UNIVERSIDADE FEDERAL DO CEARÁ

***CAMPUS* DE CRATEÚS**

CURSO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

RODRIGO LINHARES BARROSO

EMISSÃO E VALIDAÇÃO DE DIPLOMAS DIGITAIS USANDO A TECNOLOGIA BLOCKCHAIN

CRATEÚS - CEARÁ

2023

RODRIGO LINHARES BARROSO

EMISSÃO E VALIDAÇÃO DE DIPLOMAS DIGITAIS USANDO A TECNOLOGIA BLOCKCHAIN

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação do *Campus* de Crateús da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Antonio Emerson B. Tomaz

CRATEÚS - CEARÁ

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B285e Barroso, Rodrigo.
Emissão e validação de diplomas digitais usando a tecnologia blockchain / Rodrigo Barroso. – 2023.
52 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Crateús, Curso de Sistemas de Informação, Crateús, 2023.
Orientação: Prof. Dr. Antonio Emerson B. Tomaz.

1. Diploma digital. 2. Blockchain. 3. Segurança da Informação. 4. Falsificação de documentos. I. Título.

CDD 005

RODRIGO LINHARES BARROSO

EMISSÃO E VALIDAÇÃO DE DIPLOMAS DIGITAIS USANDO A TECNOLOGIA BLOCKCHAIN

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação do *Campus* de Crateús da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Antonio Emerson B. Tomaz (Orientador)
Universidade Federal do Ceará (UFC) - *Campus* de Crateús

Prof. Me. Francisco Anderson de Almada Gomes
Universidade Federal do Ceará (UFC) - *Campus* de Crateús

Prof. Me. Ítalo Mendes da Silva Ribeiro
Universidade Federal do Ceará (UFC) - *Campus* de Crateús

Prof. Ma. Amanda Drielly Pires Venceslau
Universidade Federal do Ceará (UFC) - *Campus* de Crateús

À minha família, por sua capacidade de acreditar em mim e investir em mim. Mãe, seu cuidado e dedicação foram que deram, em alguns momentos, a esperança para seguir. Pai, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada.

AGRADECIMENTOS

Dedico este trabalho ao Prof. Dr. Antonio Emerson B. Tomaz por me orientar no meu TCC.

Aos professores Me. Francisco Anderson de Almada Gomes, Me. Ítalo Mendes da Silva Ribeiro e Ma. Amanda Drielly Pires Venceslau por aceitarem fazer parte da banca.

Ao Prof. Ítalo Ribeiro também como supervisor do Proj. Integrador III e meus colegas Giniele Pinho e Leimar Ferreira por me ajudarem no meu primeiro trabalho prático sobre implementação e uso prático de uma blockchain.

A professora Lisieux Andrade pela adequação do *template* utilizado neste trabalho para que o mesmo ficasse de acordo com as normas da biblioteca da Universidade Federal do Ceará (UFC) e das normas da Associação Brasileira de Normas Técnicas (ABNT).

A meu ex-chefe Diego Lucena Tavares Leite Viana por me permitir alocar tempo para a elaboração deste trabalho.

Ao professor Marciel Barros por me apresentar a ferramenta Overleaf e como usá-la.

"Há três métodos para ganhar sabedoria: primeiro, por reflexão, que é o mais nobre; segundo, por imitação, que é o mais fácil; e terceiro, por experiência, que é o mais amargo."

(Confúcio)

RESUMO

A falsificação de diplomas é um grave problema no Brasil. Mesmo com uma rígida legislação em vigor, leis sozinhas não são suficientes para conter este mercado ilegítimo. Profissionais despreparados que usam diplomas falsos são prejudiciais tanto para o mercado de trabalho quanto para a reputação das instituições de ensino, aproveitando-se de uma brecha no ineficiente procedimento de certificação dos concluintes dos cursos de educação superior que existe tradicionalmente. Em uma era de revoluções digitais, existem muitas tecnologias alternativas ao diploma de papel que podem ser exploradas nessa problemática, sendo uma delas a tecnologia da blockchain, que tem sido empregada em vários serviços de registro de propriedade, credenciais e documentos nos últimos anos devido à sua segurança e transparência. Sendo assim, o presente trabalho visa desenvolver um sistema capaz de registrar e autenticar diplomas de educação superior usando a tecnologia blockchain. Há uma comparação de custo e tempo de execução de uma mesma operação de armazenamento e de acesso ao arquivo entre a blockchain Ethereum e blockchain Solana, que possui menor custo de uso e melhor desempenho de tempo de execução.

Palavras-chave: Diploma digital. *Blockchain*. Ensino superior. Ethereum. Solana

ABSTRACT

In Brazil, the production of fake diplomas is a significant issue. Despite having stringent laws in place, they prove insufficient in regulating this illicit market. Individuals who use counterfeit diplomas without having the necessary qualifications are detrimental to the job market and the credibility of educational institutions. They exploit a loophole in the inefficient certification process for graduates of higher education courses. With the rise of digital advancements, there are various options to consider as alternatives to paper diplomas. One such solution is blockchain technology, which has gained popularity recently due to its security and transparency. It has been effectively utilized in services such as property registration, credentials, and documents. Therefore, this work aims to develop a system capable of registering and authenticating higher education diplomas using blockchain technology. There is a comparison of cost and execution time for the same storage and file access operation between the Ethereum blockchain and the Solana blockchain, which has lower usage costs and better execution time performance.

Keywords: Digital diploma. *Blockchain*. University education. Ethereum. Solana

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade Certificadora
AES	*Advanced Encryption Standard*
IBM	*International Business Machines*
ICP Brasil	Infraestrutura de Chaves Públicas Brasileira
IES	Instituição de ensino superior
IPFS	*Interplanetary File System*
ITI	Instituto Nacional de Tecnologia da Informação
JWT	Json Web Token
MD5	*Message Digest Algorithm*
MEC	Ministério da Educação
MIT	*Instituto de Tecnologia de Massachusetts*
NFT	*Token Não-Fundível*
NIST	*National Institute of Standards and Technology*
P2P	*Peer-To-Peer*
PDF	*Portable Document Format*
pfx	Personal Information Exchange
POS	*Proof Of Stake*
RSA	*Rivest-Shamir-Adlerman Algorithm*
UFC	Universidade Federal do Ceará
USNSA	United States National Security Agency
UTXO	*Unspent Transaction Output*
VDF	função de atraso verificável

LISTA DE SÍMBOLOS

PU_b	Chave pública em sistema criptográfico assimétrico
PR_b	Chave privada em sistema criptográfico assimétrico
ϕ	Função totiente de Euler
mod	Operação de módulo
$\equiv$	Operador de equivalência

SUMÁRIO

1 INTRODUÇÃO

O mercado de diplomas clandestinos em países da América do Norte, em especial nos Estados Unidos, é muito grande (FORBES, 2023). No trabalho de Tang (2021) é mencionado que uma reitora do *Instituto de Tecnologia de Massachusetts* (MIT) foi forçada a se demitir após ser descoberto que trabalhou por quase três décadas com um diploma de bacharelado falsificado.

Estes tipos de cenários também são comuns no Brasil, embora a legislação seja mais rígida contra a falsificação de diplomas (JUSBRASIL, 1940). No entanto, fatores como a baixa renda familiar e os efeitos da pandemia de COVID-19 tem levado à crescente evasão de estudantes universitários nos últimos anos, chegando a 3.5 milhões em 2021 (GLOBO, 2022), e tem contribuído para a busca por diplomas falsificados.

Sem uma forma de conseguir um trabalho, muitos destes estudantes recorrem a comprar diplomas forjados, que segundo Firmo (2021) tem retorno de até cem por cento do investimento. Estes profissionais que entram despreparados em vagas de emprego por meio de tais documentos, prejudicam não apenas o mercado de trabalho, mas a reputação de instituições de ensino que têm diplomas fabricados em seu nome.

Neste cenário, é de crucial relevância observar que leis sozinhas não são suficientes para combater a circulação de diplomas de graduação falsos, é necessário uma forma eficiente de detectar tais documentos e desincentivar sua produção, assim como a promover a substituição do método tradicional de certificação por um procedimento mais confiável e eficiente.

Além de arriscado permitir que empresas privadas e órgãos públicos, na hora de contratar seus funcionários, confiem em documentos que podem ser facilmente fabricados, há também o fato de que tais documentos são vulneráveis a danos físicos e extravios. Em situações nas quais o formado perde seu diploma, é necessário se submeter a um processo caro e demorado para a emissão de uma segunda via (GOV.BR, 2022).

Sendo assim, o presente trabalho propõe um sistema de gerenciamento de diplomas, no formato digital, com as funcionalidades de registro em *blockchain* e verificação de conformidade, alcançadas por meio de técnicas de criptografia como assinaturas digitais.

Blockchain é um sistema de registros para transacionar valor (não apenas dinheiro) em uma rede *Peer-To-Peer* (P2P) (SINGHAL *et al.*, 2018). Os registros uma vez gravados não podem ser mais apagados e podem ser de acesso livre ou regulados por um consórcio, possibilitando o funcionamento do modelo proposto neste trabalho.

Devido a sua popularidade no mercado, foi escolhida a *blockchain Ethereum* para a

implementação do sistema, no entanto, devido ao alto custo de seus serviços uma versão usando a *blockchain Solana* também foi desenvolvida como uma opção alternativa de menor custo para o usuário da IES. A *Solana* tem surgido como uma concorrente a *Ethereum* e tem se destacado devido ao seu baixo custo de utilização Dreams (2022).

1.1 Objetivos

Este trabalho estabelece os seguintes objetivos.

1.1.1 Objetivo geral

Desenvolver um sistema de gerenciamento de diplomas digitais, voltado para IES usando uma *blockchain* de baixo custo.

1.1.2 Objetivos específicos

- Desenvolver uma aplicação usando a *Blockchain Ethereum*,
- Desenvolver uma aplicação usando a *Blockchain Solana*.
- Comparar o custo financeiro da aplicação baseada em Ethereum versus a aplicação baseada em solana.

1.2 Organização do trabalho

O restante deste trabalho é composto pelo Capítulo 2, que aborda ferramentas e técnicas a respeito de segurança da informação na *blockchain*. O Capítulo 3, que apresenta os trabalhos relacionados. Em seguida, o modelo proposto no Capítulo 4 e por fim a conclusão será apresentada no Capítulo 5.

2 FUNDAMENTAÇÃO TEÓRICA

A criptografia é uma das tecnologias mais importantes para o funcionamento da Internet atual. Criptografia se trata do estudo de técnicas matemáticas com objetivo de assegurar aspectos da segurança da informação: confidencialidade, integridade e autenticidade (MENEZES *et al.*, 2018).

Os algoritmos e técnicas usados na criptografia atual são baseados em primitivas criptográficas. Estes são algoritmos de baixo nível bem estabelecidos, que são frequentemente usados para construir protocolos criptográficos para sistemas de computadores por não terem nenhuma quebra conhecida, assim provendo segurança confiável (BARKER *et al.*, 2016). Nestes sistemas criptográficos, podemos assegurar a confidencialidade da troca de mensagens entre os participantes, assim como a integridade do conteúdo das mensagens, o conhecimento da origem de tais mensagens e a garantia de que as mensagens cheguem ao destinatário quando é preciso, sem serem interceptadas, desviadas ou adulteradas.

2.1 Criptografia Simétrica

O modelo de algoritmo criptográfico mais empregado até 1976 foi a criptografia simétrica, usada em cenários onde duas pessoas necessitavam trocar informações confidenciais em um canal privado. O exemplo mais simples de um sistema de criptografia simétrica, embora não o mais antigo, é datado do império de Júlio César e é chamado de Cifra de César . Neste, uma mensagem chamada pelo termo “texto claro” é submetida a um processo de troca dos caracteres da mensagem original, resultando em uma mensagem ininteligível e um valor chamado de chave secreta que é usado pelo receptor para decifrar a mensagem, e enviado para este por um canal considerado seguro. Na era atual este modelo foi refinado para algoritmos mais avançados como o *Advanced Encryption Standard* (AES).

A criptografia simétrica introduziu um grande problema, este que ficou conhecido como o problema da distribuição de chaves. Basicamente, o grande desafio era como assegurar um canal de forma que a chave do processo de criptografia fosse passada para o destinatário sem que um invasor se apodere dela e leia mensagens sem autorização. O problema persistiu até que *Diffie* e *Hellman* apresentaram um modelo no qual duas pessoas podem produzir uma chave secreta compartilhada através da troca de informações públicas. Esta técnica ficou conhecida como protocolo de troca de chaves *Diffie-Hellman* (DIFFIE; HELLMAN, 1976).

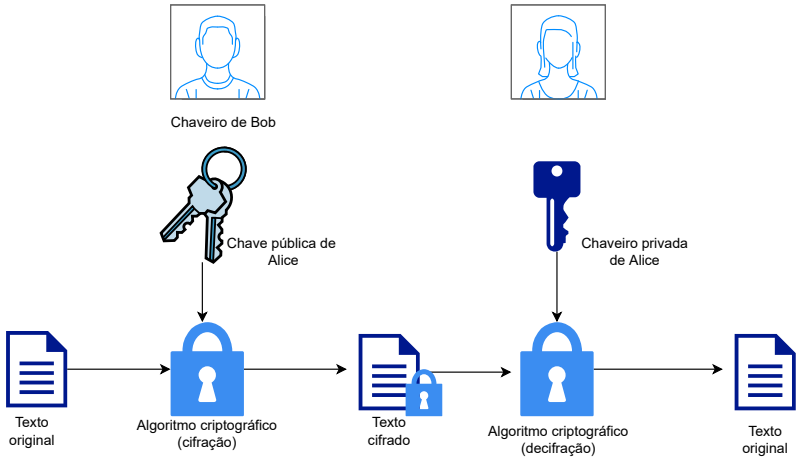
2.2 Criptografia Assimétrica

A pesquisa de troca de chaves *Diffie* e *Hellman* em 1976 (DIFFIE; HELLMAN, 1976) instigou uma nova área de estudos na criptografia a qual é atualmente chamada de criptografia assimétrica. Nesta, o conceito de chave única e secreta é substituido por pares de chaves, uma chave pública e uma chave privada. Enquanto uma chave é usada para cifrar mensagens a outra é usada para decifrar.

No contexto de criptografia assimétrica, os conceitos principais são enumerados abaixo, seguidos dos passos para se atingir um sistema de criptografia assimétrica, segundo Stallings (2006).

- Texto plano : mensagem original que é usada como entrada do algoritmo de criptografia
- Algoritmo criptográfico : algoritmo que realiza diferentes transformações no texto plano para gerar um texto cifrado.
- Chave pública e chave privada : par de chaves que são selecionadas de tal forma que se uma é usada para cifrar a outra é usada para decifrar. As transformações realizadas pelo algoritmo dependem dos valores das chaves.
- Texto cifrado : mensagem embaralhada ou transformada produzida pelo algoritmo. O valor de saída do algoritmo depende do texto de entrada e da chave usada. Duas chaves diferentes devem produzir textos cifrados diferentes para um mesmo texto plano.

Figura 1 – Modelo de Criptografia Assimetrica



Fonte: Adaptado de Stallings (2006).

Para se atingir um sistema de criptografia como da Figura 1, *Diffie* e *Hellman* estabeleceram de forma teórica as seguintes fundações.

1. Deve ser computacionalmente fácil para um usuário gerar uma chave pública e uma chave privada.
2. Deve ser computacionalmente difícil obter a chave privada a partir da chave pública.
3. Um emissor que conheça a chave pública do receptor deve ser capaz de cifrar uma mensagem com esta facilmente.
4. Deve ser computacionalmente difícil para uma pessoa não autorizada decifrar uma mensagem sem a chave privada do seu destinatário.
5. A chave privada também pode ser usada para cifrar uma mensagem contanto que a chave pública seja usada para decifrá-la.

Os termos computacionalmente fácil e computacionalmente difícil referem-se ao fato de um processo poder ser resolvido em tempo viável por um algoritmo polinomial. Caso não haja um algoritmo do tipo, dizemos que ele é de tempo exponencial e portanto inviável de ser feito por uma máquina ordinária, pois irá requerer um esforço computacional de tempo indefinido para produzir um resultado (STALLINGS, 2006). Neste ponto, é apropriado estabelecer o conceito de *One Way Function* ou *Função Trapdoor*, que se trata de uma função que exige esforço computacionalmente fácil para produzir um texto cifrado, mas requer um esforço computacionalmente indefinido para fazer o processo inverso, sendo este inviável. Geralmente a complexidade destas funções é estabelecida em problemas matemáticos que ainda não possuem uma solução existente ou não possuem uma solução que possa ser reproduzida com um computador ordinário, como por exemplo, a fatoração de números inteiros extremamente grandes, em seus fatores primos, esta que é empregada no *Rivest-Shamir-Adlerman Algorithm* (RSA).

2.3 Algoritmo de Rivest-Shamir-Adlerman (RSA)

Após a publicação da pesquisa de *Diffie* e *Hellman* discutida anteriormente, os criptoanalistas do MIT *Ron Rivest*, *Adi Shamir* e *Len Adleman* propuseram a primeira implementação de um sistema de chave pública chamado RSA, nomeado em homenagem aos seus criadores (RIVEST *et al.*, 1978). Este é um dos sistemas criptográficos mais usados atualmente. O funcionamento do algorítmo é explicado no apêndice **??**.

2.4 Funções hash

A função hash é um mapeamento unidirecional

$$H : \{0,1\}^* \rightarrow \{0,1\}^i,$$

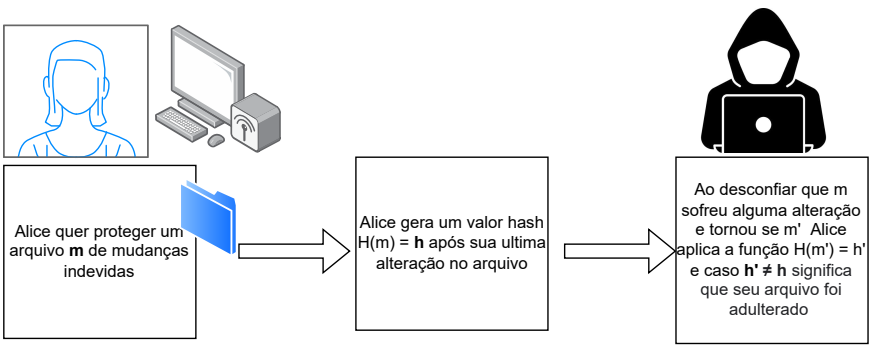
para algum $i \in \mathbb{N}$.

Neste mapeamento $D = \{0,1\}^*$ é o domínio da função, possivelmente infinito, que representa as possíveis mensagens de tamanho arbitrário. $I = \{0,1\}^i$ é a imagem da função que representa os possíveis valores hash de tamanho i.

As funções *hash* tem como objetivo gerar o valor hash que funciona como um identificador únivoco para a mensagem original do domínio, transformando qualquer tipo de dado de entrada , independentemente de seu tamanho, em uma cadeia de *bits* de comprimento fixo e geralmente com tamanho menor que o tamanho da entrada. Por esse motivo, as funções *hash* são referidas também como funções resumo, e são uma das principais primitivas criptográficas usadas na criptografia moderna (STALLINGS, 2006).

Funções *hash*, ao contrário de algortimos criptográficos não podem ser revertidas para o seu estado original e geralmente são usadas para garantir a integridade das mensagens ao invez da sua confidencialidade, sendo que um único caractere modificado no texto original irá resultar em um texto cifrado completamente diferente, permitindo que alterações sejam facilmente percebidas. No cenário de uso ilustrado na Figura 2 é possível visualizar o uso prático das funções *hash*.

Figura 2 – Garantindo a integridade com funções hash



Fonte: Elaborado pelo autor.

2.5 Funções Hash Criptográficas

Considerando o mapeamento

$$H : \{0,1\}^* \rightarrow \{0,1\}^i,$$

como o conjunto domínio $D = \{0,1\}^*$ é muito maior que o conjunto $I = \{0,1\}^i$, pode ocorrer de duas mensagens m_1 e m_2 resultarem na mesma saída h, isto é conhecido como colisão. A segurança da função *hash* está diretamente relacionada a dificuldade de gerar colisões (STALLINGS, 2006). Quanto menor a chance de gerar colisão, mais segura é a função pois é menos sucetível a ataques de força bruta em um sistema criptográfico. Segundo Garfinkel (2015), em criptografia, um ataque de Força Bruta envolve tentar todas as combinações possíveis para encontrar uma correspondência as credenciais que o atacante deseja se apoderar por meio de tentativa e erro repetidamente.

Para serem usadas em sistemas criptográficos, as funções *hash* devem satisfazer três propriedades essenciais. Se tais propriedades forem satisfeitas, elas são chamadas de *funções hash criptográficas* (STALLINGS, 2006).

1. *Resistência à pré-imagem*: Dada uma mensagem m, é computacionalmente fácil calcular um hash h. Mas dado um hash h, é computacionalmente difícil obter m.
2. *Resistência à segunda pré-imagem*: Dada uma mensagem m, é difícil encontrar uma mensagem m' tal que esta tenha o mesmo hash que a mensagem original, isto é $H(m) = H(m')$.
3. *Resistência à colisão*: Dada duas mensagens m_1 e m_2 de um mesmo domínio D e uma função *hash* H tais que, $m_1 \neq m_2$, é computacionalmente difícil encontrar $H(m_1) = H(m_2)$.

Podemos citar o algoritmo *Message Digest Algorithm* (MD5) como o principal exemplo de função *hash* não criptográfica, pois é comprovado que ele quebra a propriedade da resistência a colisão. (LENSTRA *et al.*, 2005). O capítulo de trabalhos relacionados mostra um exemplo de ataque explorando vulnerabilidades do MD5 (THOMPSON, 2005).

2.6 *Security Hash Algorythm* (SHA)

O *Secure Hash Algorithm* (SHA) foi desenvolvido pelo United States National Security Agency (USNSA) e declarado como um padrão federal de processamento de informações no artigo nomeado FIPS 180 (NIST, 1993). Posteriormente uma versão revisada foi emitido como

FIPS 180-1 em 1995 e é geralmente referido como SHA-1 (STALLINGS, 2006). SHA-1 foi desenvolvido baseado no MD4 um algoritmo precursor ao MD5, este foi considerado inseguro pelo *National Institute of Standards and Technology* (NIST) em 2005 levando a adoção de seus sucessores.

Após um caso de quebra do algoritmo MD5 em 2002 a transição de sistemas de criptografia da época para novas versões do algoritmo se instensificou. Os algoritmos SHA-256, SHA-384 e SHA-512 foram introduzidos pelo NIST como alternativas ao SHA-1. Seu principal diferencial em relação a seu antecessor é o tamanho da saída em *bits* denotado pelo número ao final do algoritmo. O SHA-1, considerado defasado, possuía apenas 160 *bits* de saída o que o tornou cada vez mais vulnerável á ataques de força bruta a medida que o poder computacional evoluía, como por exemplo ataques do aniversário (MENEZES *et al.*, 2018). Tais ataques consistem de métodos de força bruta para reduzir o tempo necessário de se realizar uma colisão dentro das possíveis saídas do algoritmo (BELLARE; KOHNO, 2004) .

O funcionamento dos algoritmos da chamada família SHA tem como princípio transformar uma mensagem de entrada de tamanho variável em uma saída de tamanho fixo de *bits*.

2.7 Assinatura Digital

Até este ponto tem sido discutido como garantir a segurança da comunicação entre autor e receptor contra ataques externos voltados a atacar a mensagem em si mas não como proteger o autor e receptor de ataques de personificação. Esta segurança só pode ser alcançada por meio da assinatura digital, que é uma prova de que uma mensagem foi de fato enviada por quem diz ser.

Kissel (2011) define personificação como a habilidade de receber uma mensagem do remetente se disfarçando como o destinatário ou se disfarçar como remetente e então enviar uma mensagem para o destinatário.

Imaginando o seguinte caso de uso:

1. Alice deseja enviar uma mensagem em nome de John á Bob. Alice poderia simplesmente escrever a mensagem em nome de John e a enviar.
2. John não escreveu a mensagem e portanto deseja negar sua autoria.

Para impedir que alquém personifique John, há duas abordagems que podem ser

tomadas. A primeira seria cifrar a mensagem por meio de sua chave privada em um sistema criptográfico. Assim apenas quem tivesse a chave pública de John poderia decifrar a mensagem, garantindo a autoria de John. No entanto, o tempo para se cifrar uma mensagem muito grande pode ser demorado pois exige esforço computacional proporcional ao tamanho da mensagem a ser cifrada. A segunda forma de garantir a autoria seria aplicar uma função *hash* ou função de resumo à mensagem para obter um valor *hash* e então cifrar o hash extraído. Como mostrado na Seção 2.4, a saída do algoritmo gera uma etiqueta menor em tamanho, mas matematicamente equivalente a mensagem original. Como no caso não é de interesse em proteger o conteúdo da mensagem, mas apenas sua autoria, a assinatura extraída pode ser anexada a mensagem do autor e confirmada pelo receptor. O algoritmo criptográfico mais usado neste tipo de sistema é o RSA.

2.8 Certificado Digital

Certificação Digital é a tecnologia que adota mecanismos de segurança, por meio de algoritmos matemáticos, capazes de garantir autenticidade, integridade e não-repúdio às informações eletrônicas (MENEZES *et al.*, 2018). No ambiente virtual, o certificado digital é um arquivo eletrônico armazenado em uma mídia digital que serve como uma comprovação de que a entidade autora de uma mensagem é de fato quem diz ser, associando seu nome a seu par de chaves e a permite fazer assinaturas digitais em seu nome com mesma validade jurídica da assinatura feita a punho. Este certificado pode ser obtido por qualquer um e é necessário se dirigir a uma Autoridade Certificadora (AC)[1] para fazer o requerimento. Seu uso mais comum na *Internet* é feito em transações comerciais, assim é possível que instituições e organizações operem de forma legal no ambiente digital.

2.9 *Blockchain*

A *blockchain* foi criada por *Satoshi Nakamoto* (NAKAMOTO, 2008) como um sistema de pagamentos eletrônicos, não regulado pelos bancos ou uma entidade central, mas pelos próprios usuários. Sua estrutura de rede P2P permite que estes sejam conectados uns aos outros e troquem criptomoedas entre si, sem dependerem de um intermediário, ao contrário do tradicional modelo cliente-servidor ou em núvem, onde os dados dos usuários são armazenados e

[1] A Autoridade Certificadora é uma entidade, que pode ser pública ou privada, responsável por emitir, distribuir, renovar, revogar e gerenciar Certificados Digitais dos solicitantes ou de outras ACs que estejam abaixo dela (CERTSIGN.COM.BR, 2020).

processados em um único centro de dados. Ao invés disso, os dados são armazenados em pacotes chamados de blocos, e replicados entre todas as máquinas da rede. Tais dados são mantidos consistentes em todos os computadores pelo algoritmo de consenso, que será discutido na Seção 2.9.1.

Modelos de rede descentralizada baseados na *blockchain* são difíceis de serem projetados, implementados, e frequentemente são associados com problemas de performance, escalabilidade e altos custos. No entanto, oferecem algumas vantagens quando comparados ao modelo cliente-servidor, como segurança, imutabilidade, confiança e transparência. Estas propriedades podem ser alcançadas não apenas porque a *blockchain* é uma única tecnologia em si, mas uma combinação de princípios econômicos, teoria dos jogos, criptografia, engenharia e ciência da computação (SINGHAL *et al.*, 2018).

Desde sua criação, a tecnologia da *blockchain* vem passando por diversas atualizações com o objetivo de tornar o sistema cada vez mais eficiente e útil em outras áreas além da economia, dando origem a milhares de novas redes, como a *Ethereum* que possúem novas funcionalidades ausentes no *Bitcoin*, como por exemplo os contratos inteligentes, tamanho do bloco e diferentes protocolos de consenso. Sendo assim não é possível determinar uma estrutura geral para todas as diferentes implementações de *blockchains* existentes, e considerando a complexidade de cada uma. Mas é possível, conforme Singhal *et al.* (2018) abstrair uma estrutura composta pelas seguintes camadas e ilustrada na Figura 3.

Camada de aplicação: É a camada onde as aplicações da rede são construídas. *Ethereum* introduzida em 2013 por *Vitalik Buterin* e as redes criadas subsequentemente introduziram o uso de contratos inteligentes nas *blockchains*, estes são aplicações programáveis que uma vez criadas e armazenadas na rede, podem executar como "agentes autônomos"sem a intervenção humana. Sendo assim, a camada de aplicação é onde estas são desenvolvidas. Mesmo já possuindo suporte a contratos inteligentes, o *Bitcoin* ainda apresenta deficiências quando comparado a *blockchains* mais recentes como a *Ethereum*, sendo estes:

- *Falta de completude de Turing*: Embora o *script* do *Bitcoin* tenha uma ampla gama de instruções computacionais, este ainda é deficiente em categorias como *loops*. Estes são usados para evitar *loops* infinitos em verificação de transações, consumindo assim mais recursos computacionais como no cálculo de curva elíptica, em contraste com o script melhor otimizado da *Ethereum*.
- *Cegueira de valor e inexistencia de estado*: Ao contrário do sistema de contas na

Ethereum, na rede *Bitcoin* o estado do saldo de uma conta após realizar uma transação é determinado pelo cálculo recursivo de seus *Unspent Transaction Output* (UTXO)s restantes, que são contabilizados como transações contendo um determinado valor em *BTC*. Mesmo o valor de uma transação sendo muito pequeno este gera um UTXO o qual é não-fungível pela natureza do *bitcoin* podendo acumular indefinidamente e gerando um aumento do espaço de armazenamento ocupado pela carteira do usuário. Este tipo de ineficiência gera uma vulnerabilidade chamada de *dust attack* ou "ataque de poeira" no qual um ou mais usuários podem sobrecarregar a carteira de outro com várias transações de *spam* com valores pequenos ao ponto de que esta seja bloqueada e não possa mais realizar transações (SAAD *et al.*, 2020).

Camada de execução: É onde as instruções realizadas na camada de aplicação são executadas. As instruções executadas pelos contratos inteligentes da *Ethereum* são efetuadas apenas quando estas chegarem a camada de execução.

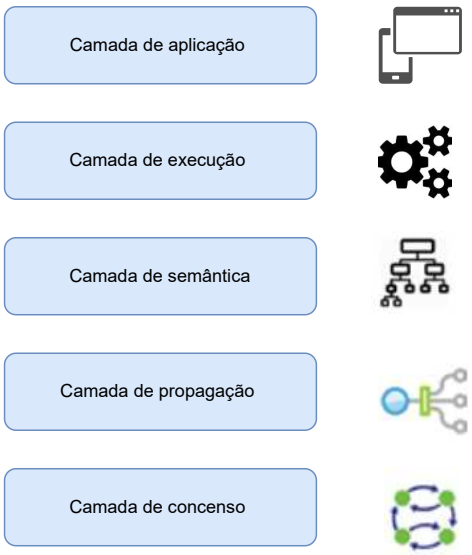
Camada de semântica: As instruções executadas são validadas e comparadas com o estado atual da rede. É nesta camada onde a rede *Bitcoin* ofereceu uma das maiores inovações da época em comparação a outros sistemas de pagamento eletrônicos que era o problema do gasto duplo. Basicamente, para que uma quantia de *bitcoin* seja gasta o protocolo automatizado da rede precisa verificar se essa quantia já foi gastada anteriormente por meio de uma validação recursiva de todas as transações anteriores (UTXOs). Posteriormente, a *Ethereum* introduziu o sistema de contas, em que quando uma transação credita uma conta outra é imediatamente debitada, assim tornando o sistema de saldo de usuários mais eficiente em tempo de performance pois o sistema do *Bitcoin* é demorado e inviável para ser adotado por sistemas de pagamentos reais já que uma transação pode levar mais de uma hora para ser confirmada devido ao crescente tamanho da rede.

Camada de propagação: As etapas anteriores ocorrem nos usuários da rede de uma forma individual. Para que esta se tornem uma parte integral da rede, precisam passar pela camada de propagação, onde serão transmitidas para os outros nós da *blockchain* para que assim seus estados sejam comparados e atinjam um único estado em comum da rede pelo concenso.

Camada de consenso: Nesta os usuários "votam"em um estado comum da rede. Basicamente, para um conjunto de novas transações na rede sejam efetivadas estas devem ser

agregadas em um pacote chamado de "bloco", validadas e aprovadas pela maioria dos usuários da rede para que possam se tornar parte integral desta. Quando nos referimos a custos para manter a rede funcionando, isto não é remetido a sua infraestrutura mas a valores de recompensa aos mineradores e validadores da rede, como incentivo a participarem do processo de concenso e trabalharem para mante-la em funcionamento. Mais detalhes serão cobertos na subseção seguinte.

Figura 3 – Estrutura em camadas da rede *blockchain*



Fonte: Adaptado de Singhal *et al.* (2018)

2.9.1 Protocolos de consenso

Por ser um dos pontos-chave da arquitetura de uma *blockchain*, frequentemente é a camada de consenso onde as estratégias para atrair mineradores mais se diversificam. Esta subseção aborda os tipos de protocolos de consenso mais comuns em vigor nas *blockchains* atuais, incluindo *Ethereum*, e aborda brevemente o protocolo de concenso empregado na *Solana*.

2.9.1.1 Proof of Work (PoW)

Traduzido como "Prova de trabalho", nesta os usuários que comportam-se como validadores de novas transações para manter o estado da rede honesto e conciso são recompensados com *bitcoins*, que são taxas pagas por outros usuários ou criados através do processo chamado de "mineração", que atribui aos validadores seu nome mais popular, "mineradores". O processo de

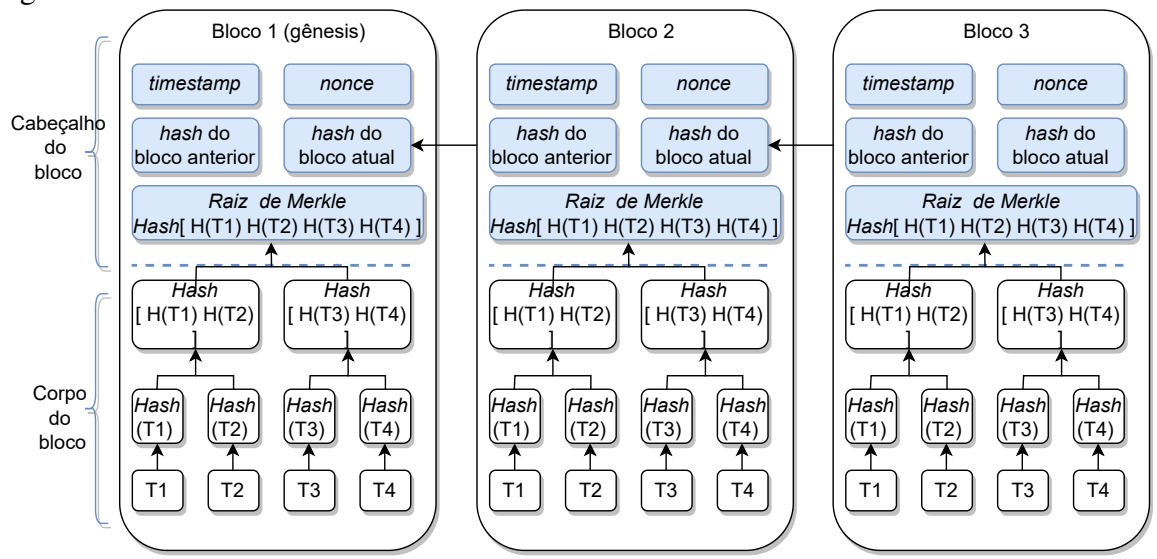
mineração de novos blocos é realizado em competição entre outros usuários e o vencedor é, em geral aquele que tem mais poder computacional para resolver um desafio de cálculo matemático.

A resolução deve ser difícil de ser produzida, garantindo assim que apenas os mineradores que trabalhem mais intensamente sejam recompensados. No entanto, a prova deve ser fácil e rápida de ser verificada pelos demais validadores. O processo de mineração é descrito como:

1. Cada novo usuário deve baixar uma aplicação cliente para tornar-se um membro da rede. Assim as transações existentes serão gravadas na sua máquina.
2. Em seguida, cada minerador ordena e grava as transações que recebeu em um bloco. A Figura 4 ilustra a estrutura de um bloco da rede *Bitcoin*. Os blocos existentes são aglomerados de transações e dados imutáveis gravados na *blockchain*.
3. O minerador deve calcular o *hash* do cabeçalho do bloco criado usando o algoritmo SHA-256. No entanto, o valor do campo do cabeçalho chamado *nonce* deve ser incrementado sob tentativa e erro repetidamente. O objetivo disso é obter uma colisão parcial, ou seja, situação em que o valor hash dado como saída do SHA-256 é menor que um valor alvo determinado pelo algoritmo de consenso.
4. Ao obter a resposta do desafio, esta deve ser anexada ao bloco proposto e transmitidos para os outros nós da rede para que possa ser validada.
5. Caso o resultado seja validado como correto pela maioria dos outros validadores da rede, então o novo bloco será adicionado a cadeia de blocos da *blockchain* e o usuário será recompensado com uma quantia de bitcoins que irão nascer do processo de mineração.

Nem todas as *blockchain*s adotam este processo, algumas optam por não gerar novas moedas e usam apenas as taxas pagas pelos demais usuários para recompensar os validadores assim como o *Bitcoin* eventualmente irá. Isto ocorre porque as moedas recompensadas aos mineradores tecnicamente não são geradas por meio da mineração, mas pertencem a uma reserva chamada *coinbase*, que foi proposta pelo como a principal forma de atrair usuários para a rede. No entanto com a crescente popularidade desta e a entrada de cada vez mais mineradores ao longo do tempo, este valor vai sendo gasto até o ponto em que não haverão mais *bitcoins* para recompensá-los e a rede terá que confiar aepnas em taxas de uso para manter o incentivo. *Bitcoins* não podem ser gerados indefinidamente, pois a confiança na moeda seria desgastada e seria equivalente a ação dos governos de imprimir dinheiro, o que desvaloriza sua moeda, segundo Keynes (1936). É exatamente a quantidade limitada e a confiança na segurança do sistema que

Figura 4 – Estrutura dos blocos do *Bitcoin*



Fonte: elaborado pelo autor

torna o *Bitcoin* uma moeda com valor monetário forte, mesmo não tendo um lastro como o ouro da economia tradicional.

2.9.1.2 Proof of Stake (POS)

Além do problema da reserva limitada o *Bitcoin* possui outro grande problema que é o de gasto de energia decorrente do poder computacional usado. Atualmente o processo de mineração é monopolizado por grandes organizações que investem em chamadas "fazendas de *bitcoins*"ou "minas de *bitcoins*". Estes se tratam de grandes *clusters* de computadores trabalhando juntos para receber parte da *coinbase*. No cenário inicial do *bitcoin* em que usuários de computadores pessoais eram os principais mineradores, não havia um gasto muito grande de energia, mas á medida que novos usuários se juntaram a rede, a dificuldade do processo têm aumentado significamente em ordem para manter a igualdade das recompensas, entre os mineradores o que tem levado a cada vez mais exigência de poder computacional e de energia.

Este cenário tem levado a intensas discussões a respeito de danos ambientas causadas pela PoW e até mesmo a ser banida em alguns países como a China (ALONSO *et al.*, 2021), forçando as novas *blockchains* emergentes a diversificar sua forma de incentivar trabalhadores na rede e a *blockchains* já existentes como a *Ethereum* a transicionar para um novo protocolo. Nesse contexto é criada a *Proof Of Stake* (POS). Seu maior diferencial é que não se trata de mineração, mas de validação de blocos de transações. Não há recompensas de mineração devido à geração de novas moedas, existem apenas taxas de transação para os mineradores (no caso há

apenas validadores) (SINGHAL *et al.*, 2018).

Nos sistemas POS, os validadores têm que vincular sua participação (hipotecar a quantidade de criptomoeda que gostaria de manter em jogo) para poder participar na validação das transações. A probabilidade de um validador produzir um bloco é proporcional à sua participação, quanto maior a quantidade em aposta, maior é a chance de validar um novo bloco de transações. Um minerador só precisa provar que possui uma certa porcentagem de todas as moedas disponível em um determinado momento em um determinado sistema monetário. Por exemplo, se um minerador possui 2% de todo o *Ether* (ETH) na rede *Ethereum*, ele seria capaz de minerar 2% de todas as transações na *Ethereum* (SINGHAL *et al.*, 2018). Em outras palavras, o usuário escolhido para gerar um novo bloco é decidido por sua quantidade de criptomoedas e não poder computacional.

2.9.1.3 Proof of History (POH)

Empregada pela primeira vez na *blockchain Solana*, este é traduzido para o portuquês como Prova de Histórico. Como os nós em uma rede distribuída não podem confiar no carimbo de tempo das mensagens recebidas de outros nós, o maior problema em redes distribuídas é o acordo de hora exata em que os eventos acontecem chamado de *timestamp*. Ou seja, uma fonte de tempo confiável para todos os nós da rede. A prova de histórico é uma função de atraso verificável (VDF) de alta frequência que executa um certo número de etapas para determinar o acontecimento de um determinado evento, mas fornece um resultado confiável. Sendo assim os nós podem usar as *timestamps* como uma fonte de verdade para gerar o próximo bloco sem ter que se fazer uma análise recursiva de toda a rede como no caso do *Bitcoin*. Como resultado, a sobrecarga do processo de consenso é reduzida(YAKOVENKO, 2018).

O tipo de algoritmo de concenso não impacta diretamente com custos de uso da *blockchain*. Assim como o caso do *Bitcoin*, o crescente número de usuários tem levado também a *Ethereum*, a rede atualmente mais popular, á ser bastante criticada por suas altas taxas de transações. Neste caso não se é referindo apenas a transações financeiras mas hospedagem de contratos e informações importantes como registro de documentos, credenciais e registros de produtos no formato de *Token Não-Fundível* (NFT). Desde então muitas redes tem sido criadas com o objetivo de competir com a *Ethereum*, seja oferecendo zero ou muito baixo custo de transação em troca de sacrificar parte da sua segurança como a *Nano*[2] ou uma forma de atrair

[2] https://nano.org/

usuários da *Ethereum* oferecendo integração a rede e mais privilégios adicionais como no caso da *Avalanche*[3] e *Polkadot*[4]. O atual cenário do mercado de criptoativos é de intensa competição.

[3] https://www.avax.network/
[4] https://polkadot.network/

3 TRABALHOS RELACIONADOS

Com os problemas do processo atual de emissão de diplomas e documentos legais já mencionados anteriormente, sendo estes o risco de perda, dano e a dificuldade de garantir a autenticidade, soluções digitais começaram a ser propostas nos últimos anos com serviços de digitalização de documentos e credenciais disponíveis para o público como BC Diploma(BCD, 2018) e Block Certs (BLOCKCERTS, 2017). No entanto, o BC Diploma opta por armazenar o documento inteiro de forma digital na *blockchain* e ambos serviços são altamente dependentes da *Ethereum*, o que são fatores que podem tornar-los investimentos de alto custo, o que para algumas IES, pode ser indesejável.

No trabalho de Saraiva *et al.* (2021) os autores propõem um sistema implementado com o atualmente descontinuado *framework* **Hyperledger Composer** da *International Business Machines* (IBM) para gerenciar diplomas de estudantes de medicina em *blockchain* (HYPERLEDGER, 2021). Nesse trabalho vale destaque das funções principais para o funcionamento do sistema, que são a função de registro exclusiva da instituição de ensino e a de verificação de diploma que pode ser feita por terceiros.

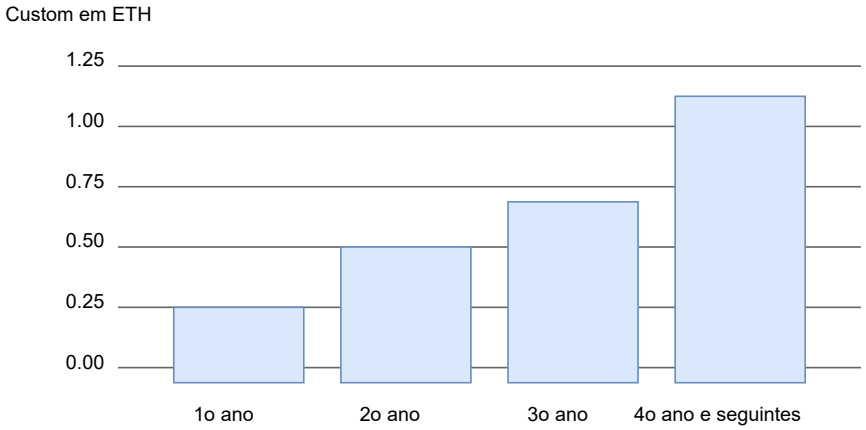
Em Cernian *et al.* (2021), os autores fazem uma análise de sistemas de soluções para gerenciamento de diplomas existentes e propõe um sistema similar a o do trabalho anterior, usando a rede *Ethereum*, na Indonésia onde muitos profissionais entram no mercado de trabalho com diplomas falsificados. Para resolver o problema, o sistema proposto gira ao redor de quatro entidades: Estudantes, diploma, universidade e o trabalhador, com detalhes dos casos de uso de geração, registro, envio, validação e cancelação do diploma.

Prado e Henriques (2018) introduziram em seu modelo proposto uma terceira entidade chamada autoridade certificadora (não confundir com AC da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil)), que é encarregada com as responsabilidades de registro e verificação na *blockchain*. O sistema é implementado usando a rede *Ethereum*.

No trabalho de Kamil *et al.* (2021) os autores propõem uma possível solução para o gerenciamento de diplomas com uso de contratos inteligentes da *Ethereum*. A solução é menos detalhada, mas vale observar a análise de custos de transações da Ethereum em que os custos sobem em quatro anos de uso da rede como ilustrado na Figura 5.

Tang (2021) propõe um modelo mais refinado e detalhado comparado aos anteriores,

Figura 5 – Custo estimado de uso da aplicação proposta usando *Ethereum* em 4 anos por uma IES da Indonésia, por Kamil *et al.* (2021)



Fonte: Adaptado de Kamil *et al.* (2021).

um que possa ser usado para o gerenciamento de diplomas e adaptado para qualquer *blockchain* permissionada ou não permissionada, dando ao implementador do sistema a opção de usar uma *blockchain* com menor custo que a *Ethereum*. Neste a função de verificação pode ser usada por qualquer terceiro que tenha acesso a *blockchain*. No entanto, assim como os outros trabalhos relacionados este também opta por armazenar o diploma em si na *Blockchain*, o que pode se tornar custoso. O modelo proposto no presente trabalho contorna este problema pelo uso da *Interplanetary File System* (IPFS) para armazenar o documento, e não a *Blockchain*.

Stellnberger (2016) propõe em detalhes uma implementação teórica similar ao de Tang (2021) mas usando MD5 como algoritmo *hash* para extrair do documento um valor *hash* ou "identificador universal" e armazenar este na *blockchain* ao invés do documento original diminuindo os custos, pois como visto na Seção 2.7, não há necessidade de cifrar um arquivo inteiro quando desejamos apenas garantir sua integridade. No entanto, o uso do MD5 como algoritmo *Hash* é inseguro pois pode ser quebrado por ataques de força bruta como mostrado por Thompson (2005) que descreve como um ataque explorando uma fraqueza do MD5 causou uma grave falha de segurança na estrutura de certificado das ACs nos Estados Unidos.

Stellnberger (2016) também sugere o uso da tecnologia Json Web Token (JWT) para geração de assinaturas digitais, esse pode ser usado para comprovar que o diploma além de existir, tenha sido de fato emitido por uma IES legítima e autorizada por uma AC. Com o identificador e a assinatura do diploma gerados, ambos são armazenados na *blockchain* escolhida.

A tabela 1 mostra uma comparação das abordagens de cada autor para a problemática

abordada no presente trabalho.

Tabela 1 – Comparação de trabalhos

Autor	Blockchain usada	Local de armazenamento	Analise dos custos
Cernian *et al.* (2021)	Ethereum	Blockchain	Não
Kamil *et al.* (2021)	Ethereum	Blockchain	Sim
Tang (2021)	não especificado	Blockchain	Sim
Saraiva *et al.* (2021)	Hyperledger Fabric	Blockchain	Não
Prado e Henriques (2018)	Ethereum	Blockchain	Não
Stellnberger (2016)	não especificado	não especificado	Não

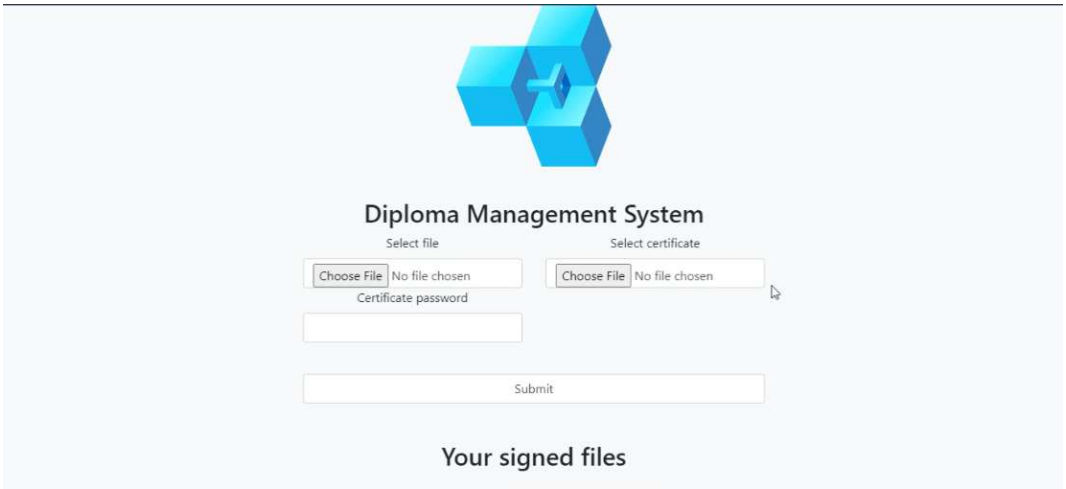
4 MODELO PROPOSTO

Na introdução discutimos as vulnerabilidades do gerenciamento tradicional de diplomas, sendo estas a falsificação, dano e perda do documento. Os riscos de dano e perda naturalmente já seriam evitados com a introdução do formato digital, no entanto é necessário que esta versão digital do documento tenha valor legal equivalente ao diploma tradicional e seja mais seguro que este do ponto de vista de não poder ser copiado ou forjado. Para isso é interessante que além da assinatura digital que já é usada atualmente, seja também empregada uma possível solução usando as propriedades *blockchain* discutidas anteriormente, estas sendo a imutabilidade, transparência, descentralização e segurança para adicionar uma camada de maior segurança e disponibilidade dos documentos.

Com esta problemática em mente e com base nos trabalhos e pesquisas já existentes, a presente pesquisa propõe um sistema para gerenciamento de diplomas usando a tecnologia da *blockchain Ethereum* e uma versão de menor custo usando a *blockchain Solana*. O sistema funcionará entre os seguintes atores:

1. Aplicação do usuário: Aplicação *web* responsável pela comunicação entre o usuário da IES e as funções da *blockchain* e da rede IPFS. A aplicação permitirá a função de registro de diplomas em formato digital que serão devidamente assinados digitalmente e registrados na IPFS por meio de contrato inteligente.

Figura 6 – Interface da aplicação do usuário

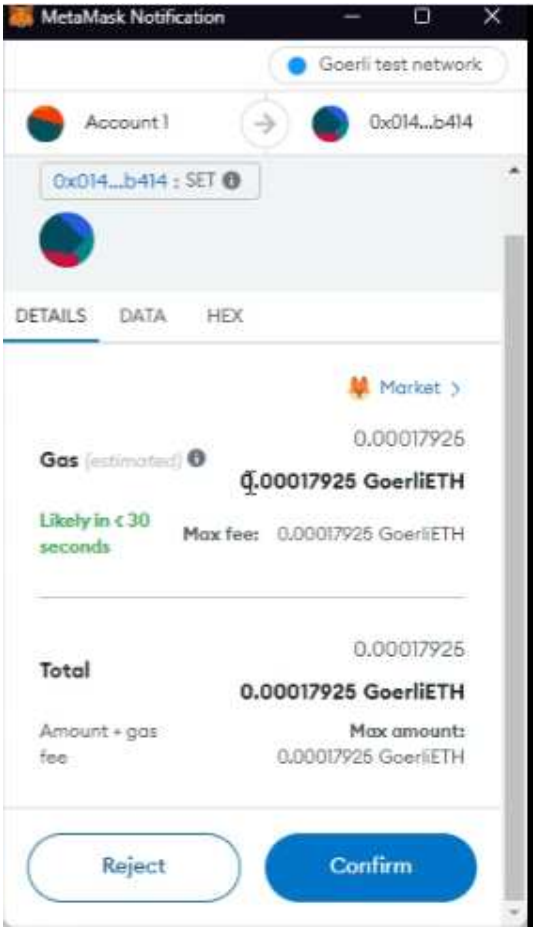


Fonte: Elaborado pelo autor.

2. Carteira da *Blockchain*: Aplicação de usuário da IES em formato de extensão de navegador responsável por permitir que o usuário interaja com a *blockchain*. Seu principal uso no

sistema em questão será de autenticar o usuário do sistema e de assinar transações com o seu par de chaves da *blockchain*. Sempre que o usuário realizar uma operação de registro de diploma, uma notificação será enviada.

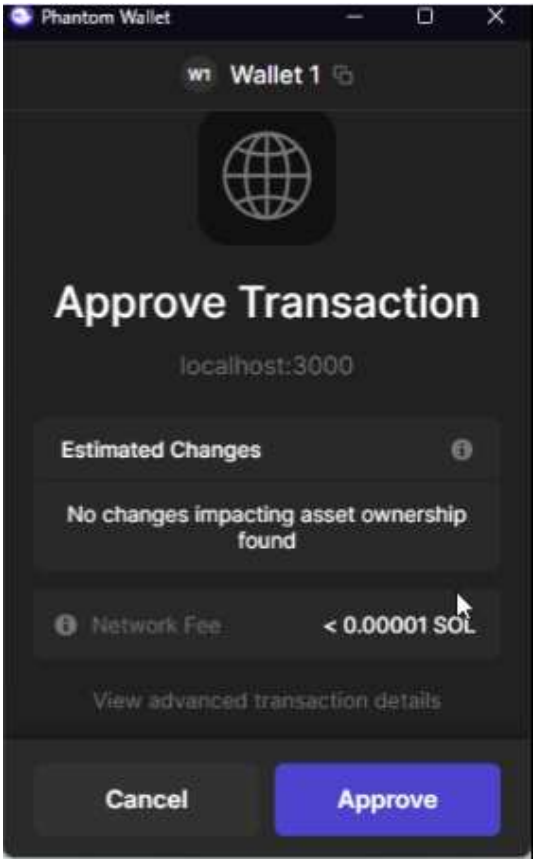
Figura 7 – Interface da carteira usada na aplicação Ethereum (notificação pedindo confirmação do usuário para realizar transação.)



Fonte: Elaborado pelo autor.

3. Usuário da IES: Membro de uma Instituição de ensino qualificada pelo Ministério da Educação (MEC) em posse de um certificado digital emitido pela ICP Brasil. O membro da IES é responsável por usar o sistema para assinar digitalmente e armazenar diplomas digitais na rede IPFS através da aplicação. Os diplomas emitidos são de total responsabilidade da IES. A instituição também deve ser responsável por guardar seguramente seu certificado digital e suas credenciais na *blockchain*, pois quando um invasor corrompe o emissor dos diplomas e obtém suas credenciais este atacante pode tentar falsificar diplomas ou fazer outras coisas (como por exemplo vazamentos de privacidade) (TANG, 2021).
4. Estudante: Ator vinculado a uma IES para obter posse de um diploma, este é matriculado

Figura 8 – Interface da carteira usada na aplicação Solana (notificação pedindo confirmação do usuário para realizar transação.)



Fonte: Elaborado pelo autor.

em um curso de educação superior dessa. Este estudante receberá de sua IES a posse de um diploma digital após terminar seu curso. Este não será usuário diretamente do sistema, pois apenas receberá da IES o produto final do sistema que é o diploma digital por algum outro meio digital (e-mail, portal da instituição, etc.).

5. Validador: Consiste de qualquer indivíduo ou organização que deseje comprovar a autenticidade de um diploma emitido pelo sistema, este pode ser uma organização recrutando para emprego, uma outra instituição onde o estudante deseje cursar (como mestrado ou doutorado) ou até mesmo algum integrante de dentro da própria instituição emissora ou o próprio estudante em si.

6. *Blockchain*: Uma fonte de valores imutável e distribuída geograficamente onde os valores *hash* dos diplomas já assinados e armazenados na *IPFS* serão registrados. Estes são identificadores dos arquivos armazenados na *IPFS* e funcionam como uma prova de que os arquivos existem e são íntegros, pois uma vez registrados na *blockchain* sua autenticidade poderá ser comprovada pela criptografia. Este modelo de solução é baseado no trabalho de

Stellnberger (2016) que opta por armazenar um hash ao invés do diploma em sí, mantendo a possibilidade de comprovar sua integridade, por meio de funções *Hash*, sem precisar arcar com os custos de armazenamento de um arquivo grande na rede.

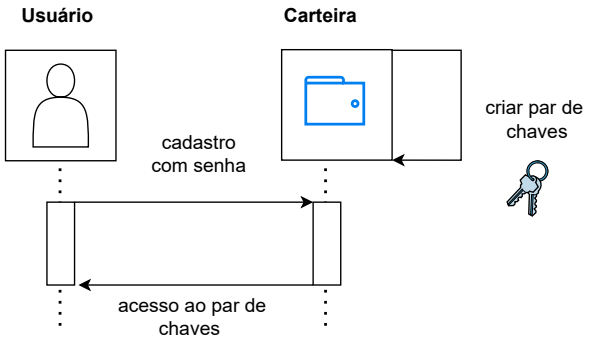
7. IPFS: É uma rede pública e P2P descentralizada similar a *blockchain* mais voltada para armazenamento de arquivos volumosos e é empregada no modelo proposto devido ao elevado custo de armazenamento de dados na *blockchain*. A IPFS será responsável por armazenar os arquivos dos diplomas enquanto a *blockchain* armazenará os identificadores *hash* dos arquivos, estes são *hashes* gerados pela IPFS com vínculo a um arquivo existente na rede.

4.1 Funcionamento do sistema

Com estes sete atores mencionados anteriormente, o sistema funcionará sob a interação de cada um deles como:

1. Cadastro de Usuário: Um representante da IES deve dirigir-se a uma AC da ICP Brasil para obter um arquivo de certificado digital no formato Personal Information Exchange (pfx). Em seguida o usuário da IES encarregado da emissão de diplomas deverá obter a aplicação cliente desejada dentre as duas opções de *blockchain* fornecidas.

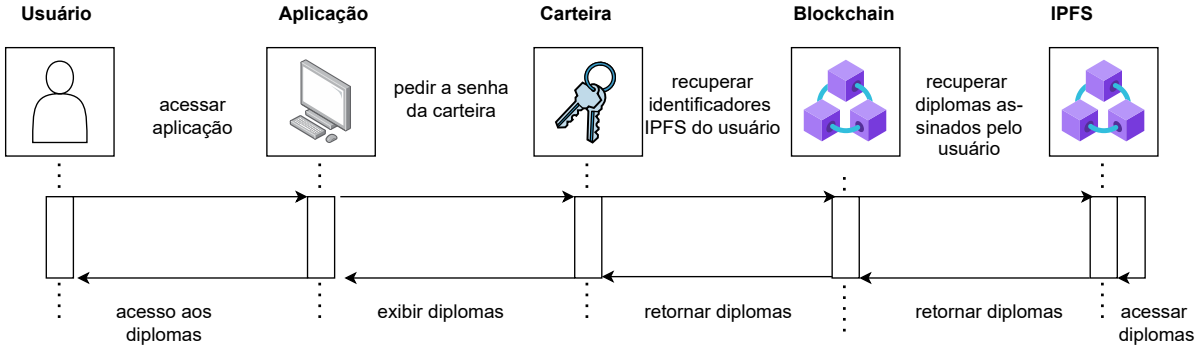
Figura 9 – Cadastro de Usuário



Fonte: Elaborado pelo autor

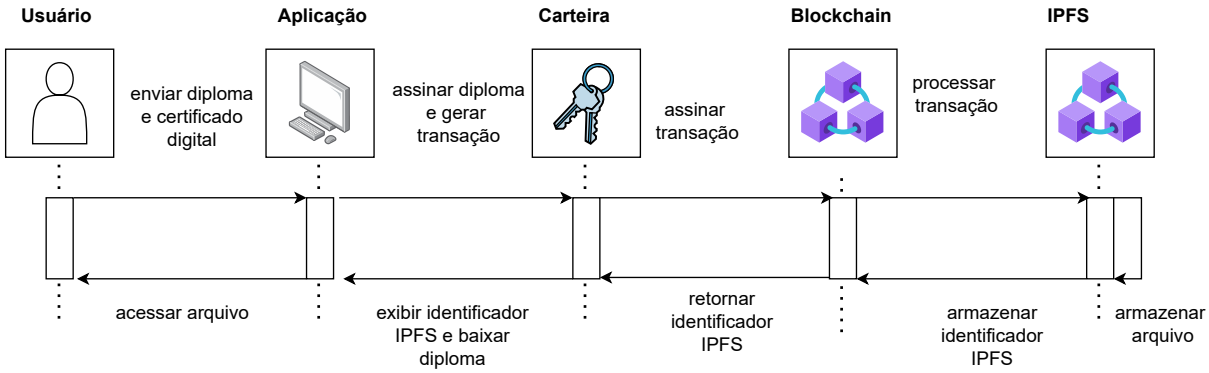
O usuário deverá também baixar e criar uma conta em uma das extensões de navegador para gerenciamento de Carteira Digital da *blockchain* escolhida. Caso escolha o cliente *Ethereum* deverá usar a *MetaMask* e caso escolha a aplicação cliente para a rede *Solana*

Figura 10 – Login de Usuário



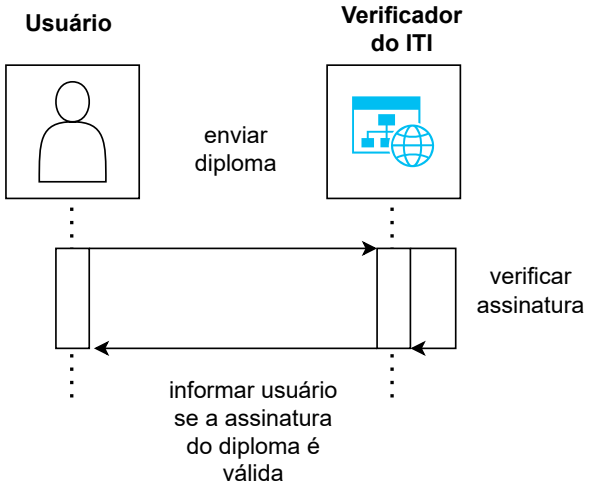
Fonte: Elaborado pelo autor

Figura 11 – Registrar diploma



Fonte: Elaborado pelo autor

Figura 12 – Autenticar Assinatura



(Usuário se refere ao verificador de posse do diploma)

Fonte: Elaborado pelo autor

deverá usar a *Phantom Wallet*. Estas aplicações são responsáveis por criar e gerenciar um par de chaves do usuário para que ele possa usar a função de registro (Não confundir com o par de chaves do certificado digital, estes serão usados para gerar a assinatura digital do

diploma enquanto o par de chaves da *blockchain* serão usados para assinar as transações do sistema). Por fim, o usuário deve adicionar saldo de cripto moedas à sua carteira para pagar pelas transações da *blockchain*. Cripto moedas reais podem ser compradas com corretoras. No entanto, na seção de testes foram usadas moedas de teste sem valor real.

2. Autenticação do usuário: Após o cadastro do usuário da IES, este poderá acessar o sistema para registrar diplomas digitais. O processo de autenticação será controlado pela extensão de navegador da carteira que pedirá a senha do usuário da IES sempre que ele acessar a aplicação. Após se autenticar o sistema irá exibir uma lista de todos os arquivos registrados por ele. Pois os arquivos são vinculados a sua carteira.
3. Registrar diploma: Após autenticado na aplicação, o usuário da IES irá fazer *upload* de um diploma no formato *Portable Document Format* (PDF) e de seu certificado digital no formato pfx e clicar no botão "*Submit*". O processo irá gerar uma transação da *blockchain* que será notificada pela extensão da carteira. O usuário deverá confirmar a transação para prosseguir com o registro do diploma e será cobrada uma taxa do balanço da sua carteira. Após alguns segundos o identificador *hash* do diploma será retornado da IPFS e exibido na tela por meio do contrato inteligente e a aplicação pedirá permissão para baixar uma cópia do arquivo para o computado do usuário.
4. Enviar diploma: A etapa de envio do identificador *hash* do diploma para o estudante poderá ser feita por *e-mail* ou disponibilizado em outro ambiente virtual como o portal da instituição.
5. Validar diploma: De posse do identificador o estudante com posse de um diploma registrado no sistema poderá acessar o sítio do Verificador de Conformidade do Instituto Nacional de Tecnologia da Informação (ITI) para validar a autenticidade deste. Na aplicação de testes a validação é feita por um leitor de PDF que possui funcionalidade de validar assinaturas digitais.

4.2 Análise de Resultados

Como mencionado anteriormente o principal objetivo deste trabalho é oferecer a IES um sistema de emissão de diplomas digitais usando *blockchain* de baixo custo. Portanto esta seção será dedicada a comparação de custo financeiro e tempo de execução para um mesmo processo de registro e recuperação de diplomas realizado em duas opções de *blockchains*

diferentes, sendo estas a *Ethereum* e a *Solana*, durante diferentes horários e dias da semana. A comparação tem objetivo de encontrar a melhor forma de a IES usar o sistema.

A escolha das *blockchains* se deu pelo fato de que a *Ethereum* é atualmente a *Blockchain* mais popular devido ao seu alto valor de mercado e ampla comunidade de desenvolvedores melhorando o sistema constantemente. No entanto, devido a este alto valor de mercado o sistema baseado nesta *blockchain* pode não ser o mais viável para uma IES que busque um melhor custo benefício. Sendo assim é proposto uma versão da mesma aplicação mas usando a *Solana*, uma *blockchain* emergente e com crescente valor de mercado devido ao seu baixo custo e alta confiabilidade.

4.3 Análise do custo financeiro

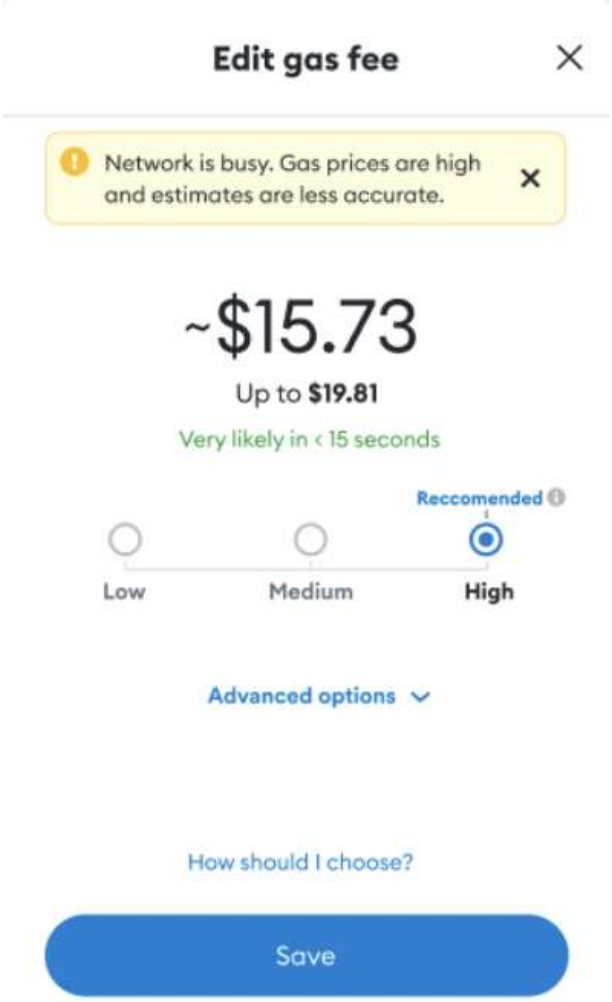
Para evitar problemas de abuso da rede, toda computação programável na *Ethereum* está sujeita a taxas chamadas de *gas fee*, como por exeemplo criar e fazer chamada de contratos (WOOD *et al.*, 2014). Tais taxas variam de acordo com a disponibilidade de computação na rede, mas são especialmente voláteis na *Ethereum* quando comparado a *Solana* (COINCODEX.COM, 2023).

Para a aplicação desenvolvida neste trabalho, é mostrada uma comparação de custo e de tempo, onde uma mesma operação com contrato inteligente é realizada em ambas *blockchains* durante diferentes horários entre os dias 17 de Abril e 5 de Maio de 2023. Os arquivos usados como diplomas foram documentos em PDF de aproximadamente 400 KB (*kilobytes* em média, durante períodos constantes de tempo.

No gráfico das Figuras 14 e 15 é possível observar que o processo de armazenamento do diploma digital assinado na IPFS por meio do contrato inteligente da *Ethereum* chega a custar em média um pico de $20 Dólares por volta do horário de meio dia devido a grande sobrecarga da rede em horário comercial, que é especialmente alto em dias de quarta-feira. Tais horários de alta são notificados pela carteira do usuário quando pedir por confirmação (Figura 13).

As transações realizadas pela *Solana* por outro lado, mantém um custo constante de $0.000109 dólares ao longo da semana e sem variações relacionadas ao horário do dia, fazendo a aplicação muito mais atrativa para as Instituições que escolherem essa opção do sistema em comparação a da *Ethereum*, em que as operações deveriam ser processadas ao final do dia para que tenham um melhor custo-benefício.

Figura 13 – Notificação de horário de alta Metamask



Fonte: demonstração *Metamask*

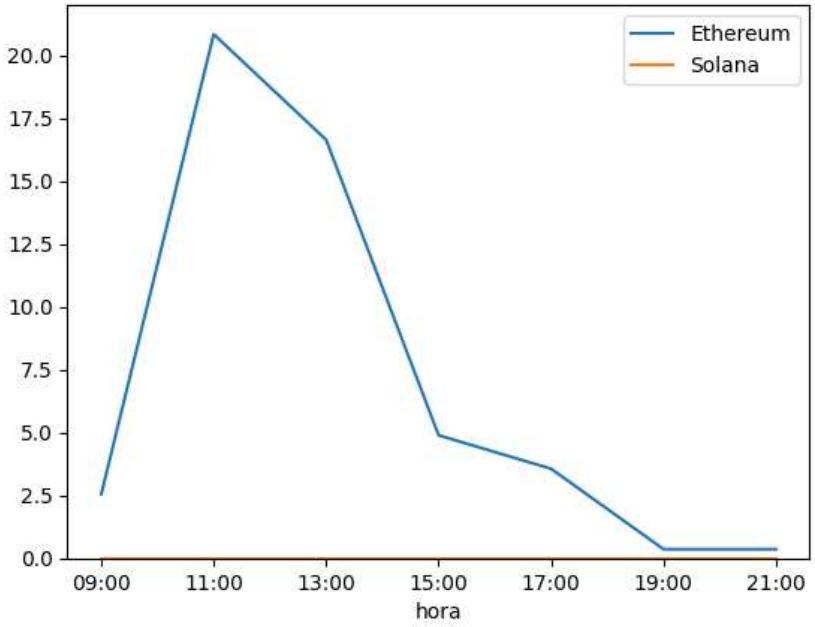
Legenda: "A rede está congestionada. Preços do Gas estão altos e estimativas menos precisas".

4.4 Análise do tempo de execução

Outro fator de grande diferença observado entre as duas aplicações é o custo de tempo para se completar uma operação que é significativamente mais baixa na *Solana* do que na *Ethereum* como ilustrado nas Figuras 16 e 17. Assim como na complexidade computacional há picos ao final da semana entre os horários de 15:00 e 17:00. Na *Solana* tais variações não são muito significativas.

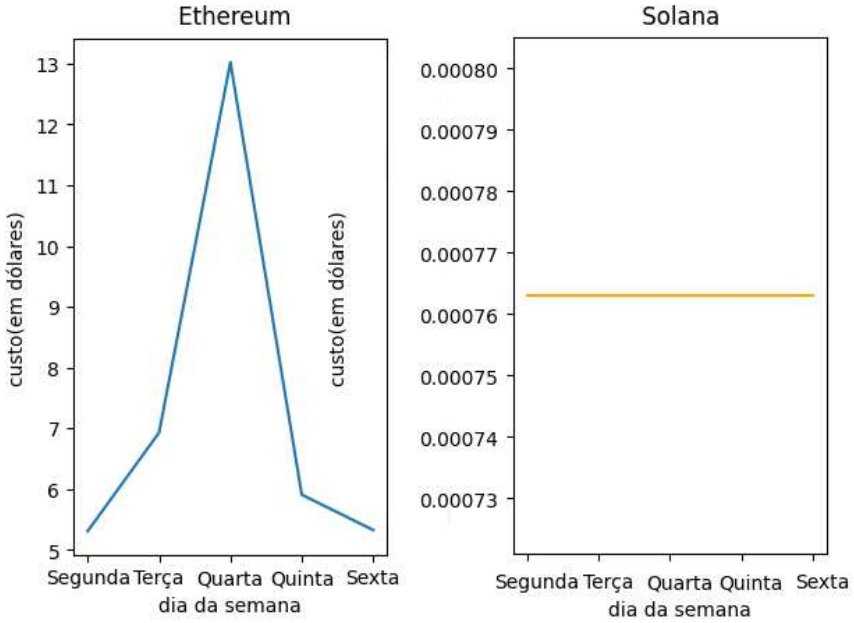
Para se recuperar os diplomas assinados por um usuário por meio do contrato inteligente da *Ethereum*, a complexidade de tempo também mostra um decréscimo proporcional ao horário e dia similar a análise de custo para se armazenar diplomas tendo picos em terça por volta das 13:00 do dia. Na *Solana* tal complexidade é muito menor como mostrado nas Figuras 18 e 19.

Figura 14 – Custo médio de transação Ethereum x Solana em Dólar por horário (cotação de 17 Abril - 5 de Maio. Registro do diploma).



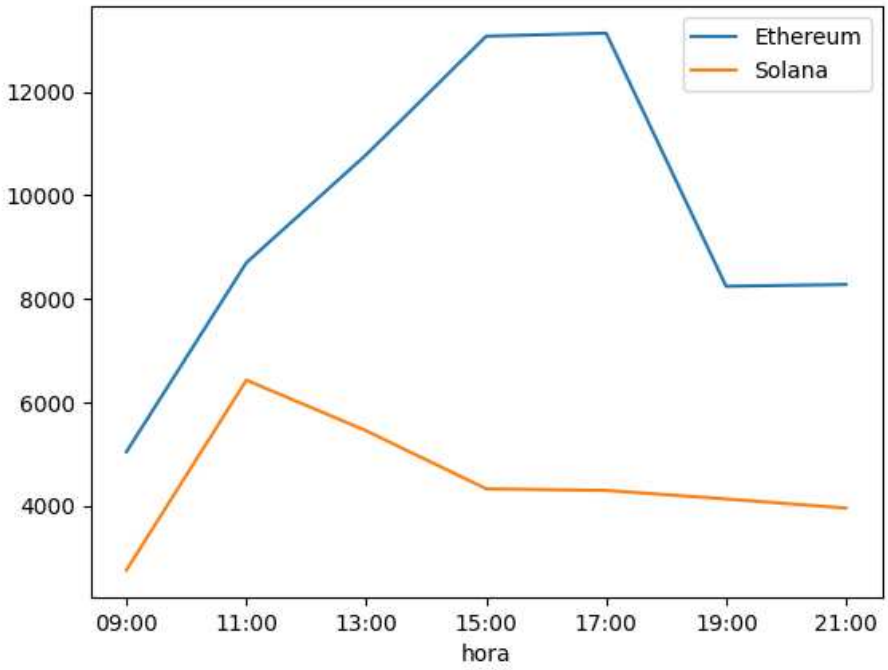
Fonte: elaborado pelo autor

Figura 15 – Custo médio estimado de transação *Ethereum* x *Solana* em Dólar por dia (cotação de 17 de Abril - 5 de Maio. Registro do diploma).



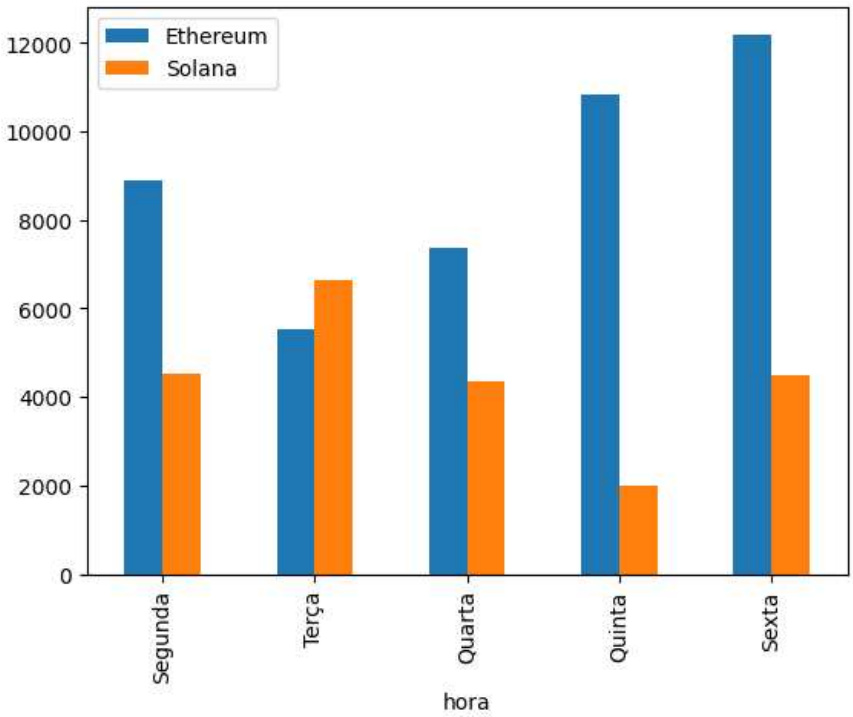
Fonte: elaborado pelo autor

Figura 16 – Tempo médio estimado por horário (em mili segundos. Registro do diploma).



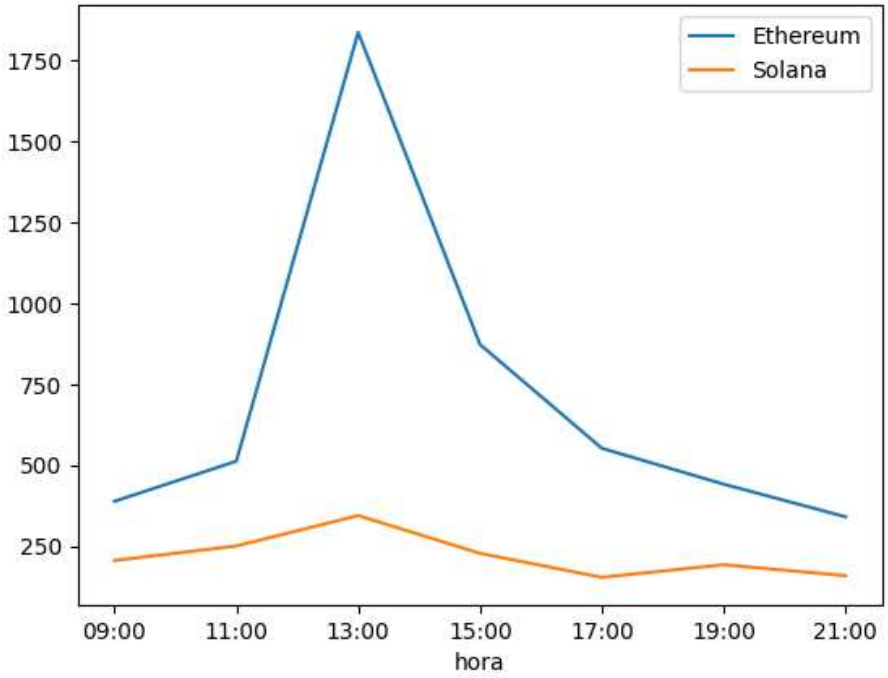
Fonte: elaborado pelo autor

Figura 17 – Tempo médio estimado por dia (em mili segundos. Registro do diploma).



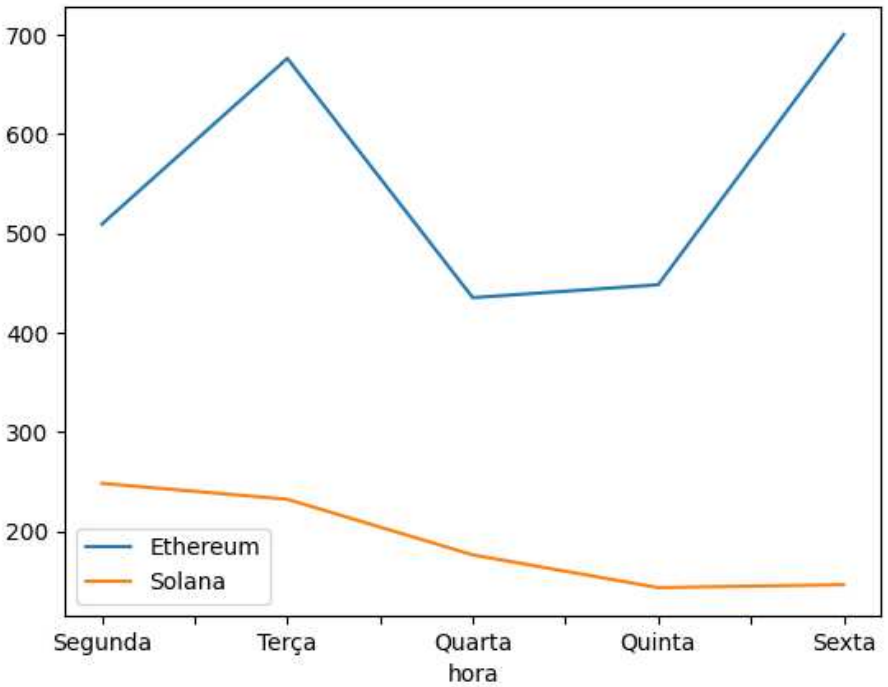
Fonte: elaborado pelo autor

Figura 18 – Tempo médio estimado por horário (em mili segundos. Recuperação do diploma).



Fonte: elaborado pelo autor

Figura 19 – Tempo médio estimado por dia (em mili segundos. Recuperação do diploma).



Fonte: elaborado pelo autor

5 CONSIDERAÇÕES FINAIS

O presente trabalho explora a viabilidade do uso da tecnologia *Blockchain* para oferecer segurança aos diplomas de estudantes de educação superior. A *Blockchain Ethereum*, apresenta-se como um opção tecnicamente viável, mas cobra um preço elevados para a execução das operações, como mostrado na seção de resultado. Assim, uma melhor opção, tanto do ponto de vista técnico como financeiro, é a *Blockchain Solana*, devido aos baixos custos de taxas de transações e crescente popularidade de mercado.

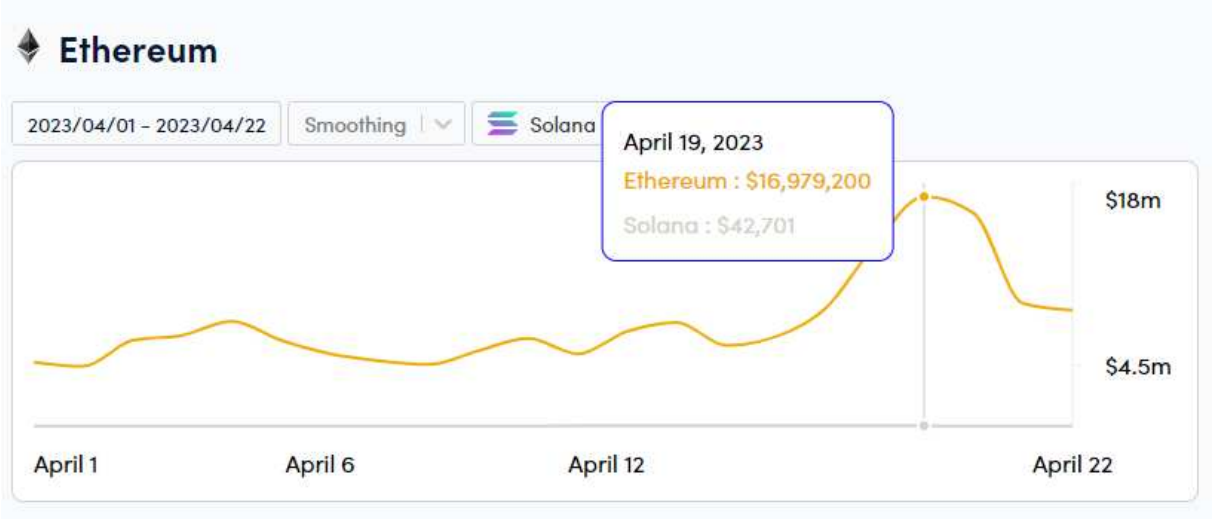
As propriedades da *Blockchain*, tais como, descentralização, transparência e imutabilidade, são pontos chave para o funcionamento do modelo proposto, pois asseguram as três propriedades da segurança da informação desejadas: integridade, disponibilidade e a autenticidade. Em conjunto com o armazenamento na rede IPFS, o modelo proposto permite que o documento digital seja mais seguro que o documento em papel, pois uma vez registrados e armazenados, os diplomas não podem ser modificados, apenas visualizados, prevenindo adulteração e falsificação. E o acesso a estes não pode ser cortado ou bloqueado pois a IPFS irá garantir que eles estejam sempre disponíveis para qualquer um que deseja acessá-los e confirmar sua autenticidade.

5.1 Ameaças a validade

Devido ao alto custo de uso, os testes realizados foram feitos nas redes de testes da *Ethereum* e *Solana*, onde as cripto moedas não possuem valor real. Estas são redes usadas por desenvolvedores de protocolos ou desenvolvedores de contratos inteligentes para testar atualizações de protocolo, bem como contratos inteligentes em potencial em um ambiente de produção antes da implantação na rede principal (ETHEREUM, 2023). No entanto o valor das taxas de uso na rede de testes é espelhado nos valores da rede comercial como é possível observar na Figura 20 que mostra o total gasto por dia com transações na rede comercial da *Ethereum* versus a *Solana*. É possível observar que os resultados são bem próximos aos obtidos na Seção 4.2.

Outra potencial ameaça a validade do trabalho seria o fato de que os testes não foram realizados em um sistema com múltiplos usuários, então a escalabilidade deste não pode ser estimada. No entanto para trabalhos futuro o código está disponível e apropriadamente documentado para possíveis continuações em <https://github.com/rodrigolb01/IPFS-digital-sign-dapp>.

Figura 20 – Comparação de custo na rede comercial da *Ethereum* vs *Solana*



Fonte: https://cryptofees.info/protocol/eth

5.2 Trabalhos Futuros

1. Oferecer uma versão do sistema que use apenas uma carteira para as duas versões diferentes da aplicação. Atualmente a *Phantom Wallet* possui suporte tanto para *Ethereum* quanto para *Solana*.
2. Integração com o verificador de conformidade. Pois atualmente o usuário deve realizar a validação de conformidade dos diplomas assinados pelo sistema de forma externa pelo verificador do ITI.
3. Armazenar o certificado digital do usuário na aplicação ou manter na seção do usuário para melhor conveniência.
4. Buscar opções de menor custo as *blockchains* usadas para a baratear anda mais a aplicação.

REFERÊNCIAS

ALONSO, S. L. N.; JORGE-VÁZQUEZ, J.; FERNÁNDEZ, M. Á. E.; FORRADELLAS, R. F. R. Cryptocurrency mining from an economic and environmental perspective. analysis of the most and least sustainable countries. **Energies**, MDPI, v. 14, n. 14, p. 4254, 2021.

BARKER, E. *et al.* Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms. **NIST special publication**, p. 800–175B, 2016.

BCD. **Blockchain Certified Data Token WhitePaper V2**. 2018. <https://www.allcryptowhitepapers.com/blockchain-certified-data-token-whitepaper/>. Accessado: 2022-06-23.

BELLARE, M.; KOHNO, T. Hash function balance and its impact on birthday attacks. In: SPRINGER. **International conference on the theory and applications of cryptographic techniques**. CA, USA, 2004. p. 401–418.

BLOCKCERTS. **Issue of Blockcerts under Ethereum [under development]**. 2017. <http://community.blockcerts.org/t/issue-blockcerts-on-ethereum-under-development/348>.

CERNIAN, A.; VLASCEANU, E.; TIGANOAIA, B.; IFTEMI, A. Deploying blockchain technology for storing digital diplomas. In: IEEE. **2021 23rd International Conference on Control Systems and Computer Science (CSCS)**. Polytechnic University of Bucharest, 2021. p. 322–327.

CERTSIGN.COM.BR. **O que é uma Autoridade Ceritifcadora?** 2020. <https://blog.certisign.com.br/o-que-e-uma-autoridade-certificadora/>.

COINCODEX.COM. **How much is Solana gas fee?** 2023. <https://coincodex.com/article/24933/solana-gas-fees/>.

DIFFIE, W.; HELLMAN, M. E. **New directions in cryptography**. Stanford, CA, USA: Routledge, 1976. 143–180 p.

DREAMS, T. **The Solana Gas Fee Trend**. 2022. <https://www.techdreams.org/crypto-currency/the-solana-gas-fee-trend/12713-20220206>.

ETHEREUM. **Ethereum networks**. 2023.

FIRMO, M. G. **Fake Diplomas and Signaling in Labor Markets: Evidence from Brazil**. Tese (Doutorado) — PUC-Rio, 2021.

FORBES. **How Thousands of Nurses Got Licensed With Fake Degrees**. 2023. <https://www.forbes.com/sites/emmawhitford/2023/02/21/how-thousands-of-nurses-got-licensed-with-fake-degrees/?sh=39c319755c6d>.

GARFINKEL, S. L. Nistir 8053. de-identification of personal information. **National Institute of Standards and Technology, US Department of Commerce, Gaithersburg, Maryland, USA**, 2015.

GLOBO, G. **Quase 3,5 milhões de alunos evadiram de universidades privadas no Brasil em 2021**. 2022. <https://g1.globo.com/educacao/noticia/2022/01/02/quase-35-milhoes-de-alunos-evadiram-de-universidades-privadas-no-brasil-em-2021.ghtml>.

GOV.BR. **Obter Segunda Via De Diploma de Graduação**. 2022. <https://www.gov.br/pt-br/servicos/obter-segunda-via-de-diploma-de-graduacao>.

HYPERLEDGER. **Hyperledger Composer End Of Life**. 2021. <https://www.hyperledger.org/use/composer>.

JUSBRASIL. **Artigo 304 do decreto lei n 2848 de 07 de dezembro de 1940**. 1940. <https://www.jusbrasil.com.br/topicos/10599626/artigo-304-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940>. Accessado: 2022-07-07.

KAMIL, M.; SUNARYA, P. A.; MUHTADI, Y.; ADIANITA, I. R.; ANGGRAENI, M. Blockcert higher education with public key infrastructure in indonesia. p. 1–6, 2021.

KEYNES, J. M. **The General Theory of Employment, Interest and Money**. University of Cambridge, UK: Macmillan, 1936. 14th edition, 1973.

KISSEL, R. **Glossary of key information security terms**. Gaithersburg, MD: Diane Publishing, 2011.

LENSTRA, A.; WANG, X.; WEGER, B. de. **Colliding X.509 Certificates**. 2005. Cryptology ePrint Archive, Paper 2005/067. <https://eprint.iacr.org/2005/067>. Disponível em: <https://eprint.iacr.org/2005/067>.

MENEZES, A. J.; OORSCHOT, P. C. V.; VANSTONE, S. A. **Handbook of applied cryptography**. University of Waterloo, ON, CA: CRC press, 2018.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, p. 21260, 2008.

NIST. **FIPS 180**. 1993. <https://csrc.nist.gov/publications/detail/fips/180/archive/1993-05-11>.

PRADO, N. F.; HENRIQUES, M. A. On-block certs: blockchain-based lightweight digital certificates. p. 177–180, 2018.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, ACM New York, NY, USA, v. 21, n. 2, p. 120–126, 1978.

SAAD, M.; SPAULDING, J.; NJILLA, L.; KAMHOUA, C.; SHETTY, S.; NYANG, D.; MOHAISEN, D. Exploring the attack surface of blockchain: A comprehensive survey. **IEEE Communications Surveys & Tutorials**, IEEE, v. 22, n. 3, p. 1977–2008, 2020.

SARAIVA, R.; ARAÚJO, A. A.; SOARES, P.; SOUZA, J. Miriam: A blockchain-based web application for managing professional registrations of medical doctors in brazil. p. 1–2, 2021.

SINGHAL, B.; DHAMEJA, G.; PANDA, P. S. **Beginning Blockchain: A Beginner's guide to building Blockchain solutions**. Bangalore, Karnataka, India: Apress, 2018.

STALLINGS, W. **Cryptography and network security, 4/E**. [S.l.]: Pearson, 2006.

STELLNBERGER, M. **Document Certification Through the Blockchain**. 2016. <https://www.martinstellnberger.co/document-certification-through-the-blockchain>. Accessed: 2022-06-23.

TANG, Q. Towards using blockchain technology to prevent diploma fraud. **IEEE Access**, IEEE, v. 9, p. 168678–168688, 2021.

THOMPSON, E. Md5 collisions and the impact on computer forensics. **Digital investigation**, Elsevier, v. 2, n. 1, p. 36–40, 2005.

WOOD, G. *et al.* Ethereum: A secure decentralised generalised transaction ledger. **Ethereum project yellow paper**, v. 151, n. 2014, p. 1–32, 2014.

YAKOVENKO, A. Solana: A new architecture for a high performance blockchain v0. 8.13. **Whitepaper**, 2018.

ANEXO A – FUNCIONAMENTO DO RSA

Para fazer uso do RSA, cada usuário pode gerar suas próprias chaves, isto é, a chave pública e a chave privada. Todo o processo de geração de chaves e criptografia do RSA tem base na aritmética modular (RIVEST *et al.*, 1978).

1. A geração das chaves começa pela escolha de dois números primos p e q. Os números escolhidos devem ser grandes (com tamanho superior a 100 algarismos) pois isto é fundamental para a segurança do sistema.
2. Com os dois números escolhidos, calcula-se

$$n = p \times q.$$

3. O próximo passo é escolher um exponente, denotado por e que seja primo relativo a $\phi(n)$, em que:

$$\phi(n) = (p-1)(q-1),$$

é a *função Totiente de Euler*.

4. Em seguida, calcula-se um inteiro d que satisfaça:

$$d \equiv e^{-1} \mod \phi(n).$$

5. Agora os números p e q não são mais importantes, na verdade devem ser descartados para evitar que vazem e comprometam a segurança do sistema. Os números n, e e d serão suficientes para gerar as chaves pública e privada.

Os números e e n representam a chave pública. E os números d e n representam a chave privada.

Sendo M o texto plano e C o texto cifrado, A cifração é realizada como:

$$C = M^e \mod n.$$

E a decifração de C é realizada como:

$$M = C^d \mod n.$$