Uso da Blockchain para Gerenciamento de Certificados

André R. O. Cagliari, Gustavo Fonseca A. da Silva, Lucas P. Santos, Ismar Frango Silveira

[1]Ciência da Computação, Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie (UPM)

CEP: 01302-907 – Campus Higienópolis, São Paulo, SP – Brasil

andrer0dirgues01@gmail.com, gus.fonnseca@gmail.com, lucasp_santos@outlook.com, ismar.silveira@mackenzie.br

Abstract. *Certifications are designated executive credentials by an individual that verify their legitimacy and competence to perform a job. In the digital environment, it is extremely important that documents be tamper-proof, stored for the long term and easily verified. Nowadays, many models have a setback in some points for having centralized servers susceptible to unforeseen events, breaches or slow validation processes. In this article, the first concepts of a model that can solve these problems when using a blockchain are presented.*

Key-words: *blockchain, ethereum, smart contract, certificate*

Resumo. *Certificações são credenciais designadas obtidas por um indivíduo que verifica sua legitimidade e competência para realizar um trabalho. No meio digital, é de extrema importância que os documentos sejam invioláveis, armazenados a longo prazo e facilmente verificados. Hoje em dia, muitos modelos possuem um revés em um desses pontos por terem servidores centralizados passíveis a imprevistos, brechas de violação ou processos demorados de validação. Neste artigo, apresenta-se os primeiros conceitos de um modelo que pode solucionar esses problemas ao utilizar a blockchain.*

Palavras-chave: *blockchain, ethereum, smart contract, certificado*

1. Introdução

1.1 Contextualização e Relevância do Tema

Certificados são documentos que servem como evidência ou testemunho escrito, de status, qualificações, privilégios ou a verdade de algo. Após completar um bacharelado de Ciência da Computação, por exemplo, os certificados habilitam os formandos a serem intitulados como bacharel desse curso.

Os certificados podem ser entregues de forma física ou digital, no entanto, esses modelos possuem desvantagens:

> Os estudantes não conseguem acessar diretamente suas credenciais e acabam dependendo de terceiros. Se as organizações ou indivíduos cessam o armazenamento das credenciais, eles se tornam inválidos ou órfãos [...] O processo de verificação dos papéis tradicionais são lentos e podem tomar semanas após o pedido. [Jirgensons e Kapenieks 2018]

Além das dificuldades de manutenção, é perceptível os impactos causados por fraudes. Segundo Allen Ezell e John Bear (2005), existem diversas fábricas de diplomas falsos e a venda total ultrapassa meio bilhão.

Por essas razões, a existência de um sistema que possui certificados invioláveis, de fácil acesso e verificação é extremamente importante.

1.2 Objeto de Pesquisa

1.2.1 Contextualização do Problema de Pesquisa

Atualmente, muitos modelos de gerenciamento de certificados possuem um revés em um dos pontos apresentados na seção 1.1 por terem servidores centralizados passíveis a imprevistos, brechas de violação ou processos demorados de validação.

Neste contexto, a seguinte pergunta será respondida nesta pesquisa: Um sistema de gerenciamento de certificados baseado na blockchain pode resolver os principais problemas encontrados pelo setor?

1.2.2 Hipótese

A criação de uma aplicação descentralizada que permite o gerenciamento de certificados na blockchain possibilitará que os certificados sejam únicos, facilmente verificados por meio de seus códigos e permanentes.

1.3 Objetivos do Estudo

1.3.1 Objetivo Geral

O presente trabalho tem por objetivo final o desenvolvimento de uma aplicação que permita o gerenciamento e a verificação de certificados na blockchain, verificando como o modelo se comporta perante os problemas existentes no ciclo de vida dos certificados.

1.3.2 Objetivos Específicos

O estudo apresenta os seguintes objetivos específicos:

1. Estudar os princípios da blockchain;
2. Tornar o armazenamento de certificados permanentes, sem precisar manutenir registros ou banco de dados diretamente;
3. Utilizar a blockchain para que os certificados sejam invioláveis, combatendo tentativas de fraude;
4. Permitir uma validação confiável, direta e simplificada dos certificados;
5. Criar uma aplicação de alta disponibilidade por não rodar em poucos servidores e sim na blockchain;

1.4 Justificativa

Nota-se que a blockchain já possui as características necessárias para combater os problemas de longa data dos portadores e verificadores de certificações como emissão à prova de violação, armazenamento permanente e validação facilitada por meio dos códigos criptografados.

Por essas razões, busca-se entender e desenvolver uma plataforma baseada nessa tecnologia que vem sendo cada vez mais utilizada atualmente.

2. Metodologia da Pesquisa

Em relação à metodologia empregada neste TCC, o trabalho iniciou com a revisão da literatura específica sobre o tema da pesquisa. A revisão em questão teve foco nos conceitos fundamentais da blockchain e nas técnicas utilizadas em plataformas de gerenciamento de certificados.

Os fundamentos teóricos foram obtidos através de artigos científicos, sites, cursos e vídeos.

A metodologia também envolveu estudos de casos de sucesso das plataformas que utilizam a blockchain para gerenciamento de certificados, como a do MIT que utiliza a rede do Bitcoin.

Em seguida, foi analisado os conceitos de sistemas distribuídos, como o IPFS (sistema de arquivos interplanetário), e também desenvolvido um produto mínimo viável de uma plataforma para gerenciamento de certificados usando a linguagem Solidity para o desenvolvimento dos contratos inteligentes e a linguagem Javascript para as lógicas da interface.

Após a finalização do desenvolvimento e a análise de sua eficiência, as conclusões finais foram consolidadas e documentadas na composição final do trabalho de conclusão de curso.

Assim, pode-se dizer que as etapas que foram desenvolvidas neste estudo são:

1. Revisão bibliográfica dos temas
2. Desenvolvimento da aplicação
3. Escrita da documentação teórica

Em termos de classificação desta pesquisa, segundo os enfoques clássicos de classificação de uma pesquisa científica, entende-se que esta pode ser enquadrada conforme se apresenta na sequência:

- Quanto à natureza, esta é uma pesquisa aplicada, já que busca-se a solução de problemas práticos concretos.
- Quanto à forma de abordagem, a pesquisa pode ser classificada com quantitativa em sua maior parte, mas nota-se também aspectos qualitativos.
- Quanto aos fins, a pesquisa é metodológica e apresenta características de avaliação e proposição, uma vez que foi analisada a efetividade do programa final e também houve a proposição da tecnologia estudada, mostrando os prós e contras.
- Quanto aos meios, os seguintes recursos foram utilizados: bibliografia, dados documentais e pesquisa de laboratório.

3. Referencial Teórico

3.1. Certificados

Certificados são credenciais designadas obtidas por um indivíduo para verificar sua legitimidade e competência para realizar um trabalho. Os estudantes costumam os receber em dois formatos possíveis, o físico e o digital.

Quanto às características, os certificados físicos são difíceis de forjar porque possuem recursos de segurança embutidos, além disso o detentor consegue armazená-lo e mostrá-lo facilmente para uma pessoa desejada. Contudo, esse modelo requer verificação manual de veracidade por terceiros e as autoridades de certificação precisam manter registros por longos períodos de tempo. [Gräther et al. 2018]

Os certificados digitais, uma alternativa do modelo físico, implicam manuseios e usos mais simplificados, porém mais esforços são necessários para manter os certificados seguros e um padrão global de assinatura deve ser usado para que a verificação global seja possível. [Gräther et al. 2018] Em muitos países, não existe um padrão aberto universalmente usado para assinaturas digitais, levando a certificados que só podem ser verificados no contexto de ecossistemas de software específicos [Grech e Camilleri 2017].

Como os certificados são muito valiosos, fraudes costumam ocorrer principalmente na área da educação. De acordo com Bear e Ezell (2005), existem mais de trezentas fábricas de diplomas ativas que estão vendendo milhares de diplomas falsos a cada semana, incluindo para cursos de medicina e direito. Suas vendas totais ultrapassam quinhentos milhões de dólares por ano, mas o dano que seus clientes causam é incomensurável. Segundo Garwe (2015), as fraudes de certificados acadêmicos causam um prejuízo de $600 bilhões de dólares todo ano.

3.2. Blockchain

Para solucionar os problemas mencionados anteriormente, é possível utilizar a blockchain, "um livro-razão distribuído que fornece uma maneira das informações serem registradas e compartilhadas por uma comunidade" [Grech e Camilleri 2017].

A blockchain recebe esse nome pela maneira que armazena dados de transações em blocos que estão ligados entre si para formar uma cadeia. Cada bloco contém um registro de data e hora, o valor hash do bloco anterior, o valor hash do bloco atual e os dados principais armazenados [Lin e Liao 2017]. Esse é um dos conceitos que garantem a integridade da blockchain até o primeiro bloco (genesis block), pois os valores hash são únicos e uma mudança em um bloco da corrente mudaria imediatamente o seu respectivo valor hash [Nofer et al. 2017].

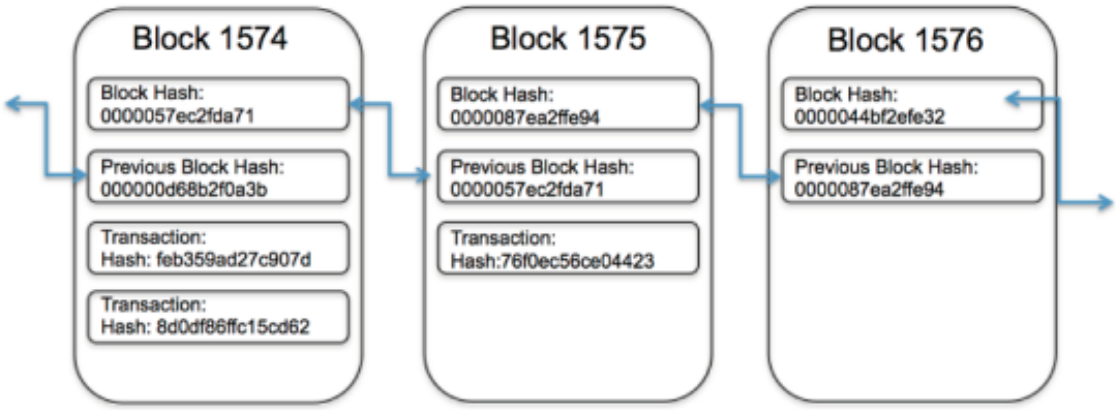

Figura 1. Ilustração de registros de transações em uma série de blocos, formando uma blockchain [GUPTA 2017]

Para que um novo bloco seja adicionado na corrente, a maioria dos nós daquela rede precisam validar o novo bloco e as transações feitas pelo próprio, esse mecanismo é chamado de consenso [Nofer et al. 2017]. De acordo com Lin e Liao (2017), o mecanismo de consenso "é um processo onde todos os nós da blockchain precisam ter um acordo sobre a mesma mensagem, isso garante com que a última alteração feita seja adicionada corretamente e evita que essa alteração seja um ataque malicioso".

Dentre os dois principais mecanismos de consenso, nota-se o proof of work e o proof of stake. O proof of work "exige que todas as máquinas de blockchain tenham uma cópia do livro-razão para a resolução de um quebra-cabeça complexo baseado na nova versão do livro. As máquinas que possuem cópias iguais formam grupos [...] o primeiro time a resolver o desafio vence, todas as máquinas consideradas perdedoras atualizam os seus livros para que eles fiquem iguais ao do time vencedor" [Gupta 2017].

Já o proof of stake é "uma alternativa mais econômica em energia e mais eficiente que o proof of work, nesse processo a seleção das máquinas é feita pela quantidade de moedas que um minerador possui. Acredita-se que quanto mais moedas um participante tem, menos suscetível ele será de cometer um ataque"[Zheng et. al. 2017]. Nesse processo, executar um ataque seria bem mais caro e os incentivos para cometer são reduzidos porque o atacante precisaria ter quase a maioria das moedas daquela blockchain e portanto sofreria severamente com o seu próprio ataque [Lin e Liao 2017].

Percebe-se então que a blockchain contém características de descentralização e imutabilidade, visto que os mineradores são formados por diversos grupos e pessoas, já os dados são armazenados permanentemente e não podem ser mudados a não ser que alguém detenha o controle de 51% das máquinas do sistema ao mesmo tempo [Lin e Liao 2017].

Por essas mesmas características, nota-se que os certificados poderiam ser verificados independente dos imprevistos possíveis de acontecer com a universidade emissora ou com os registros que ela contém. Esse cenário que não é encontrado em sistemas centralizados, pois se o registro de um sistema centralizado sofre algum

imprevisto externo, o acesso a ele é comprometido permanentemente e assim pessoas interessadas não conseguem resgatar nem verificar os seus certificados, mesmo que válidos.

3.2.1. Ethereum

Dentre as blockchains existentes, destaca-se a Ethereum, uma plataforma aberta, descentralizada e turing-completa que pode-se comparar com um sistema de computação global [Cheng et. al. 2018].

Essa blockchain possui ferramentas úteis para o sistema proposto, pois nela encontra-se a máquina virtual Ethereum, conhecida como EVM. Segundo Cheng et. al. (2018), a EVM é uma blockchain programável que possibilita que os desenvolvedores executem qualquer programa da maneira que desejam, o que o faz diferente do Bitcoin que provém um número fixo de comandos.

Por meio da máquina virtual e de uma linguagem de alto nível como a Solidity é possível executar os contratos inteligentes, um protocolo computadorizado que executa os termos de um contrato [Szabo 1994]. Seu principal objetivo é satisfazer condições contratuais comuns, minimizar exceções maliciosas ou acidentais e minimizar a necessidade de um intermediador confiável [Szabo 1994].

3.2.2 Transações e Gás

Uma transação Ethereum refere-se a uma ação iniciada por uma conta gerenciada por uma ação humana. Se há uma transferência entre duas contas, a conta de um deve ser debitada e a de outro creditada. Essas ações de mudança de estado ocorrem dentro de uma transação [Ethereum 2022].

Como cada transação Ethereum requer recursos computacionais para ser executada, cada transação requer uma taxa. O gás refere-se à taxa necessária para realizar uma transação na Ethereum com sucesso, trata-se de uma unidade que mede a quantidade de esforço computacional necessário para executar operações específicas na rede Ethereum [Ethereum 2022].

As taxas existem para ajudar a manter a rede Ethereum segura.

> Ao exigir uma taxa para cada computação executada na rede, evitamos que os maus atores enviem spam para a rede. Para evitar loops infinitos acidentais ou hostis ou outro desperdício computacional no código, cada transação deve definir um limite de quantas etapas computacionais de execução de código ela pode usar. [Ethereum 2022]

Reforça-se que as taxas são cobradas apenas de transações, ou seja, apenas de execuções que mudam algum estado interno. As execuções que envolvem somente leitura não são cobradas.

3.3. IPFS

O Sistema de Arquivos Interplanetário, conhecido como IPFS, é um sistema de arquivos distribuídos que busca conectar todos os dispositivos computacionais no mesmo sistema de arquivos. [BENET 2014]

Quando um arquivo é adicionado no IPFS, ele é criptografado e recebe uma única impressão digital chamada de identificador de conteúdo (CID). [IPFS 2022]

No momento em que um nó busca um determinado arquivo, é iniciado uma busca pelos nós das redes para ver qual nó está armazenando um arquivo de determinado CID. Assim que o conteúdo é visualizado ou baixado, o nó buscador armazena uma cópia em cache e se torna um outro provedor daquele conteúdo. Cada nó da rede armazena apenas o conteúdo que tiver interesse. [IPFS 2022]

Se uma nova versão de um arquivo é adicionada no IPFS, sua hash será diferente e então isso terá um novo CID, com isso os arquivos armazenados nesse sistema são resistentes a fraudes e censura, já que qualquer mudança não sobrescreverá o arquivo original. [IPFS 2022]

Se nenhum usuário do sistema tiver um conteúdo de determinado endereço disponível para que outros acessem, ninguém conseguirá resgatá-lo. Por outro lado, um conteúdo não pode ser removido do IPFS enquanto alguém suficientemente interessado o mantenha disponível. [IPFS 2022]

3.4. Trabalhos Correlatos

Quando trata-se do gerenciamento de certificados na blockchain, é possível citar algumas instituições que exploraram essa ideia. O laboratório de mídia do MIT foi uma das primeiras, pois criou um padrão aberto de criação, emissão, visualização e verificação de certificados baseados na blockchain Bitcoin, a BlockCerts. [MIT Media Lab 2016]

Os certificados contêm informações básicas dos alunos, são criptograficamente assinados e à prova de adulteração. Do ponto de vista da verificação, os empregadores podem verificar os certificados diretamente na plataforma e também podem criar o seu próprio serviço de consulta baseado nas mesmas informações. [MIT Media Lab 2016]

A TrueRec da empresa SAP também possibilitou o armazenamento de certificados na blockchain, diferente da BlockCerts, essa plataforma optou pela blockchain Ethereum. Nessa aplicação, os alunos possuem uma carteira digital onde podem armazenar os seus certificados e compartilhá-los diretamente com os empregadores, esses por sua vez podem colocar o código recebido na plataforma existente, comparando os resultados apresentados com o que foi recebido [Boeser 2017].

4. Resultados

O sistema de gerenciamento de certificados terá diferentes tipos de acesso para cada usuário, isso será feito pelos endereços públicos, um identificador único que o usuário recebe após criar uma conta no ecossistema Ethereum.

Todo funcionamento da aplicação começará com uma entidade intitulada de organização. Como um exemplo, pode-se assemelhar a organização com o Ministério da Educação, que pode ser uma entidade que define as universidades reconhecidas pela mesma.

Quando a organização faz o lançamento do contrato inteligente de gerenciamento de certificados na blockchain, o mesmo recupera o endereço de quem o lançou e reconhece como o primeiro membro da organização no sistema, a partir desse momento o membro terá as permissões desejadas.

O sistema conta com uma interface que permite a verificação de certificados e o gerenciamento de usuários. Para ocorrer a comunicação entre a interface e o contrato inteligente armazenado na blockchain, foi utilizado um pacote feito com Javascript. O diagrama de implementação a seguir ilustra a composição de cada parte e o que possibilita essa comunicação.

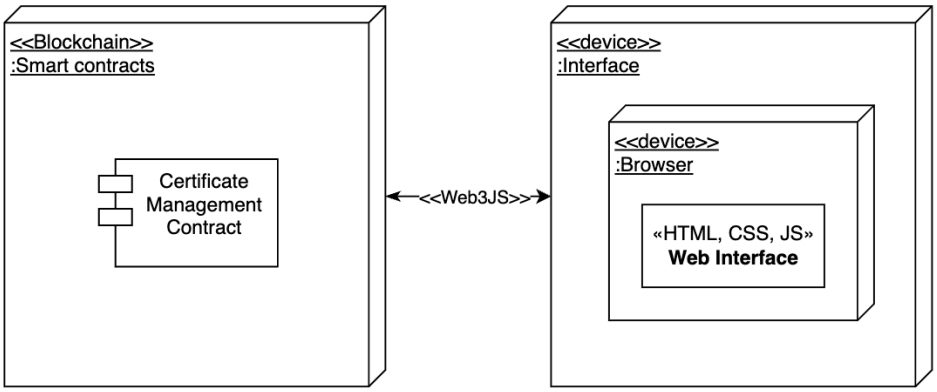

Figura 2. Diagrama de implementação do sistema

O código-fonte da interface[1] e do contrato inteligente[2] podem ser acessados no Github.

Quanto à hospedagem, o site da aplicação está armazenado no IPFS, o que significa que não só a organização pode ser provedora do conteúdo como também as universidades. Enquanto um desses membros estiver hospedando em condições normais, o site poderá ser acessado e assim a indisponibilidade da plataforma fica dificultada.

O diagrama de casos de uso a seguir denota todas as ações possíveis para cada tipo de ator no sistema.

[1] O código-fonte da interface pode ser visualizado em https://github.com/fscgustavo/front-certificate-management

[2] O código-fonte do contrato pode ser visualizado em https://github.com/fscgustavo/certificate-management

Figura 3. Diagrama de casos de uso

4.1. Informações das Universidades no IPFS

Ao contrário dos outros tipos de usuários, é necessário cadastrar outras informações além do endereço de uma universidade. Sem dados complementares, seria difícil a maioria das pessoas relacionarem um endereço criptografado a uma universidade específica.

Por esse motivo, todo registro de universidade é acompanhado por um CID do IPFS que contém as informações da universidade.

Essas informações não foram cadastradas diretamente na blockchain Ethereum porque o custo de registro de uma nova universidade seria consideravelmente aumentado, quanto maior o tipo de dado, mais caro é armazená-lo na blockchain. Ao invés de ter o custo de armazenar múltiplas informações e até imagens, o organizador terá o custo de armazenar um único dado que é o CID.

Essa informação continuará distribuída visto que a organização, a universidade e qualquer outro usuário podem ser provedores do arquivo. Enquanto um deles estiver provendo, será possível recuperar esses dados do IPFS.

4.2. Gerenciamento dos Certificados

Os tópicos a seguir denotam as etapas necessárias em cada uma das ações relacionadas aos certificados. As ações relacionadas a gerenciamento de usuário foram omitidas por serem operações CRUD simples.

4.2.1. Emissão do Certificado

O registro de certificados na blockchain só pode ser feito pelos certificadores pertencentes a universidades válidas. Assim que esse usuário possui o arquivo PDF do certificado, o mesmo pode levá-lo ao sistema para preencher as informações como título, data de emissão, data de expiração e descrição que pode receber informações diversas.

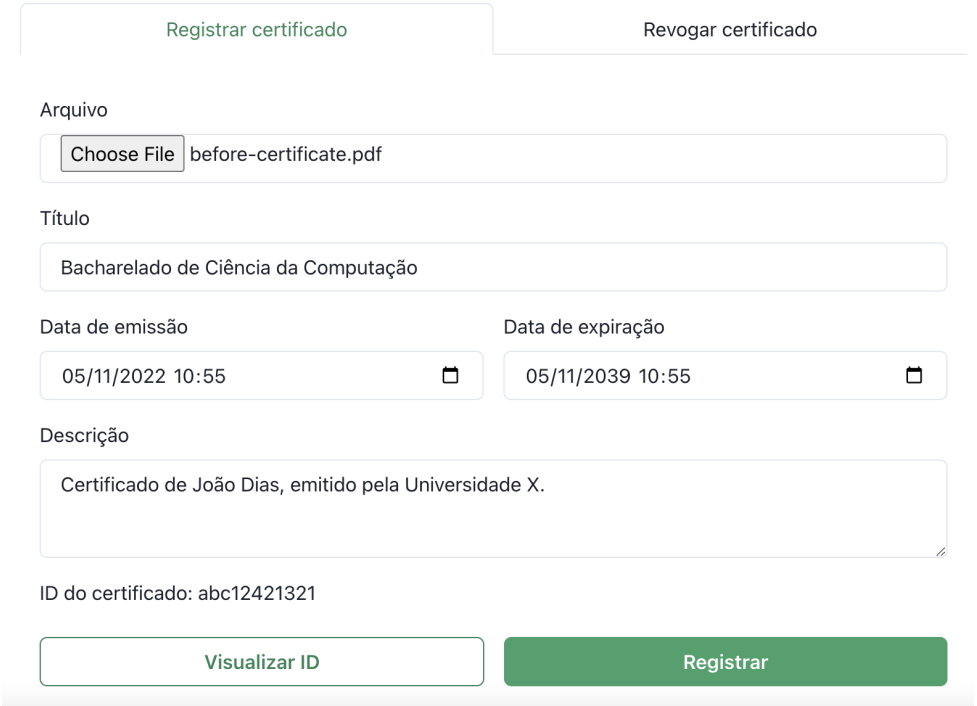

Figura 4. Formulário de registro preenchido

Assim que o certificador submete as informações, o sistema transforma as datas em milissegundos para facilitar futuras comparações, encaixa os dados em uma estrutura para transformá-los em um texto único porque esse é o único formato possível para eles serem criptografados com o algoritmo keccak256.

O keccak256 foi escolhido por ser um algoritmo que gera um ID único para cada combinação de caracteres recebido. Se uma pessoa alterar qualquer caractere do texto gerador, o id do arquivo alterado será completamente diferente no verificador, resultando em um certificado inexistente ou inválido.

Figura 5. Etapas para a geração do ID do certificado

Após gerar o ID com as informações do certificado, o sistema registra-o no contrato inteligente junto com as datas e os endereços do certificador e de sua respectiva universidade.

O armazenamento do ID em uma estrutura do contrato resulta em uma conexão do id com documento original. Como o documento em si não é publicado na blockchain diretamente, a privacidade de suas informações é preservada.

Ao detectar que os dados foram armazenados com sucesso em um armazenamento do contrato, o sistema usa a estrutura previamente ilustrada na figura 5 para preencher os metadados do PDF selecionado. Dessa forma, o texto gerador é salvo no PDF e o sistema conseguirá usá-lo para chegar no id do certificado durante uma verificação.

O ID do certificado e o ID da transação também são salvos nos metadados, mas esses são armazenados em um campo de palavras-chave que não é usado para a geração do identificador do certificado.

Após a alteração do arquivo, o certificador poderá enviá-lo para que o estudante o armazene de acordo com sua preferência.

4.2.2. Revogação do Certificado

A revogação do certificado pode ser feita por um membro da organização, por uma universidade válida ou por um certificador pertencente a uma universidade válida. A universidade envolvida na revogação deve ser igual a universidade que emitiu o certificado.

Para concluir a ação, esses usuários devem submeter o ID do certificado existente e também o motivo da revogação.

Figura 6. Formulário de revogação preenchido

Assim que o certificado com determinado ID é invalidado, toda verificação mostrará esse estado e o motivo registrado.

4.2.3. Verificação do certificado

A verificação de certificados na blockchain pode ser feita por qualquer usuário.

Assim que uma pessoa recebe o arquivo do certificado de um estudante, a mesma pode enviá-lo ao formulário.

Figura 7. Formulário de verificação preenchido

Após o envio, o sistema lê os metadados do PDF, apresenta-os na tela e faz os mesmos passos ilustrados na figura 5 para que o ID seja obtido e para que a consulta seja feita, retornando o estado do certificado, as datas e as informações obtidas no IPFS sobre a universidade emissora.

7.3. Relação entre os Certificados do Sistema e os NFTs

As documentações da Ethereum (2022) constam que NFTs são

> tokens que podemos usar para representar a propriedade de itens exclusivos. Elas nos permitem transformar arte, colecionáveis e até imóveis em ativos digitais. A propriedade de um ativo é assegurada pela blockchain Ethereum. Ninguém pode modificar o registro de propriedade ou copiar/colar um novo NFT existente.

O não fungível de sua sigla significa que os tokens não podem ser trocados por outros itens porque eles possuem propriedades únicas. Por outro lado, os itens fungíveis são definidos pelo seu valor, não por suas propriedades exclusivas e por isso podem ser trocados [Ethereum 2022].

Conceitualmente, os certificados são considerados tokens não fungíveis contudo, os padrões dos NFTs não foram utilizados no sistema por existir empecilhos técnicos conforme relatado por Vitalik Buterin (2022), criador da Ethereum:

> Existem desafios técnicos em fazer os tokens intransferíveis e únicos. Há uma "interface" desconfortável entre o desejo de limitar ou impedir transferências em um ecossistema blockchain onde até agora todos os padrões são projetados em torno da máxima transferibilidade.

O padrão mais popular de NFTs chamado ERC-721, por exemplo, especifica que um token deve ter funcionalidade de transferência entre contas, de obter o endereço do dono daquele token e também o custo total do token provido na rede [Ethereum 2022].

Nota-se que o certificado desejado não pode ser transferível nem precificável, o que deixa-o distante de muitos padrões. Ainda assim, o modelo de emissão e verificação de certificados do sistema proposto atende os requisitos definidos.

4.4. Custo-médio das transações

Conforme descrito em outro capítulo, as ações que mudam o estado interno de algo armazenado na blockchain implicam em cobranças de taxas.

Com auxílio de um pacote de desenvolvimento, foi possível obter o custo médio de cada uma dessas ações ao rodar os testes unitários do contrato em 7 de novembro de 2022 às oito horas da noite:

Tabela 1. Custo médio das transações do sistema

Ação	Custo médio
cadastrar membro da organização	R$ 5,82
remover membro da organização	R$ 3,20
cadastrar universidade	R$ 8,71
invalidar universidade	R$ 7,81
cadastrar certificador	R$ 5,85
remover certificador	R$ 3,20
registrar certificado	R$ 12,56
revogar certificado	R$ 9,91
armazenar o contrato inteligente na blockchain	R$ 310,00

Fonte: Elaborado pelos autores

As taxas diminuem à medida que a Ethereum recebe atualizações que a deixe mais performática. Um menor esforço computacional para a validação e a inserção de um novo bloco é um fator chave para barateá-las.

5. Conclusão

Nesse trabalho foi conhecido os problemas existentes para os modelos de certificados físicos e digitais. Em busca de uma alternativa, foi apresentado um modelo onde os registros relacionados de um certificado são armazenados em um contrato inteligente localizado na blockchain.

Considera-se o objetivo do trabalho cumprido, pois foi possível implementar e analisar um sistema onde os registros dos certificados são invioláveis, permanentes e facilmente verificáveis.

Quanto à disponibilidade, define-se como alta porque o contrato, o site e seus conteúdos estáticos são sustentados por múltiplos dispositivos computacionais e por isso é descentralizado. Mesmo que um imprevisto ocorra com um dos nós, muitos outros estarão suportando toda a funcionalidade.

O sistema apresentado é uma versão inicial de uma prova de conceito, mas é reconhecido que o mesmo pode receber otimizações em trabalhos futuros que melhorem a segurança e a funcionalidade.

Na versão atual, as taxas das transações de emissão e de remoção feitas pelo certificador são debitadas de seu próprio fundo. Para evitar isso, pode-se criar uma estrutura onde os certificadores possuem as suas cobranças restituídas de um fundo criado no sistema pela universidade, assim as taxas seriam mais facilmente cobradas das universidades e não de seus funcionários.

Quanto às transações de adição e remoção dos organizadores, é notável que ambas podem receber mecanismos que evitem alterações bruscas e erradas, como a necessidade da aprovação de pelo menos dois membros de uma organização antes que uma ação seja concluída. Sem isso, uma conta Ethereum burlada poderia sequestrar o sistema para si ao deletar os outros membros da organização ou poderiam alterar estados importantes do sistema que são trabalhosos de reverter.

Os conceitos apresentados para o ciclo de vida dos certificados também podem ser explorados em outros sistemas que gerenciam diferentes tipos de documentos. As hierarquias, regras das alterações de estado podem mudar para cada documento, mas no final os benefícios alcançados serão os mesmos.

Referências

BENET, Juan. IPFS - Content Addressed, Versioned, P2P File System. Cornell University, 2014. Disponível em: https://doi.org/10.48550/arXiv.1407.3561. Acesso em: 17 out. 2022

BUTERIN, Vitalik. Soulbound. Vitalik Buterin's website. Disponível em: https://vitalik.ca/general/2022/01/26/soulbound.html. Acesso em: 4 out. 2022

CHENG, Jiin-Chiou. et al. Blockchain and smart contract for digital certificate. IEEE, 2018. Disponível em: https://doi.org/10.1109/ICASI.2018.8394455. Acesso em: 30 out. 2021.

ETHEREUM. ERC-721 Non-fungible Token Standard. Disponível em: https://ethereum.org/en/developers/docs/standards/tokens/erc-721. Acesso em: 4 out. 2022

ETHEREUM. Gas and Fees. Ethereum. Disponível em: https://ethereum.org/en/developers/docs/gas . Acesso em: 23 out. 2022

ETHEREUM. Transactions. Ethereum. Disponível em: https://ethereum.org/en/developers/docs/transactions . Acesso em: 23 out. 2022

EZELL, Allen; BEAR, John. Degree mills: The billion-dollar industry that has sold over a million fake diplomas. Pyr Books, 2005 BOESER, Benjamin. Trusted Digital Credentials Powered by Blockchain. San José, 2017. Disponível em: https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain. Acesso em: 27 mai. 2022.

GARWE, E. Chiyevo. Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. Zimbabwe, p.119-135, 1 mai. 2015. Disponível em: https://doi.org/10.5296/jse.v5i2.7456. Acesso em: 21 mai. 2022.

GRÄTHER, Wolfgang. et al. Blockchain for Education: Lifelong Learning Passport. EUSSET Digital Library, 2018. Disponível em: http://dx.doi.org/10.18420/blockchain2018_07. Acesso em: 30 out. 2021.

GRECH, Alex; CAMILLERI, Anthony F. Blockchain in Education. European Commission, 2017. Disponível em: http://dx.doi.org/10.2760/60649. Acesso em: 30 nov. 2021.

GUPTA, Manav. Blockchain for Dummies. Nova Jersey: John Wiley & Sons, 2018.

IPFS. IPFS Documentation. Disponível em: https://ipfs.tech. 17 out. 2022

JIRGENSONS, Merija; KAPENIEKS, Janis. Blockchain and the Future of Digital Learning Credential Assessment and Management. ERIC, 2018. Disponível em: https://eric.ed.gov/?id=EJ1218203. Acesso em: 30 out. 2021.

LIN, Iouon-Chang; LIAO, Tzu-Chun. A Survey of Blockchain Security Issues and Challenges. Department of Photonics and Communication Engineering - Asia University, Taiwan, 2017. Disponível em: http://dx.doi.org/10.6633/IJNS.201709.19(5).01. Acesso em: 03 jun. 2022.

MIT MEDIA LAB. Blockcerts: An Open Infrastructure for Academic Credentials on the Blockchain. Cambridge, 2016. Disponível em: https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f. Acesso em: 27 mai. 2022.

NOFER, Michael; GOMBER, Peter; HINZ, Oliver. Blockchain: Business & Information Systems Engineering v.59, p. 183–187, 20 mar. 2017. Disponível em: https://doi.org/10.1007/s12599-017-0467-3. Acesso em: 05 jun. 2022

SALEH, Omar; GHAZALI, Osman; RANA, Muhammad. Blockchain based framework for educational certificates verification. 2020. Disponível em: http://dx.doi.org/10.31838/jcr.07.03.13. Acesso em: 26 mai. 2022.

SZABO, Nick. Formalizing and Securing Relationships on Public Networks. First Monday, Chicago, 01 set. 1997. Disponível em: https://doi.org/10.5210/fm.v2i9.548. Acesso em: 04 jun 2022.

YAGA, Dylan; MELL, Peter; ROBY, Nik; SCARFONE, Karen. Blockchain Technology Overview. National Institute of Standards and Technology Internal Report, 26 Jun 2019. Disponível em: https://arxiv.org/abs/1906.11078. Acesso em: 05 jun. 2022.

Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, Disponível em: https://doi.org/10.1109/BigDataCongress.2017.85. Acesso em: 04 jun. 2022.