em 2020, a solução foi implementada em cinco instituições federais de ensino, devendo ser ampliada para mais instituições em 2021 [MEC 2018]. Outro projeto com o objetivo de validar certificações é proposto por Brasil Open Badge[3], que utiliza a tecnologia blockchain da *Ethereum* com foco na emissão de certificação digital por parte de empresas e instituições de ensino. O projeto Carteira de Cursos apresenta uma solução baseada em blockchain privada para as instituições de ensino [Carvalho 2019].

A nossa solução difere das propostas anteriores pelo uso de *smart contracts* em blockchain pública da rede *Ethereum* com a tecnologia de NFT's para a criação e registro de diplomas digitais. A prova de conceito apresenta o uso de tecnologias que permitem a integração de aplicações e a realização de testes do sistema. A solução proposta pode ser integrada facilmente aos sistemas de registros acadêmicos existentes nas IES.

3. Arquitetura proposta

A modelagem de um sistema que visa prover confiabilidade, transparência, imutabilidade e facilidade de acesso para emissão, assim como o registro e a verificação de diplomas e certificados deve considerar três questões principais: (1) a inserção de informações na blockchain; (2) a verificação das transações ocorridas na blockchain; e, (3) a alta disponibilidade ao acesso dos documentos produzidos e inseridos na blockchain.

Devido às característica de imutabilidade da blockchain, os dados armazenados não podem ser alterados tornando possível garantir as propriedades necessárias para os documentos arquivísticos, tais como: a organicidade, a unicidade, a confiabilidade e a autenticidade [Arquivo Nacional 2019]. As aplicações blockchain aliadas com *smart contracts* tornam-se mais flexíveis e interessantes, pois podem ser aplicadas em uma grande variedade de casos de uso, sendo um deles a geração de documentos.

Levando em consideração a flexibilidade proporcionada pelos *smart contracts* e a propriedade de imutabilidade das blockchains, é proposta neste trabalho a criação de um *smart contract* para a geração de *tokens* para representar um diploma. Os diplomas devem ser únicos, isto é, só deve existir uma única instância de tal documento na rede. Por isso, é interessante que o *token* pertença à categoria dos *NFTs*. Os *NFTs* são *tokens* criptográficos que podem ser utilizados para representar itens únicos [Ethereum 2021].

Apesar de ser possível conectar-se à blockchain para observar o histórico das transações, essa tarefa pode ser desafiante para um usuário final que não tenha intimidade com a tecnologia. Com o objetivo de promover a comunicação com a blockchain, tornando-a transparente para o usuário final, uma aplicação *web* foi adicionada à arquitetura do sistema de forma a eliminar o uso de ferramentas como *MetaMask* ou similares e facilitar o processo de verificação das informações pelos usuário finais.

[3]Disponível em: <https://bropenbadge.com>. Acesso em: 10 set. 2020.

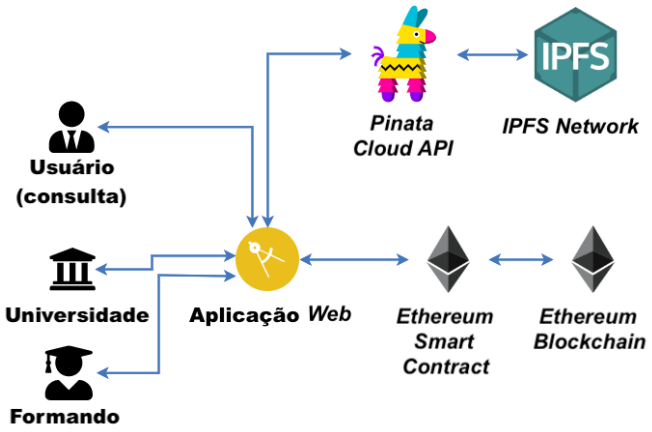

Figura 1. Arquitetura proposta para o sistema. Os usuários interagem com uma aplicação *web* responsável por realizar chamadas à IPFS e ao *smart contract*.

Um sistema é dito com alta disponibilidade se ele é capaz de resistir a falhas para prover serviços ou recursos pelo máximo de tempo possível. Como um sistema pode ser composto por várias entidades, quanto maior a replicação e redundância das informações menores serão os pontos únicos de falhas. Visando promover uma alta disponibilidade dos arquivos dos diplomas, é proposto que a arquitetura do sistema utilize a rede IPFS para realizar o armazenamento distribuído dos arquivos [IPFS 2021]. O modelo apresentado na Figura 1 consiste de uma aplicação *web* que comunica-se com a rede IPFS através da *Pinata Cloud API* [Pinata 2021]. A aplicação *web* comunica-se com o *smart contract* do NFT, que é então executado na *Ethereum Virtual Machine* (EVM).

4. Resultados

Nesta seção apresentaremos os resultados obtidos a partir da implementação do sistema para emissão e registro de diplomas de acordo com a arquitetura apresentada na Figura 1. O sistema possui três tipos de usuários: (1) o aluno que recebe o diploma ou certificado; (2) a instituição que certifica o aluno; e, (3) o usuário que deseja validar um diploma. Os usuários (1) e (2) precisam se cadastrar e autenticar no sistema para ter acesso às suas informações. No entanto, qualquer usuário pode verificar a veracidade de um diploma sem a necessidade de realizar cadastro ou autenticação.

A compilação e execução do *smart contract* é realizada através dos softwares *Truffle* [Truffle 2021] e *Ganache* que permitem a emulação da *Ethereum Virtual Machine* localmente e a observação do comportamento da aplicação. Quando uma blockchain é iniciada através do *Ganache* são gerados endereços das carteiras que devem ser vinculados aos usuários. No processo de cadastro, alunos e instituições devem informar o endereço de suas carteiras na rede *Ethereum*. O endereço da carteira é utilizado para a geração e transferência dos *tokens*. Em uma situação prática, as carteiras dos alunos e instituições devem existir previamente e serem gerenciadas pelos seus proprietários.

4.1. Geração e inclusão do diploma/certificado na blockchain

A instituição de ensino possui a lista dos alunos que satisfazem às condições para a geração do diploma. Ao preencher as informações dos alunos, a instituição submete o formulário ao servidor e o processo de geração do documento continua como segue:

1. O servidor gera o arquivo com as informações do aluno.
2. O servidor envia uma requisição contendo o arquivo criado para o serviço *Pinata Cloud*. O *Pinata* faz a comunicação com a rede IPFS, que armazena o arquivo. Em seguida, retorna para o servidor o *hash* do arquivo registrado na rede IPFS.
3. O servidor comunica-se com o *smart contract* invocando o método *awardDiploma()* enviando o endereço da carteira do aluno e o *hash* do arquivo na IPFS.
4. O *smart contract* gera o NFT e retorna os dados da transação para o servidor.
5. Por fim, o servidor salva no banco de dados o endereço da transação referente ao estudante e retorna uma mensagem de sucesso para a aplicação.

O *smart contract* desenvolvido estendeu o padrão ERC-721 que define a estrutura de um NFT. No contrato foi criado o método *awardDiploma()* que é responsável por vincular a referência do diploma na rede IPFS ao *token* gerado na blockchain.

A execução do *smart contract* gera um *token* e o padrão ERC-721 define que um evento do tipo *Transfer* deve ser disparado. Isso possibilita o armazenamento de informações nos *logs* da transação, sendo possível garantir a imutabilidade da informação armazenada. Além disso, como o *token* estará vinculado a apenas um recurso da rede IPFS, ele tornar-se-á único em todo o sistema, permitindo rastreá-lo através do código da transação ocorrida na blockchain ou através do identificador do *token*.

4.2. Visualização e busca dos documentos

Um aluno pode acessar a sua lista de diplomas e certificados na blockchain através da aplicação *web*. Deste modo é possível compartilhar o *hash* das transações para terceiros interessados em verificar a validade do diploma ou certificado. Um usuário pode possuir mais de um diploma ou certificado em sua carteira.

A busca por um diploma é feita através do *hash* da transação na blockchain. Quando um usuário deseja verificar o conteúdo do diploma, ele acessa a página relativa à validação no cliente *web* e informa o *hash* da transação em que o NFT do diploma foi gerado, submetendo o formulário de busca ao servidor como segue:

1. O servidor procura pelo *hash* da transação na blockchain.
2. Ao acessar as informações da transação, o servidor obtém o identificador do *token* que foi armazenado nos eventos do tipo *Transfer* da transação.
3. Em seguida, o servidor comunica-se com o *smart contract* invocando o método *tokenURI* e passa como argumento da chamada o identificador do *token*. O *smart contract* retorna o *hash* do recurso na rede IPFS para o servidor.
4. Por fim, o servidor retorna a *url* de acesso ao arquivo. Assim, usuário solicitante é capaz de acessar o arquivo e baixar o diploma.

5. Conclusões e trabalhos futuros

O projeto apresentado é uma solução viável para criação, registro e manutenção dos registros dos diplomas digitais através de um sistema seguro, de alta disponibilidade, que contribuirá para a redução de fraudes e verificação da veracidade das informações contidas em tais documentos. A solução utiliza a tecnologia blockchain para garantir confiabilidade, transparência e imutabilidade aos documentos, além de utilizar *smart contracts* para a geração de NFT's e IPFS para garantir a disponibilidade dos dados.

As instituições podem customizar a apresentação dos diplomas na aplicação *web* de acordo com o padrão usado alterando textos e imagens, dentre outros recursos. Assim, a solução pode ser acoplada aos sistemas acadêmicos existentes nas IES. Uma limitação encontrada no modelo proposto, mas que não está no escopo do trabalho, é provar que uma instituição emissora de um documento é de fato quem ela diz ser, ou seja, autenticar as instituições emissoras de diplomas na rede. Uma possível solução em trabalhos futuros pode ser vincular a carteira à instituição e tornar esta informação pública.

Referências

Arquivo Nacional (2019). Gestão de Documentos da Administração Pública Federal. Disponível em: ⟨http://www.arquivonacional.gov.br/images/conteudo/servicos_ao_governo/Capacitacao_treinamento/apostila_completa_2019_06.pdf⟩. Acesso em: 11 set. 2020.

Buterin, V. (2013). Ethereum whitepaper. Disponível em: ⟨https://ethereum.org/en/whitepaper/⟩. Acesso em: 20 out. de 2020.

Carvalho, R. (2019). Carteira de cursos baseados na tecnologia blockchain. *Trabalho de Conclusão de Curso, Escola Nacional de Administração Pública*, 1.

Costa, R., Faustino, D., Lemos, G., Queiroga, A., Djohnnatha, C., Alves, F., Lira, J., and Pires, M. (2018). Uso não financeiro de blockchain: Um estudo de caso sobre o registro, autenticação e preservação de documentos digitais acadêmicos. In *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações*. SBC.

Ethereum (2021). Non-fungible tokens (NFT). Disponível em: ⟨https://ethereum.org/en/nft/#what-are-nfts⟩. Acesso em: 23 maio 2021.

Greve, F. G., Sampaio, L. S., Abijaude, J. A., Coutinho, A. C., Valcy, Í. V., and Queiroz, S. Q. (2018). Blockchain e a revolução do consenso sob demanda. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos*.

IPFS (2021). Interplanetary file system. Disponível em: ⟨https://ipfs.io/⟩. Acesso em: 25 maio 2021.

MEC (2018). Diploma digital. Disponível em: ⟨http://portal.mec.gov.br/diplomadigital/⟩. Acesso em: 10 set. 2020.

MIT (2016). Blockcerts. Disponível em: ⟨https://www.blockcerts.org/about.html⟩. Acesso em: 11 set. 2020.

Palma, L. M., Vigil, M. A., Pereira, F. L., and Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in brazil. *International Journal of Network Management*, 29(3):e2061.

Pinata (2021). Pinata cloud. Disponível em: ⟨https://pinata.cloud/⟩. Acesso em: 30 maio 2021.

Szabo, N. (1997). The idea of smart contracts. Disponível em: ⟨https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html⟩. Acesso em: 25 out. 2020.

Truffle (2021). Truffle — overview. Disponível em: ⟨https://www.trufflesuite.com/docs/truffle/overview⟩. Acesso em: 25 maio 2021.