Programa de Pós-Graduação em

Computação Aplicada

Mestrado/Doutorado Acadêmico

Mateus Schmitz da Silveira

UNIVCHAIN: Um modelo para autenticação de documentos acadêmicos baseado em blockchain

São Leopoldo,
2020

Mateus Schmitz da Silveira

UNIVCHAIN: UM MODELO PARA AUTENTICAÇÃO DE DOCUMENTOS ACADÊMICOS BASEADO EM BLOCKCHAIN

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre pelo Programa de Pós-Graduação em Computação Aplicada da Universidade do Vale do Rio dos Sinos — UNISINOS

Orientador:
Prof. Dr. Rodolfo S. Antunes

Co-orientador:
Prof. Dr. Cristiano André da Costa

São Leopoldo
2020

S587u Silveira, Mateus Schmitz da.
UNIVCHAIN: um modelo para autenticação de documentos acadêmicos baseado em blockchain / Mateus Schmitz da Silveira. – 2020.
89 f. : il. color. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Computação Aplicada, São Leopoldo, 2020.
"Orientador: Prof. Dr. Rodolfo S. Antunes ; Co-orientador: Prof. Dr. Cristiano André da Costa."

1. Blockchains (Base de dados). 2. Documentos acadêmicos. 3. Assinaturas digitais. 4. Validação de documentos. I. Título.

CDU 004.65

Dados Internacionais de Catalogação na Publicação (CIP)
(Bibliotecária: Bruna Sant'Anna – CRB 10/2360)

À minha mãe.

What do we live for, if not to make
life less difficult for each other?
— GEORGE ELIOT

AGRADECIMENTOS

Agradeço primeiramente à minha família, que sempre me apoiou e deu o suporte necessário para que este trabalho fosse finalizado.

Agradeço à minha mãe, que mesmo sem os anos de estudo que gostaria, nunca deixou de me apoiar nesta jornada acadêmica.

Agradeço à minha namorada, Letícia, que de forma brava resistiu às minhas variações de humor e minhas noites em claro, mas nunca deixou de me incentivar.

Agradeço imensamente ao meu orientador Prof. Dr. Rodolfo S. Antunes, que tanto contribuiu para a realização deste trabalho bem como para a manutenção do foco e do ânimo durante o caminho. Agradeço também ao meu co-orientador Prof. Dr. Cristiano André da Costa, que sempre trouxe excelentes colocações durante todo este processo.

Agradeço à empresa KingHost, que financiou este trabalho durante o primeiro ano inteiro.

Por último, mas não menos importante, agradeço aos meus colegas de pós-graduação, principalmente ao amigo Me. Júnior André Marostega.

RESUMO

Em meio ao constante avanço tecnológico, a validação de documentos acadêmicos segue sendo um desafio para universidades, alunos e o mercado de trabalho. Documentos comumente emitidos em papel possuem algumas desvantagens quanto a uma forma eficiente de verificação, armazenamento e livre distribuição a terceiros. A verificação destes documentos ocorre normalmente através de trabalho manual da entidade emissora e envolve custos. O papel é um material frágil e pode ser inutilizado em pouco tempo sob condições adversas. O uso destes documentos para comprovação acadêmica pode ser feito somente com envio de cópias físicas ou digitais, o que invalida grande parte dos recursos físicos de segurança aplicados no documento. Além disso, estes nem sempre possuem todas as informações relevantes do aluno e seu curso.

Este trabalho apresenta um modelo baseado em blockchain que permite a emissão e verificação de documentos acadêmicos sem a necessidade de intermediários ou recorrer a entidade emissora para atestar sua veracidade. O modelo proposto faz uso de blockchain pública que per- mite amplo acesso, aplicabilidade e redução de custos. O modelo de dados utilizado é baseado em um padrão aberto, facilitando adoção, extensão e melhorias. O uso de um modelo aberto beneficia também a internacionalização de diplomados brasileiros. O padrão de assinaturas digitais proposto pelo ICP-Brasil, e utilizado neste trabalho, torna os documentos emitidos pelo modelo, válidos legalmente no Brasil.

As características deste modelo o tornam único quando comparado aos modelos encontrados na literatura, provendo três verificações de segurança aos documentos emitidos. A Assinatura Digital é a primeira verificação, seguido pela verificação de *fingerprint* na blockchain e por último a checagem de revogação. A aplicação deste modelo pode ser feita concomitantemente com a emissão física já realizada hoje pelas entidades acadêmicas.

Os resultados foram coletados através da construção de um protótipo baseado no modelo proposto e pela realização de casos de uso baseados em um caso real. O protótipo demonstrou pouca variação nos tempos de emissão, onde 75% dos documentos emitidos levaram até 422 segundos. A maior variação percebido foi identificada no tempo de confirmação do bloco, etapa esta que levou três vezes mais tempo que as demais etapas somadas. Além disso, o protótipo demonstrou uma baixa demanda por recursos de memória.

Palavras-chave: Blockchain. Documentos acadêmicos. Assinatura Digital. Validação de documentos.

ABSTRACT

Amid constant technological advances, academic document validation remains a challenge for universities, students, and the labor market. Documents commonly issued on paper have some disadvantages in terms of an efficient way of checking, storing, and free distribution to third parties. Verification of these documents usually occurs through manual labor of the issuer and involves costs. The paper is a fragile material and can be useless in a short time under adverse conditions. The use of these documents for academic proof can only be done by sending physical or digital copies, which invalidates much of the security resources applied in the document. Also, these do not always have all the relevant information of the student and his course.

This work presents a model based on blockchain that allows the issued and the verification of academic documents without the need of intermediaries or to resort to the issuing entity to attest their veracity. The proposed model makes use of public blockchain that allows broad access, applicability, and cost reduction. The data model is based on an open standard, facilitating adoption, extension, and improvements. The use of an open model also benefits the internationalization of Brazilian graduates. The standard of digital signatures proposed by ICP-Brasil, and used in this work, makes the documents issued by the model, legally valid in Brazil.

The characteristics of this model make it unique when compared to the models found in the literature, providing three security checks on the documents issued. The Digital Signature is the first check, followed by the fingerprint verification at blockchain and lastly the revocation check. The application of this model can be made concomitantly with the physical emission already carried out today by the academic entities.

The results were collected through the construction of a prototype based on the proposed model and the realization of use cases based on a real case. The prototype showed little variation in the emission times, where 75% of the documents issued took up to 422 seconds. The most significant variation perceived was identified in the block's confirmation time, a step that took three times as long as the other steps added up. Besides, the prototype demonstrated a low demand for memory resources.

Keywords: Blockchain. Academic documents. Digital Signature. Document validation.

LISTA DE FIGURAS

LISTA DE ALGORITMOS

LISTA DE TABELAS

LISTA DE SIGLAS

JSON	JavaScript Object Notation
API	Application Programming Interface
XML	Extensible Markup Language
XSD	XML Schema Definition
IPFS	InterPlanetary File System
DAO	Data Access Object
FTP	File Transfer Protocol
PHP	PHP: Hypertext Preprocessor
MIT	Massachusetts Institute of Technology
REST	Representational State Transfer
UFRGS	Universidade Federal do Rio Grande do Sul
RAM	Random Access Memory
SHA2	Secure Hash Algorithm

SUMÁRIO

1 INTRODUÇÃO

Em um mundo em constante avanço tecnológico, ainda existem muitas dificuldades em autenticar documentos acadêmicos. Estas dificuldades vão desde os meios disponíveis para isso até a quantidade de trabalhos manuais necessários (SINGHAL; S. PAVITHR, 2015), inviabilizando ainda mais em caso de verificações de muitos documentos de uma só vez. Em um cenário onde o aluno deseja se candidatar a uma vaga de emprego, ou ingressar novamente em uma universidade, e precisa comprovar suas qualificações, é enviado ao possível empregador uma cópia destes documentos. Um papel impresso, assinado e a palavra do candidato é a única informação disponível para comprovação das competências necessárias. É possível realizar um trabalho de checagem de veracidade deste documento, porém, ele é feito através de uma solicitação à universidade que o emitiu. Este trabalho de verificação pode levar dias e possuir taxas associadas a ele. A adição de um processo manual, e a possível existência de taxas para verificação desta informação pode tornar a operação inviável.

A universidade ante a emissão de um diploma precisa realizar uma série de registros acadêmicos, que são compartilhados com a entidade responsável pela educação nacional, no caso do Brasil o MEC[1]. Além disso, sempre que uma solicitação de verificação de um documento é feita, um profissional precisa ser destacado para realizar a tarefa manualmente. Algumas instituições possuem serviços de verificação digitais, porém, eles normalmente se aplicam a documentos de uso único como comprovantes de matrícula e frequência.

O estudante certificado precisa realizar a guarda dos documentos de forma segura (HAN et al., 2018). A perda, o extravio ou a destruição destes documentos faz com que o aluno precise solicitar uma nova via à universidade. Este processo mais uma vez pode levar dias, envolve taxas e tempo para retirada do documento, que precisa de assinatura manual do estudante. Outro ponto crucial é o fato de o aluno possuir apenas este para efetivamente comprovar suas competências. Da mesma forma que a empresa empregadora possui apenas um documento como prova, o estudante possui apenas um documento disponível para apresentar. É ponto relevante o fato de a falsificação de documentos acadêmicos causar prejuízos na casa dos milhões de dólares (GARWE, 2015).

1.1 Motivação

Analisando o processo atual de emissão e verificação de diplomas percebe-se claramente que ele possui pontos que podem ser melhorados e otimizados com o emprego de um modelo mais eficiente, transparente, seguro e possivelmente com menor custo. Como objeto de estudo para este trabalho será considerada somente a emissão de documentos a nível de graduação.

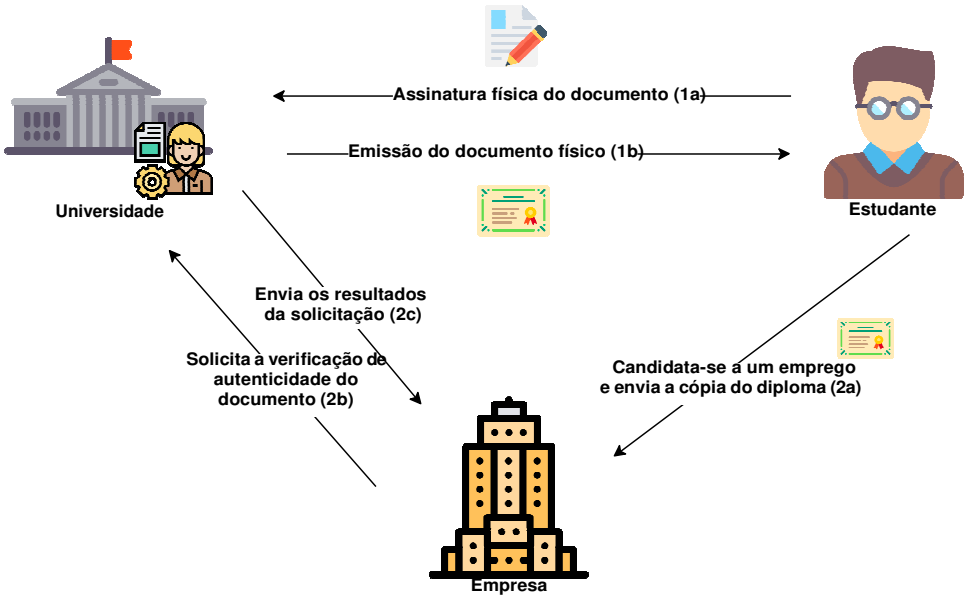
A Figura 1 mostra os processos envolvidos na emissão e verificação de um diploma. Ele está dividido basicamente em dois processos e em todos eles algum tipo de ação manual deve

[1]https://www.mec.gov.br/

ser empregada. Não são consideradas ações manuais, para este cenário, o envio de e-mails ou mensagens.

Os passos 1a e 1b ilustrados na Figura 1 são todos efetuados manualmente e com a necessidade de que o aluno se dirija até a universidade para retirar o documento, pois é necessária à sua assinatura. O processo 2a trata do envio de uma cópia do documento acadêmico, que pode ser uma cópia digital ou até mesmo uma cópia física entregue diretamente na empresa. As seções 2b e 2c também precisam de alguma ação manual, porém, sem a necessidade de deslocamento até a universidade. Este processo, no entanto, pode levar vários dias e ter taxas envolvidas.

Figura 1: Processo de emissão e verificação de um diploma



Fonte: Elaborado pelo Autor

1.1.1 Verificação de Autenticidade

Após ser diplomado um aluno recebe comumente uma via do seu diploma, um certificado de conclusão e o histórico do curso. A depender da entidade educacional, podem existir outros documentos entregues ao aluno no momento da diplomação, entretanto, para condução deste trabalho, apenas os citados serão considerados. Estes três documentos comprovam não só a diplomação como também todo o histórico curricular com notas, cargas horárias e aproveitamentos. O diploma é emitido em papel timbrado da universidade com assinaturas de todas as partes envolvidas, como mostrado nos processos 1a e 1b da Figura 1. Já o certificado de conclusão e o histórico são versões simples impressas em papel comum A4.

Estes documentos podem conter recursos adicionais de segurança (SINGHAL; S. PAVITHR, 2015), que são conhecidos normalmente somente pela entidade que o emitiu. Para que a autenticidade do documento possa ser verificada é necessário que a universidade e forneça

Os dados constantes no diploma. Este processo pode levar vários dias a depender da universidade emissora e da demanda pelo serviço (2b e 2c). Além disso, este tipo de consulta pode demandar o pagamento de taxas.

1.1.2 Emissão de novas vias do documento

Sabendo que o diplomado recebe somente uma via de cada um dos documentos citados na seção anterior, caso algum destes seja perdido, é necessária a solicitação de um novo documento. O processo de solicitação exige o contato com a universidade por um dos meios disponibilizados pela mesma. O processo pode levar vários dias e exigir o pagamento de taxas para a emissão da segunda via. Ao final o diplomado precisa se deslocar à universidade e retirar o documento, uma vez que é necessário que o mesmo assine o documento. O processo para solicitação de uma nova via do documento é o mesmo demonstrado nos processos (1a e 1b).

Analisando do ponto de vista da universidade, é necessário realizar a busca dos dados do aluno, inclusive em seus livros de registros acadêmicos e realizar a nova emissão do diploma (GRECH; CAMILLERI, 2017). Esta nova emissão precisa novamente de todas as assinaturas das pessoas responsáveis, inclusive do aluno. Este processo demanda que pelo menos 1 pessoa seja deslocada para realização deste trabalho.

1.1.3 Custo de emissão

Os processos de emissão, seja primeira ou segunda via, e verificação de autenticidade envolvem a necessidade de trabalho manual. O trabalho manual não se resume somente ao realizado pela universidade, mas também aquele realizado pelo diplomado e a terceiros que precisam verificar a autenticidade de um documento acadêmico. Os processos 1a, 1b, 2b e 2c mostrados na Figura 1 são aqueles onde algum trabalho manual se faz necessário.

A universidade normalmente não cobra taxas para a primeira emissão de um diploma, porém, cobra taxas para a verificação de autenticidade e emissão de segundas-vias. A cobrança destas taxas não significa, porém, que o processo seja lucrativo para a universidade.

1.2 Questão de Pesquisa

Com a popularização de criptomoedas, o cerne do seu funcionamento tem sido alvo de estudo: a blockchain. Sua característica descentralizada, imutável e criptografada tem sido testada nos mais diversos contextos (ZHANG; XUE; LIU, 2019; LI et al., 2017). Este trabalho se propõe a responder a seguinte questão de pesquisa: *Como blockchain pode ser aplicado na construção de um modelo de emissão, verificação e revogação de documentos acadêmicos de forma a reduzir as etapas manuais do processo, garantindo a integridade dos documentos emitidos?*

Para responder a esta pergunta, este trabalho propõe um modelo baseado em blockchain que prevê emissão, verificação e revogação de documentos. A partir desta proposta de modelo será implementado um protótipo a fim de realizar os testes necessários para validar os objetivos apontados. Os dados coletados servirão como base estatística para análise da performance e viabilidade técnica do modelo.

1.3 Objetivos

Os objetivos deste trabalho são divididos em duas partes. Objetivo principal, que é o objetivo do trabalho, e objetivos secundários que são os objetivos do modelo. O principal objetivo é desenvolver um modelo para emissão, verificação e revogação de documentos acadêmicos, utilizando processos independentes através de uma plataforma baseada em blockchain. Com processos independentes, o modelo visa permitir que cada uma das etapas possa ser executada sem a necessidade de contato com os outros atores mapeados no Capítulo 4. O trabalho também analisa a viabilidade do modelo proposto através de experimentos realizados com uma prova de conceito.

Além do objetivo principal, são definidos também os objetivos secundários, que são os objetivos do modelo proposto e implementado por este trabalho. O modelo proposto tem seu projeto baseado nas seguintes metas:

- Avaliação de documentos sem a necessidade de uma entidade terceira, garantindo amplo acesso à validação de veracidade;
- Prover plenos direitos ao aluno sobre os arquivos acadêmicos emitidos, permitindo sua livre distribuição e armazenamento;
- Prover validação utilizando Assinatura Digital com padrão reconhecido;

Este trabalho, ao explorar as lacunas existentes nos trabalhos já existentes, apresenta um método seguro composto por três fatores de verificação. Através destes fatores, é possível garantir a veracidade dos documentos emitidos, bem como o seu livre armazenamento. A independência dos métodos de verificação, que podem ser realizados de forma individual, traz celeridade ao processo de análise dos documentos. O método de revogação implementado pelo modelo UnivChain permite que qualquer documento emitido por este seja revogado, disponibilizando inclusive os motivos de revogação.

O modelo UnivChain, por ser basear em tecnologias amplamente utilizadas, abertas e já validadas, provê documentos que facilitam a integração internacional, permitindo que um documento possa ser validado por qualquer entidade acadêmica do mundo. Esta contribuição abre importante margem para integração entre unidades educacionais distribuídas geograficamente.

1.4 Organização do Trabalho

No capítulo2 são apresentadas as fundamentações para realização do trabalho, mostrando conceitos importantes para o prosseguimento da pesquisa e prova do modelo. O capítulo 3 detalha os trabalhos relacionados com este trabalho, descrevendo cada um deles e os comparando com o modelo proposto.

O modelo proposto e que será construído encontra-se detalhado na Capítulo 4, onde são mostrados os atores, artefatos, processos e plataformas utilizadas na proposição. O Capítulo 5 mostra o design e a implementação do protótipo detalhado no capítulo anterior a ele. Ainda no Capítulo 5 é detalhada a metodologia utilizada na avaliação do modelo proposto.

O Capítulo 6 é reservado para a exibição dos resultados obtidos pela execução dos cenários de teste no protótipo criado. Por fim, o Capítulo 7 apresenta as considerações finais, com perspectivas de trabalhos futuros e conclusão

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo visa esclarecer e situar os principais pontos que fundamentam o desenvolvimento deste trabalho. O ponto principal é a definição do que de fato é a tecnologia Blockchain e como ela é utilizada, seguido das definições de suas variações, como Blockchain Pública e Permissionada. Em seguida é apresentada a Assinatura Digital e seu funcionamento, bem como uma explicação de Criptografia Assimétrica, base para uso de Assinaturas Digitais. Por fim são conceituados os formatos de assinatura disponibilizados pela ICP-Brasil[1].

2.1 Blockchain

A tradução literal para *blockchain* é "Cadeia de Blocos". Este termo é utilizado para definir uma estrutura que representa uma lista encadeada de blocos de dados (ZHENG et al., 2018). Cada bloco possui suas próprias informações que podem ser desde transações financeiras a armazenamento de documentos. Além disso, cada bloco possui ainda um *hash* criptográfico que é a representação dos dados do bloco anterior (ANDROULAKI et al., 2018). Por este motivo o nome da estrutura é relacionado a uma cadeia de blocos, ou uma corrente de blocos. Este processo é repetido sempre que um novo bloco é adicionado à cadeia.

Para a geração do *hash* criptográfico, são utilizadas as informações que constituem o bloco (ZHENG et al., 2018). Como esta operação criptográfica é determinística, sempre que ela for executada com as mesmas informações resultará em uma mesma saída. Esta característica torna impossível a alteração dos dados de um bloco sem que seja necessário o recálculo de todos os blocos subsequentes, devido a mudança do hash identificador do bloco fraudado (NAKAMOTO, 2009). Isso significa que quanto mais antigo o bloco, mais complexo e maior poder computacional é necessário para uma eventual fraude. Estas características dão parte da segurança necessária para o funcionamento desta estrutura.

A estrutura da blockchain não prevê deleção ou alteração de dados de blocos já adicionados à cadeia (ANDROULAKI et al., 2018). Esta característica imutável, aliada à segurança provida pela forma como os dados são ligados e verificados torna a blockchain um objeto de estudo interessante e também um dos maiores avanços em se tratando de estruturas de dados distribuídas e transparentes (IANSITI; LAKHANI, 2017). Existem pelo menos dois tipos de blockchain: públicas e privadas (YANG et al., 2020).

2.1.1 Blockchain Pública

A Blockchain Pública permite que qualquer pessoa possa se ligar à rede, fazer transações e adicionar blocos à cadeia, respeitando os processos de prova de cada uma delas (M. BACH; MIHALJEVIC; ZAGAR, 2018). Estas plataformas não possuem restrição quanto a quem pode

[1] https://www.iti.gov.br/icp-brasil

adicionar informações nem quanto a quais dados dos blocos podem ser visualizados. Tudo nestas plataformas é de conhecimento público e pode ser auditado. As plataformas públicas mais utilizadas atualmente são as redes do Bitcoin e do Ethereum.

2.1.2 Blockchain Permissionada

Em se tratando de blockchain Permissionada, elas são ecossistemas fechados e comumente atribuídos a consórcios (E. PECK, 2017). Estas estruturas possuem regras bem definidas e mais rígidas quanto a quem tem permissão para adicionar novos blocos a cadeia como quem tem permissão de ler e quais dados possui permissão de ler. Este tipo de plataforma de forma geral implementa uma estrutura de Autenticação e Autorização (ANDROULAKI et al., 2018) para acesso e uso. Este tipo de estrutura acaba permitindo um modelo híbrido, onde parte dos dados está disponível de forma pública, porém, a gravação de novos dados na cadeia e outras informações confidenciais somente são acessadas pelos atores permitidos.

2.1.3 Versões de blockchain do Bitcoin

Ao longo do tempo a plataforma Bitcoin sofreu com diversos *forks*, alguns para a criação de outras criptomoedas, outros para criar versões alternativas à rede principal, chamada de mainnet. Para desenvolvimento de soluções e testes sobre a blockchain do Bitcoin, ela possui versões testnet (RESHEF KERA, 2020) e regtest. A rede regtest é uma rede utilizada para ambientes de desenvolvimento, onde não existe necessidade de simulação do processo de mineração dos blocos. Já a rede testnet é conhecida por ser uma rede paralela à rede principal, possuindo carteiras e bitcoins sendo transacionados por ela. É importante salientar que as carteiras e bitcoins não possuem valor efetivo fora da rede testnet. Atualmente a rede de teste encontra-se em sua versão 3.

2.2 Transações não financeiras na Blockchain

O protocolo utilizado pelo Bitcoin fornece uma instrução especial, utilizada para armazenamento de metadados, chamada OP_RETURN (BARTOLETTI; POMPIANU, 2017). Estas instruções são comumente utilizadas para armazenamento de informações para posterior verificação, uma vez que estes dados possuem característica imutável. O uso desta instrução é possível em qualquer transação realizada na blockchain, inclusive naquelas realizadas para si próprio. Isso permite que para armazenar permanentemente uma informação na blockchain do Bitcoin, seja necessário apenas a criação de uma transação que envie algum valor para a mesma carteira emissora e utilize a instrução citada.

2.3 Assinatura Digital

A Assinatura Digital possui a mesma função que a assinatura física de determinada pessoa, só que utilizada no ambiente digital. Ao assinar digitalmente um documento é possível atestar por meio de processo criptográfico, que aquela assinatura é de fato de quem diz ser. Com isso, é definido que uma assinatura digital é capaz de fornecer autenticidade (REN; YANG; ZHENG, 2018).

No momento em que um documento é assinado digitalmente é realizado um processo criptográfico com base nas informações que constam naquele documento. Esta assinatura não pode ser movida para outro documento nem o documento pode sofrer modificações, pois isso invalida a assinatura digital (POOJA; YADAV, 2018). Neste caso, é possível afirmar que a Assinatura Digital provê integridade ao documento assinado.

2.3.1 Criptografia Assimétrica

Criptografia Assimétrica é a base para funcionamento de uma Assinatura Digital (POOJA; YADAV, 2018). Ela consiste na existência de duas chaves distintas, uma pública e uma privada. A chave privada é a chave que deve ser guardada e jamais divulgada. Já a chave pública deve ser distribuída de forma que qualquer pessoa tenha acesso a ela. Estes dois pontos são importantes para a compreensão das funções das chaves. Ao assinar digitalmente um documento, usa-se a chave privada, aquela que não pode ser divulgada a terceiros. Ao enviar este documento assinado a um terceiro, o mesmo pode ser verificado utilizando as informações da assinatura do documento e a chave pública de quem assinou (WARASART; KUACHAROEN, 2019).

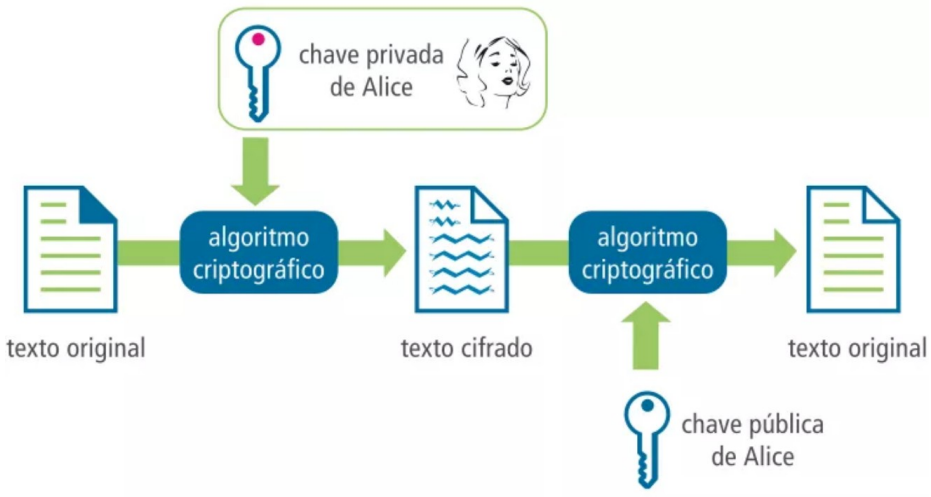
No processo descrito acima e detalhado na Figura 2, é fundamental que a chave pública seja amplamente divulgada ou que esteja em local público de fácil acesso. Existem repositórios de chaves públicas que suprem justamente esta necessidade, mantém estas chaves acessíveis a todos.

2.3.2 Padrão ICP-Brasil

No Brasil existe uma entidade responsável pelo gerenciamento de chaves públicas e certificados digitais. Certificados Digitais não serão abordados por estarem fora do escopo do trabalho, mas de forma básica são os responsáveis por ligar um determinado ente ao par de chaves criptográficas citado anteriormente. A entidade responsável é a ICP-Brasil e é de sua competência, entre outras coisas, a definição de padrões de assinaturas digitais. Para que um documento assinado digitalmente tenha validade legal no Brasil, é necessário que a assinatura tenha sido feita seguindo um dos padrões definidos pela ICP-Brasil.

- Assinatura digital com Referência Básica (AD-RB): é a assinatura simples, que é formada pelo identificador da assinatura digital padrão ICP-Brasil.

Figura 2: Processo de assinatura com chave privada



Fonte: http://aprendis.gim.med.up.pt/index.php/Certificação_Digital_do_Médico_no_Brasil

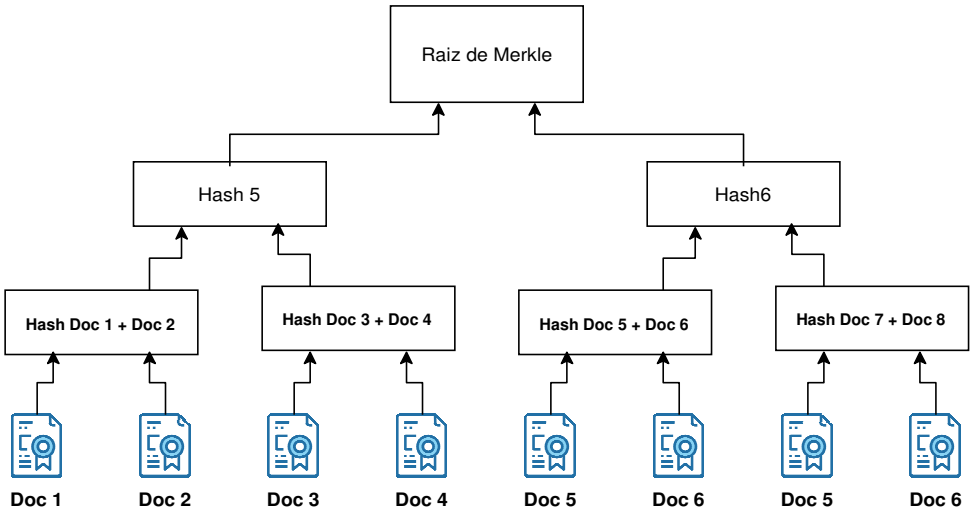
- Assinatura digital com Referência de Tempo (AD-RT): é constituída da Assinatura AD-RB acrescida ou logicamente conectada a um carimbo do tempo emitido por uma Autoridade de Carimbo do Tempo (ACT) credenciada na ICP-Brasil.
- Assinatura digital com Referências para Validação (AD-RV): é formada de uma assinatura com Referência de Tempo (AD-RT) na qual foram acrescentadas referências sobre todos os certificados de chave pública e sobre todas as Listas de Certificados Revogados (LCR) ou respostas de Online Certificate Status Protocol (OCSP) que são necessários para a validação daquela assinatura. Sobre esses dados é acrescentado ou logicamente conectado outro carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil.
- Assinatura digital com Referências Completas (AD-RC): é constituída por uma assinatura digital com referências para Validação (AD-RV) a qual foram acrescentados todos os dados necessários para validação da assinatura.
- Assinatura digital com Referências para Arquivamento (AD-RA): uma assinatura com referência de Tempo (AD-RT) com a adição de todos os dados necessários para validação da assinatura. Além disso, é adicionado um carimbo de tempo sobre todo este conjunto de dados.

2.4 Árvore de Merkle

Árvore de Merkle é uma das formas mais conhecidas para verificação de integridade de dados (MERKLE, 1988). O grande destaque deste método é a possibilidade de verificação de qualquer um dos documentos que compõem a árvore sem a necessidade de conhecimento de todos os documentos originais. De forma resumida, é possível atestar que um documento está

presente na árvore apenas conhecendo alguns poucos elementos. A Figura 3 mostra o processo de cálculo de todos os nós da árvore de Merkle, até que reste somente um, chamado de raiz de Merkle. No exemplo mostrado na figura, para determinar se o Doc 5 pertence à essa raiz, basta que sejam conhecidos o hash do Doc 6, o Hash Doc 7 + Doc 8 e o Hash 5. Esta estrutura de verificação vem sendo aplicada em inúmeras plataformas de blockchain (Swan, 2015) (Liang et al., 2017), inclusive o Bitcoin (NAKAMOTO, 2009).

Figura 3: Processo de cálculo da Raiz de Merkle



Fonte: Elaborado pelo Autor

2.5 JSON-LD

JSON é um formato muito utilizado para serialização de dados e intercomunicação entre sistemas, sendo comumente um substituto para o formato XML. A especificação JSON-LD é construída sob o formato JSON e tem o intuito de permitir a serialização de dados conectados (KELLOGG; CHAMPIN; LONGLEY, 2019). A sintaxe foi desenvolvida para facilitar a integração entre sistemas que já utilizam o formato JSON e necessitam de maior controle sobre os tipos de informações trafegadas.

Para fins de comparação, o JSON-LD possui a mesma função executada pelos arquivos XSD em se tratando de XML. Por meio desta especificação é possível garantir que o documento possui os campos necessários e em formato válido, conforme o padrão definido. Além disso, todos os tipos podem ser estendidos e modificados para atender as mais diversas demandas, tornando todas as definições reaproveitáveis.

2.6 Considerações Parciais

Os temos abordados neste capítulo são todos de suma importância para o desenvolvimento deste trabalho. Árvore de Merkle é uma forma segura de realizar verificação de informações (YU et al., 2020) e um dos pilares no qual a blockchain do Bitcoin se apoia. Como destacado, é utilizado como uma forma de verificar a existência de uma transação dentro de um determinado lote de transações. Como forma adicional de segurança, é abordado aqui o modelo de certificação digital, que é utilizado como garantia de integridade de documentos distribuídos digitalmente. Documentos estes que utilizam um modelo de dados flexível e adotado nos mais diversos casos de uso devido a sua flexibilidade e legibilidade, o JSON. Como forma de se beneficiar das vantagens do uso de documentos JSON e garantir um padrão de documentos, é utilizado o padrão JSON-LD (SPORNY; KELLOGG; LANTHALER, 2014). Por fim, existem transações não-financeiras na blockchain do Bitcoin, que permite a realização de uma transação sem a necessidade de envio de bitcoins a um terceiro. Estas transações são comumente utilizadas para armazenamento de dados na cadeia.

3 TRABALHOS RELACIONADOS

Este capítulo apresenta os trabalhos que possuem alguma similaridade com o trabalho aqui proposto, por envolverem blockchain aplicada à validação de documentos acadêmicos. A pesquisa e seleção dos trabalhos mais pertinentes foram feitos utilizando as ferramentas Google Acadêmico[1] e IEEE Explorer[2]. Foram considerados somente trabalhos publicados a partir de 2018, ano em que se iniciam trabalhos mais relevantes á área de pesquisa. Para filtragem dos resultados foram utilizados os termos: *blockchain*, *blockchain-based*, *blockchain academic*, *blockchain scholar*. Os termos foram pesquisados tanto em língua inglesa como em português. Os termos foram pesquisados utilizando as seguintes *strings* de consulta:

- ’blockchain’ OR ’blockchain-based’ OR ’blockchain academic’ OR ’blockchain scholar’
- ’blockchain’ OR ’baseado em blockchain’ OR ’blockchain acadêmico’ OR ’blockchain escolar’

O objetivo principal deste capítulo é analisar os trabalhos relacionados à pesquisa atual e os comparar quanto aos aspectos utilizados no modelo apresentado.

3.1 A Graduation Certificate Verification Model via Utilization of the Blockchain Technology

O modelo teórico apresentado por GHAZALI; SALEH (2018) propõe uma possível solução para verificação e emissão de diplomas e certificados acadêmicos. O trabalho utiliza como motivação problemas enfrentados na emissão de certificados como a falsificação destes que são oriundos de 5 fontes diferentes: venda de diplomas, falsificação de diplomas, documentos modificados, documentos emitidos por funcionários corruptos e documentos traduzidos (GARWE, 2015). São citados ainda limitações do modelo atual de diplomação tais como: propriedade, disponibilidade, dependência de entidades terceiras, consumo de tempo e o custo.

A pesquisa de GHAZALI; SALEH (2018) divide o modelo proposto em dois processos: a emissão do certificado e a verificação do mesmo. A visão geral do modelo por ser verificada na Figura 4.

3.1.1 A emissão do certificado

A emissão do certificado consiste primeiramente da assinatura digital do documento virtual gerado pela instituição de ensino. Esta assinatura digital segue o padrão de chaves assimétricas, pública e privada, além do *hash* criptográfico SHA256 (DANG, 2015) e o *timestamp* (DATA ELEMENTS AND INTERCHANGE FORMATS — INFORMATION INTERCHANGE —

[1] https://scholar.google.com.br
[2] https://ieeexplore.ieee.org/Xplore/home.jsp

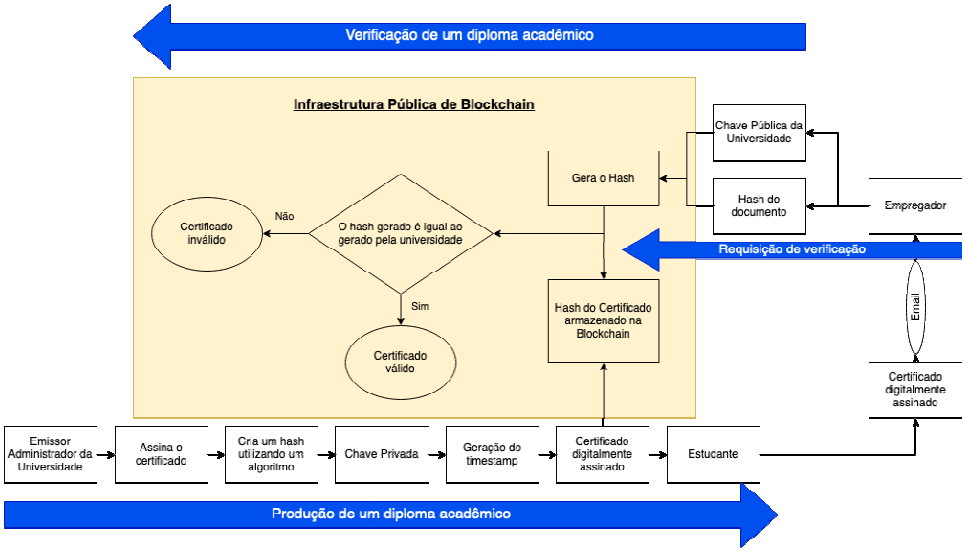
REPRESENTATION OF DATES AND TIMES, 2004), usado como carimbo do tempo para indicar o preciso momento de emissão do documento. Além disso o modelo prevê a assinatura com a chave pública do estudante certificado, garantindo que somente o mesmo, em posse de sua chave privada, possa descriptografar o documento. Concluídas as assinaturas, o modelo prevê a geração de um novo *hash* do documento já assinado e este sim é gravado na blockchain.

3.1.2 Verificação do certificado

Para verificação do diploma emitido conforme a seção anterior, é necessário possuir a chave pública da instituição emissora e o documento assinado digitalmente. Com estes dados um software de verificação é usado para verificação da assinatura digital.

O modelo apresentado consegue de fato prover uma proposta de validação via blockchain, apesar de não deixar explícito o real ganho da sua utilização no modelo. O mecanismo de validação apresentado funciona e atende ao proposto, porém, nenhuma informação armazenada na blockchain é utilizada, tornando assim a sua utilização questionável. Os trabalhos futuros relacionados a este modelo incluem a sua implementação, sua adoção e extensão para uso de *smart contracts* (E. PECK, 2017).

Figura 4: Modelo proposto por GHAZALI; SALEH (2018)



Fonte: Adaptado de (GHAZALI; SALEH, 2018)

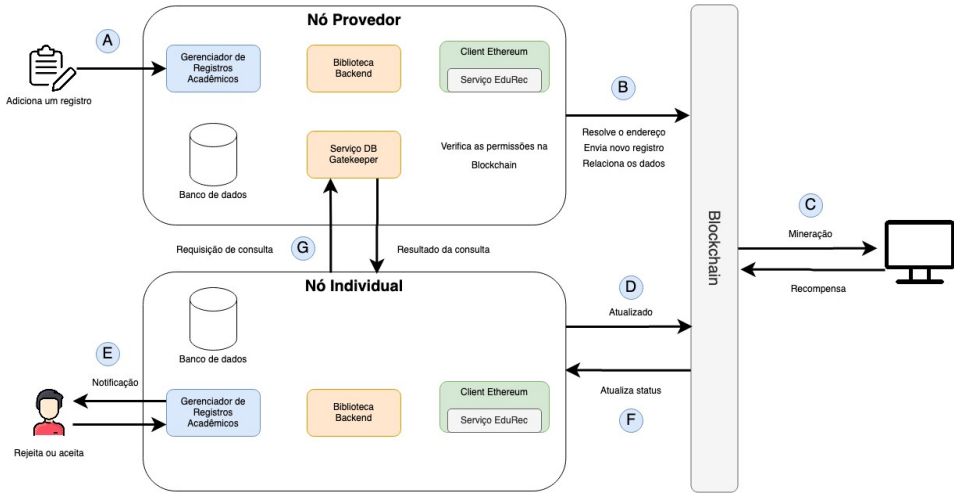
3.2 A Novel Blockchain-based Education Records Verification Solution

A proposta de HAN et al. (2018) propõe uma nova técnica baseada em blockchain para prover um ambiente onde os indivíduos sejam donos de seus respectivos registros acadêmicos oficiais e consigam compartilhar estes registros livremente com terceiros. Considerando que

educação não é apenas um período de experiência e sim um projeto de vida, o modelo apresentado visa prover funções que permitam o utilizar para demais experiências e aprendizados.

A arquitetura proposta transforma tanto as entidades emissoras quanto os alunos e demais interessados em validar documentos acadêmicos, em nós da plataforma, chamados de nós individuais. Além disso, o nó minerador[3] segue existindo e executando o mesmo trabalho feito em outras plataformas blockchain, que é o de validar e adicionar novos blocos à cadeia. Todas as informações e documentos acadêmicos são primeiramente gravados em um banco de dados do próprio nó e somente então, por meio de *smart contracts* os dados são gravados na blockchain. Para que um nó individual possa verificar estas informações é necessário que este nó estabeleça uma relação com o nó provedor e a partir de então será permitido a ele consultar as informações e documentos. A visão geral do modelo pode ser visualizada na Figura 5.

Figura 5: Arquitetura do modelo proposto por HAN et al. (2018)



Fonte: Adaptado de (HAN et al., 2018)

3.3 Blockchain for Education

Para desenvolvimento do trabalho foram consideradas três tarefas principais: as identidades das autoridades de certificação devem ser criadas e mantidas, as autoridades devem emitir certificados para os alunos e a terceira tarefa é o processo de verificação do certificado. Baseado nestas tarefas, o modelo proposto por GRäTHER et al. (2018) suporta entidades certificadoras, os alunos e empregadores.

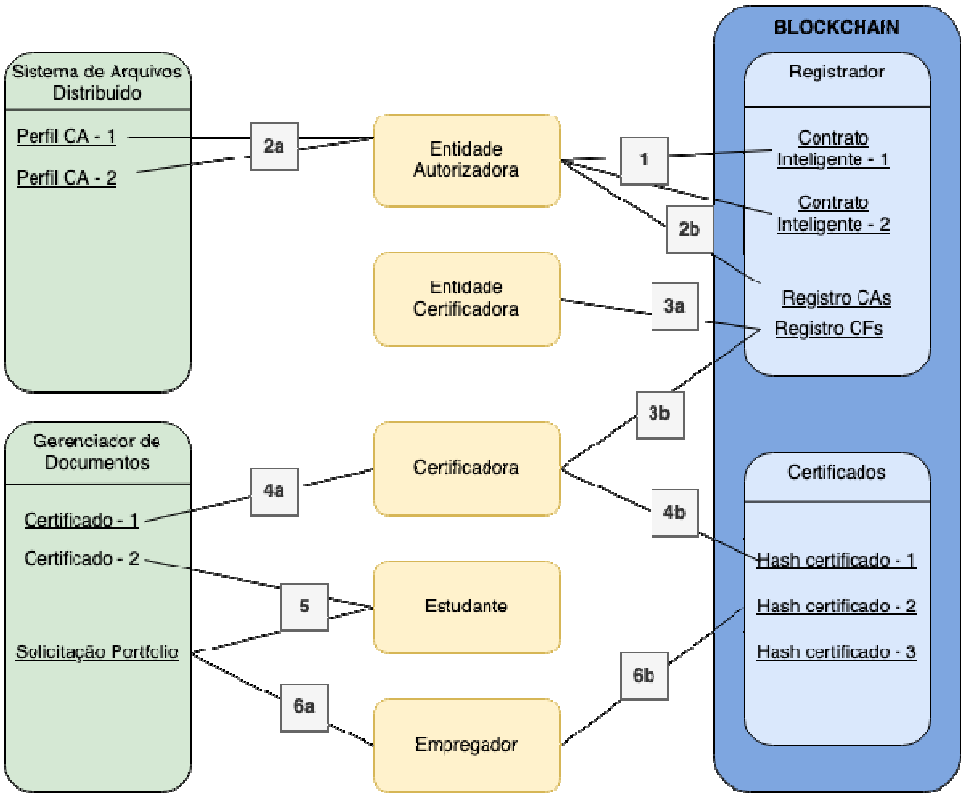
A Figura 6 mostra uma visão geral e conceitual do modelo proposto. A proposta segue um modelo hierárquico onde uma Autoridade de Acreditação é a responsável por criar e manter os *smart contracts* necessários para funcionamento da rede. Esta mesma autoridade é a responsável por cadastrar e autorizar as Entidades Autorizadoras, por meio da entidade pública cadastrada na blockchain. Por sua vez, as entidades autorizadoras podem realizar o cadastramento dos

[3]https://bitcoin.org/en/vocabulary#mining

Certificadores. Estes Certificadores por sua vez são os responsáveis pela emissão dos diplomas em si.

O modelo ainda destaca o uso de um sistema de arquivos distribuído IPFS[4], onde são armazenados os perfis das entidades autorizadoras e um sistema de gerenciamento de documentos. Este sistema de gerenciamento de documentos é utilizado para armazenamento dos certificados e portfólio de alunos. Além disso, este sistema é o único componente centralizado do modelo.

Figura 6: Arquitetura conceitual proposta por GRäTHER et al. (2018)



Fonte: Adaptado de (GRäTHER et al., 2018)

3.4 CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials

A proposta de ARENAS; FERNANDEZ (2018) busca aplicar um modelo de blockchain permissionada à verificação descentralizada de documentos educacionais. O trabalho, chamado de CredenceLedger, propõe um modelo baseado em blockchain que armazena provas de veracidade de documentos acadêmicos e que podem ser facilmente verificados.

O uso de uma blockchain permissionada permite que somente algumas informações do documento possam ser exibidas em uma consulta, porém, a plataforma é capaz de armazenar todas as informações. Isso tudo pode ser configurado através de metadados no momento em

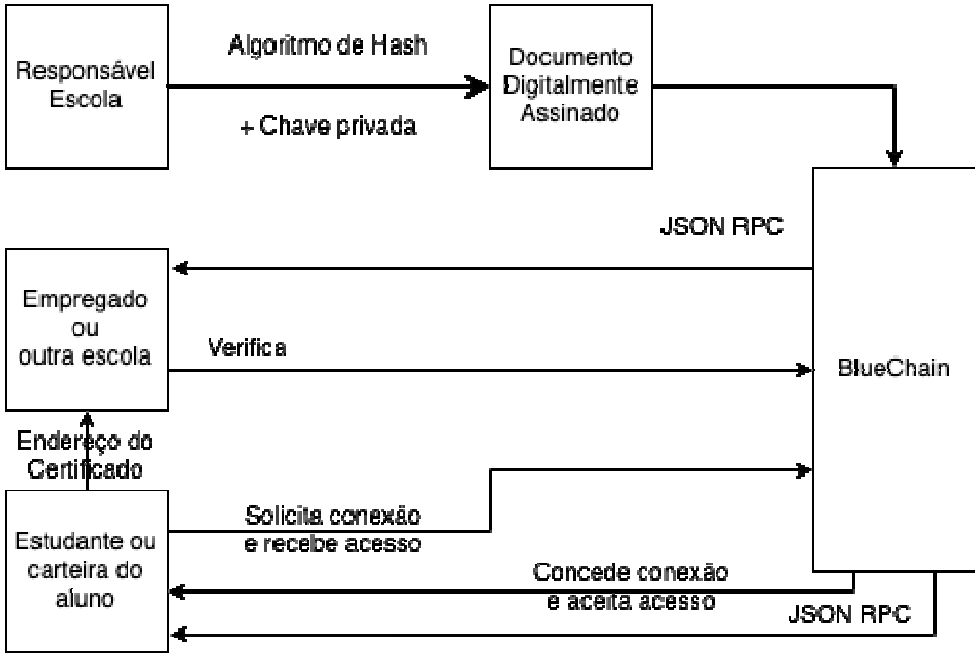
que uma

[4]https://ipfs.io/

informação é salva. A plataforma proposta define que para acesso das informações de determinado certificado, uma solicitação é feita para o dono dos dados. Através de um aplicativo desenvolvido, o dono dos dados pode aprovar o acesso às informações. Em posse destas informações é possível efetuar a validação da veracidade do documento digital. Uma das vantagens citadas pelo CredenceLedger é o não uso de criptomoedas para gravação das informações.

A proposta de ARENAS; FERNANDEZ (2018), que tem sua arquitetura exibida na Figura 7, é capaz de prover versões digitais de documentos acadêmicos facilmente verificáveis, sem a necessidade de uso de uma blockchain pública e o uso de criptomoedas. Uma blockchain permissionada também é escalável a ponto de permitir um banco de dados distribuído no qual diversas entidades podem utilizá-la sem a necessidade de um sistema centralizado. Como último ponto é destacado que uma plataforma permissionada é um eficiente sistema para gerenciar certificados devido a: alta capacidade de processar transações e baixo consumo de recursos.

Figura 7: Arquitetura do CredenceLedger proposto por ARENAS; FERNANDEZ (2018)



Fonte: Adaptado de (ARENAS; FERNANDEZ, 2018)

3.5 The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling

A proposta de GRESCH et al. (2019), parte do levantamento de requisitos feito com os *stakeholders* (M. JONES; WICKS; FREEMAN, 2017) do projeto na University of Zurich (UZH). O projeto toma como base entrevistas feitas com as partes interessadas, e os requisitos levanta- dos nestas entrevistas, para a definição do modelo. Os requisitos considerados podem ser vistos na Tabela 1.

O modelo, detalhado na Figura 8, pode ser dividido em 3 partes. A primeira cobre os re-

quisitos referentes a universidade emissora, assim como a segunda parte cobre os requisitos referentes ao destinatário do diploma, ou aluno. Por fim, a terceira parte do modelo cobre o processo de verificação de um diploma, a ser executada por companhias ou até mesmo universidades interessadas em comprovar a veracidade de um documento. Uma característica interessante da proposta é que ela funciona dentro do sistema de emissão já existente na universidade, tendo como entrada os diplomas em formato PDF.

Tabela 1: Requisitos levantados com stakeholders na UZH

Emissor
RQ1 - Apenas departamentos autorizados do UZH estão autorizados a emitir diplomas RQ2 - Os dados do diploma devem ser confidenciais aos seus destinatários RQ3 - O processo de emissão e verificação de diplomas deve abstrair as complexidades técnicas RQ4 - Vários diplomas devem ser processados em lote
Verificador
RQ5 - Os recursos de verificação devem ser acessíveis a qualquer empresa RQ6 - Diplomas devem ser verificados de forma autônoma
Destinatário
RQ7 - Os graduados devem receber seus diplomas em formato digital

Fonte: Adaptado de (GRESCH et al., 2019)

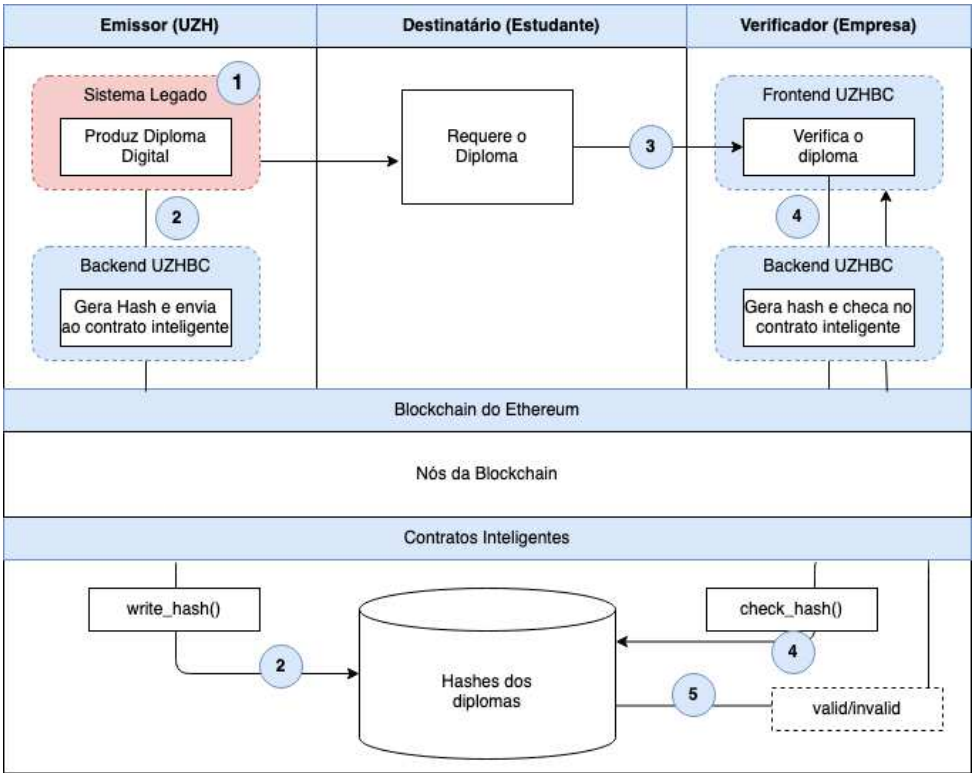
O diploma digital, em formato PDF, é utilizado para a geração de um *hash* criptográfico, que será enviado a um *smart contract* e consequentemente gravado definitivamente à blockchain do Ethereum. O aluno por sua vez recebe este documento PDF tal qual o gerado e utilizado para geração do *hash* e pode o distribuir para terceiros, como por exemplo uma empresa na qual esteja fazendo processo seletivo. A empresa em posse deste documento pode verificar a autenticidade do mesmo utilizando a aplicação web disponibilizada pela plataforma UZHBC. Com a implementação do modelo proposto, o UZHBC consegue com sucesso atender aos requisitos propostos. Trabalhos futuros envolvem aprovação do modelo por parte da diretoria da universidade, onde outros requisitos podem ser necessários.

3.6 Blockchain and Smart Contract for Digital Certificate

CHENG et al. (2018) apresenta um modelo distribuído baseado na blockchain do Ethereum, que possui como característica principal a implementação de Smart Contracts. O modelo apresentado define 4 grupos de usuários, sendo eles: as escolas ou unidades de certificação, os estudantes ou companhias, os provedores de serviço e a plataforma Ethereum.

Todos os processos como o registro do estudante, a emissão do diploma e a verificação do mesmo é realizada através do modelo apresentado. Algumas das imagens presentes no artigo exibem uma verificação de revogação do documento, porém, isso não é detalhado no texto e, portanto, para fins de comparação, será considerada inexistente. O processo de certificação pode ser visto na Figura 9. Ele consiste nos seguintes passos:

Figura 8: Arquitetura proposta por GRESCH et al. (2019) para UZHBC



Fonte: (GRESCH et al., 2019)

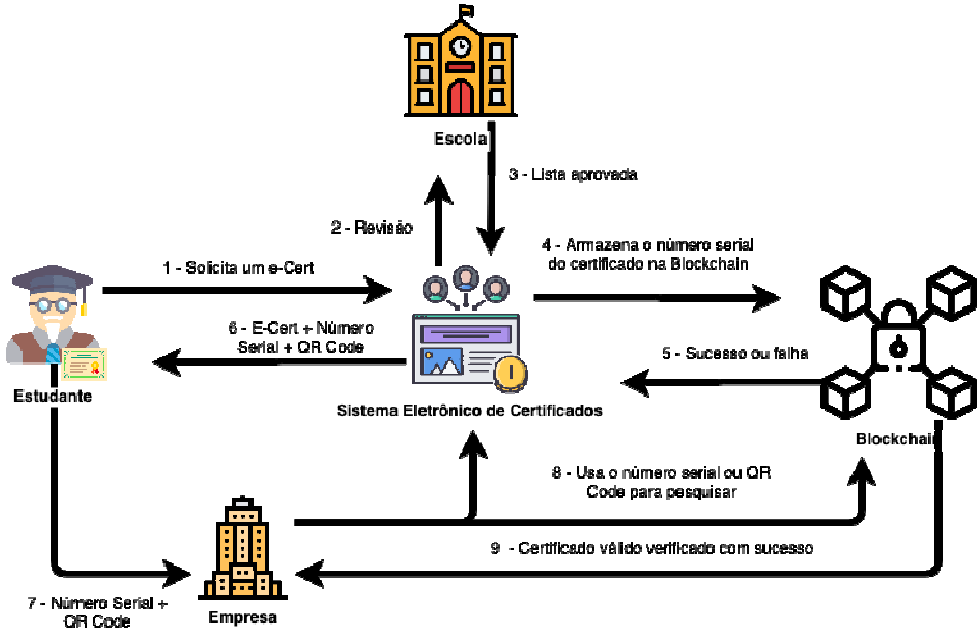
- Escola e/ou universidade emite o diploma e insere os documentos no sistema, que é gravado na Blockchain.
- O sistema realiza todas as validações necessária e envia ao estudante os documentos digitais e um QR Code para verificação do documento.
- Quando se candidatar a uma vaga de emprego o estudante pode enviar o QR Code ou o serial do documento ao empregador
- A empresa, em posse do serial ou do QR Code, pode consultar o documento através da plataforma proposta

3.7 Issuing and Verifying Digital Certificates with Blockchain

O modelo apresentado por (HUYNH et al., 2018) é chamado Unicert e baseado no Unicoin, uma criptomoeda desenvolvida sobre a tecnologia blockchain. O modelo apresentado pode inclusive ser estendido para atender outros nichos de mercado como o da música, patentes e direitos autorais. A rede Unicoin utilizada se assemelha muito com a rede Bitcoin, inclusive utilizando o mesmo tipo de algoritmo de consenso, o *Proof of Work*.

As interações com a plataforma acontecem através de uma aplicação chamada Unicert App, que permite a emissão e a verificação de documentos acadêmicos emitidos pelo sistema. Os

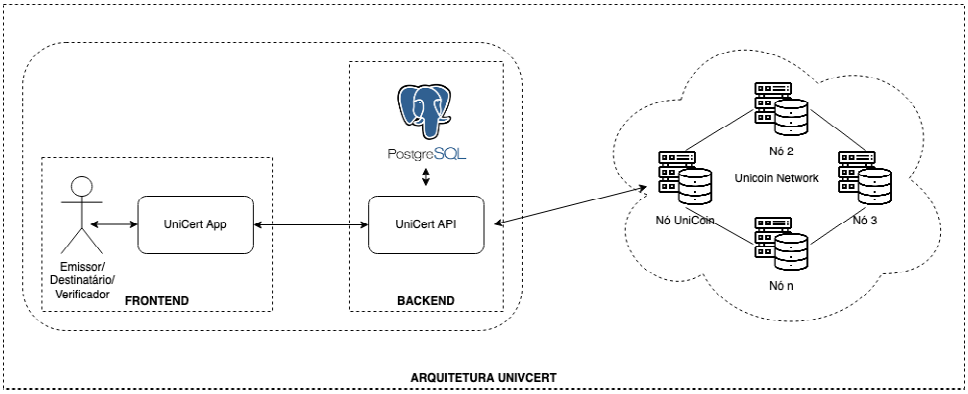
Figura 9: Arquitetura proposta por (CHENG et al., 2018)



Fonte: Adaptado de (CHENG et al., 2018)

diplomas emitidos são agrupados por meio da Raiz de Merkle, permitindo sua emissão em lote. É importante salientar que o modelo de (HUYNH et al., 2018) necessita utilizar criptomoedas para a realização das suas transações. Além disso, a chave pública do usuário, neste caso, é o endereço do estudante na rede Unicoin. A Figura 10 apresenta a arquitetura do modelo proposto.

Figura 10: Arquitetura proposta por (HUYNH et al., 2018)



Fonte: Adaptado de (HUYNH et al., 2018)

3.8 Comparação entre os Trabalhos Relacionados

Através dos dados extraídos da Tabela 2 os trabalhos relacionados foram comparados ao modelo proposto por todos os 6 espectros, que serão detalhados abaixo.

3.8.1 Adaptável a qualquer Blockchain

Este atributo visa determinar quais os modelos são atrelados a um tipo específico de plataforma blockchain, se públicas, privadas, permissionadas ou com uso de contratos inteligentes. A relevância deste atributo se deve ao fato de quanto mais amplo o universo de plataformas utilizáveis com o modelo, mais extensível e facilmente utilizável a plataforma pode ser.

Com exceção do modelo proposto por GHAZALI; SALEH (2018), os demais modelos analisados são dependentes de uma estrutura específica de blockchain. Isso torna o modelo mais suscetível a um possível abandono de uma plataforma em se tratando de suporte, atualizações e manutenibilidade. Os modelos propostos por HAN et al. (2018) e o modelo UZHBC possuem grande dependência da rede Ethereum, inclusive com o uso de contratos inteligentes da plataforma. Já o modelo Blockchain for Education possui dependência do uso de contratos inteligentes, porém, não está necessariamente dependente da rede Ethereum pois implementa seus contratos utilizando os padrões OpenZeppelin[5]. Em se tratando do modelo CredenceLedger de ARENAS; FERNANDEZ (2018), o mesmo é modelado sob a plataforma Multichain[6] e pro- põe uma rede permissionada, reduzindo as possibilidades de plataformas disponíveis para uso e tornando o modelo dependente destes requisitos.

3.8.2 Modelo de dados extensível

A comparação quanto ao modelo de dados utilizado tem relevância quando se avaliam as possibilidades de extensão, melhora e aproveitamento do modelo. Optou-se por avaliar os modelos quanto à suas características e uso de modelos *Open Source* já existentes. Neste ponto, a única plataforma a utilizar um modelo já existente e aberto é o trabalho Blockchain for Education. As demais plataformas utilizam modelos próprios ou não detalhados para geração e assinatura. O modelo UZHBC, no entanto, é o único a não utilizar uma versão digital do diploma modelada para a plataforma. A proposta trata do uso do mesmo documento PDF utilizado para impressão e entrega ao aluno.

3.8.3 Permissão do aluno para emissão

A análise dos modelos quanto à necessidade de permissão ou cadastro do aluno para que a entidade possa realizar a emissão de um diploma, visa avaliar os processos de emissão propostas versus o modelo de diplomação atual. Do ponto de vista prático, a entidade emissora hoje não tem necessidade de solicitar permissão ao aluno, o diploma é emitido e retirado pelo aluno em momento que lhe convir.

Os modelos propostos por HAN et al. (2018) e o modelo UZHBC não propõem aprovação

[5]https://openzeppelin.org/
[6]https://www.multichain.com/

do aluno para emissão de certificado. A proposta Blockchain for Education prevê cadastro do aluno em casos de gerenciamento de portfólios de diplomas dentro da plataforma. Se tratando do modelo de GHAZALI; SALEH (2018) é necessário que o aluno possua um par de chaves, pública e privada, para emissão e assinatura do seu certificado. No caso do modelo CredenceLedger é necessário que o aluno crie uma carteira virtual através do aplicativo do modelo e assim consiga acesso aos seus diplomas.

3.8.4 Emissão em lotes

A emissão em lotes é pertinente ao analisar o custo envolvido em armazenar uma informação na blockchain. As maiores plataformas públicas, são as utilizadas para transações de criptomoedas e consequentemente, armazenar uma informação nelas exige o pagamento de taxas. O processamento de lotes de diplomas é uma alternativa para a redução de custos na emissão, uma vez que permite a universidade gravar um lote de diplomas utilizando uma única transação e assim pagar taxas somente para esta. O limite de diplomas está ligado ao tamanho máximo permitido pelo bloco de cada plataforma.

O único modelo estudado e que possui recurso de emissão por lotes é a plataforma proposta por HAN et al. (2018). O modelo prevê a entidade Registro Educacional, que pode ser agrupado e salvo em um mesmo bloco de dados. As demais plataformas não possuem recursos explícitos de uso de processamento em lotes. Este recurso pode ser questionado em plataformas que não possuem dependência de criptomoedas, conforme destacado na seção 3.6.6.

3.8.5 Histórico completo do Diploma

Com o uso de versões digitais de diplomas, é possível que estes documentos sejam incrementados, disponibilizando também informações como as disciplinas cursadas, atividades práticas, seminários ministrados, atividades de extensão ou até mesmo diplomação parcial, caso de algumas universidades como a Unisinos. Tendo isso em vista, os modelos foram avaliados quanto a presença ou possibilidade de inclusão do histórico completo do curso.

O modelo Blockchain for Education não possui em sua estrutura, recursos ou informações para adição da histórico completo do curso em suas emissões. Os modelos de GHAZALI; SALEH (2018), CredenceLedger e UZHBC foram citados como potencialmente podendo atender a esta demanda, uma vez que seu modelo de dados não é especificado na proposta. O modelo UZHBC pode facilmente implementar isto devido ao seu modo de geração de *hashes* via PDF do diploma.

3.8.6 Uso de criptomoedas

A avaliação quanto ao uso de criptomoedas está intrinsecamente ligada ao citado na seção 3.6.4, quando abordada a emissão por lotes de certificados. O uso de criptomoedas torna a universidade mais suscetível a possíveis oscilações do mercado, podendo tornar a emissão muito cara caso o valor da criptomoeda suba muito.

Os modelos de GHAZALI; SALEH (2018), HAN et al. (2018), Blockchain for Education e UZHBC são modelos que possuem dependência do uso de criptomoedas. GHAZALI; SALEH (2018) não propõem um modelo de blockchain, mas usam uma plataforma pública o que acarretará em custos para transação. Os modelos HAN et al. (2018), Blockchain for Education e UZHBC, por utilizarem a plataforma Ethereum, também precisam de criptomoedas para sua operação. A plataforma CredenceLedger é a única a não depender de criptomoedas pois implementa sua própria plataforma por meio da MultiChain.

3.9 Oportunidade de contribuição

A proposta deste trabalho consegue atender cinco dos seis requisitos relacionados na Tabela 2, sendo a única exceção o uso de criptomoedas no processo. O modelo proposto é agnóstico de plataforma blockchain pois a utiliza apenas como forma de armazenamento dos *hashes* resultantes de seu processo criptográfico. Isso faz com que o modelo possa ser aplicado virtualmente a qualquer plataforma que possua este recurso, seja ela pública, privada, com ou sem contratos inteligentes. Pensando em um modelo que possa ser constantemente melhorado e estendido, o modelo de dados utilizado é Open Source. Visando a facilidade e menor modificação do pro- cesso atual de diplomação, o modelo proposto não exige que o aluno realize nenhum cadastro na plataforma nem que precise informar chave pública para sua identificação. A identificação do aluno será feita conforme o modelo atual, mediante nome, data de nascimento e Registro Geral.

A emissão do certificado por parte da universidade será sempre feita em lotes, o que ocasionará economia em sua emissão e permitirá melhor aproveitamento de dados em blocos. O documento emitido e assinado pela universidade contará com todo o histórico do aluno, além do seu diploma e o certificado de conclusão do curso. Por meio destas informações o aluno pode comprovar toda sua vida acadêmica e garantir que possui a qualificação que diz ter. Para manutenção de um modelo agnóstico de plataforma e que permita a utilização das maiores plataformas atuais, Bitcoin e Ethereum [7], se faz necessário manter a dependência de criptomoedas. Este custo traz ganhos ao modelo, que pode ser aplicado de forma mais ampla e estendido para atender as mais diversas emissões acadêmicas.

A contribuição científica deste trabalho é desenvolver um modelo que permita a emissão, verificação e revogação de documentos acadêmicos através de uma estrutura distribuída baseada

[7] https://www.coindesk.com/

em blockchain. Por consequência, outra contribuição deste trabalho é a análise da viabilidade do modelo proposto através de experimentos realizados com uma prova de conceito.

Tabela 2: Tabela Comparativa

	Adaptável a diferentes Blockchain	Modelo de dados extensível	Permissão do estudante	Emissão por lotes	Histórico completo	Utiliza cripto moeda
(GHAZALI; SALEH, 2018)	Sim	Não	Sim	Não	Não	Sim
(HAN et al., 2018)	Não	Não	Não	Sim	Sim	Não
(GRäTHER et al., 2018)	Não[a]	Sim	Não[b]	Não	Não	Sim
(ARENAS; FERNANDEZ, 2018)	Não	Não	Sim	Não	Não	Não
(GRESCH et al., 2019)	Não	Não	Não	Não	Sim[c]	Sim
(CHENG et al., 2018)	Não	Não	Sim	Não	Não	Sim
(HUYNH et al., 2018)	Não	Não	Sim[d]	Sim	Não	Sim
UnivChain	Sim	Sim	Não	Sim	Sim	Sim

Fonte: Elaborado pelo autor

[a]Suportado apenas em plataformas que implementem contratos inteligentes
[b]Necessário caso estudante queira manter um portfólio na plataforma
[c]Plataforma usa documento digital em formato PDF, que potencialmente permite que ele armazene o histórico
[d]É necessário um endereço da rede Unicoin

4 MODELO UNIVCHAIN

Este capítulo descreve detalhadamente o modelo proposto. Ele inicia com a definição do escopo da proposta e as características do modelo. Em seguida seguem as definições dos atores que interagem com o modelo e seus papéis, passando pela definição dos artefatos utilizados e as plataformas envolvidas. Por fim são detalhados os processos aos quais o modelo atende e a conclusão da apresentação da solução.

O objetivo principal deste trabalho é prover um modelo para emissão de diplomas e certificados acadêmicos por meio do uso de blockchain. O modelo permite a validação das informações sem a necessidade de envolvimento de uma entidade terceira e pode prover até três níveis de segurança. Além disso, o modelo também provê a possibilidade de revogação dos documentos emitidos. Conforme descrito na comparação de trabalhos relacionados, o modelo proposto aqui possui as seguintes características:

- Uma plataforma agnóstica de blockchain, que possa ser utilizada com quaisquer ferramentas que permitam a gravação de transações em blocos.
- Um modelo de dados aberto e de amplo acesso, que permita a sua extensão, melhoramento e avaliação pública por comunidades de pesquisa da área bem como aproveitamento em trabalhos futuros.
- Para viabilizar agilidade na emissão de diplomas e por julgar que as informações que já constam no diploma são suficientes para identificação do aluno, não é necessária a autorização do mesmo por meio de chave pública ou cadastro em plataformas do modelo.
- O modelo proposto atua somente com emissão de diplomas em lotes, viabilizando a emissão de uma quantidade maior de documentos em uma mesma transação. Todas as emissões são feitas em lotes, inclusive as que tiverem somente um diploma a ser emitido.
- O diploma digital será um espelho virtual do diploma físico, o que significa que ele tem as mesmas informações do documento em papel. Isso garante que o espelho terá as mesmas informações obrigatórias previstas pela legislação brasileira vigente.
- O modelo permite a revogação dos documentos acadêmicos por meio da publicação de uma API por parte da entidade emissora.
- O modelo não provê nenhum tipo de interface de controle gráfico para cadastro de documentos e/ou emissão dos mesmos. Toda a comunicação é realizada através de API.
- Através de uma interface web é possível verificar a validade do documento emitido.

Este modelo não analisa requisitos de escalabilidade relacionados a plataforma blockchain, já que ele se propõe a utilizar redes estabelecidas e já amplamente validadas. Aliado a isso, a

característica de não dependência de uma blockchain específica torna o processo de mudança de rede possível de forma fácil.

A visão arquitetura apresentada na Figura 11 mostra os módulos providos pelo modelo. A API UnivChain é responsável pela comunicação de sistemas terceiros da universidade com o modelo. A emissão dos documentos parte do recebimento dos diplomas através desta interface. É importante salientar que esta API não possui nenhuma limitação quanto a implementação, podendo ser uma API via Webservice, via DAO ou até mesmo através de outros protocolos como FTP.

O Frontend UnivChain é a interface web responsável pela verificação dos documentos já emitidos. Através dela é possível, em posse de um documento emitido, realizar a verificação da assinatura digital, da raiz de Merkle e da correta gravação na blockchain. Tanto o Frontend como a API se comunicam com um conjunto de módulos chamados de Backend UnivChain. O Módulo de Assinatura é responsável pela assinatura digital dos documentos a serem emitidos e também pela verificação da mesma. O Módulo de Merkle é responsável única e exclusivamente às tarefas relacionadas a Raiz de Merkle, como o seu cálculo e sua verificação. O Módulo Universidade é o responsável pela comunicação com qualquer API externa relacionada a universidade e neste caso, fica a cargo dele a checagem de revogações, utilizada no processo de verificação de documentos.

Os dois últimos módulos dizem respeito a comunicação com a blockchain. O Client de Blockchain é a biblioteca responsável pela criação da transação na blockchain e seu acompanhamento. O Nó de Blockchain é o nó necessário para que seja possível gravar novas transações na cadeia. Ele não possui nenhuma responsabilidade que não a de realizar o envio das transações geradas pelo Client para os demais nós da rede.

4.1 Atores

4.1.1 Universidade

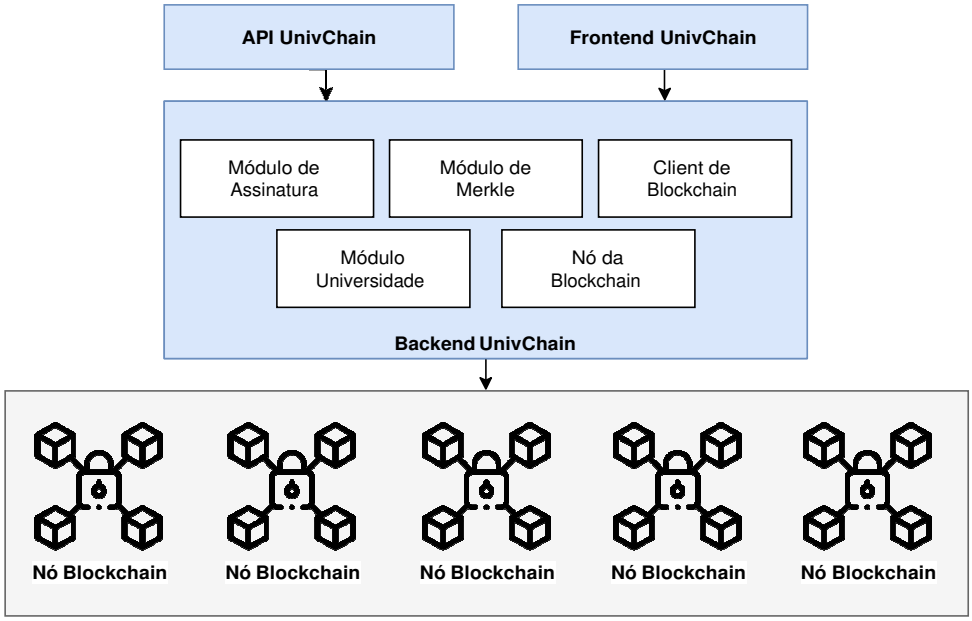
A universidade aqui é considerada qualquer entidade acadêmica oficialmente licenciada pelo MEC e capacitada para oferecer cursos de ensino superior. Esta entidade é a responsável por manter os dados de seus estudantes e consequentemente de suas formações. Mais do que isso, a universidade é a detentora da informação original capaz de atestar que determinado indivíduo possui ou não determinada capacidade. Levando isso em consideração, a universidade é a responsável por prover todas as informações a respeito do diploma e do aluno ao qual se refere.

4.1.2 Estudante

O estudante aqui é considerado qualquer pessoa que tenha vínculo acadêmico de graduação com a universidade. O estudante, ou aluno, é o portador do diploma após sua emissão e

consequentemente tem a capacidade de o armazenar e distribuir como achar necessário. Neste caso, o aluno tem total controle sobre seus dados e do curso do qual o diploma foi emitido. O compartilhamento por sua vez é algo de total responsabilidade do aluno dono do documento, bem como seu armazenamento em dispositivos seguros.

Figura 11: Visão arquitetural do modelo UnivChain



Fonte: Elaborado pelo autor

4.1.3 Empresa

A empresa é o ator que possui a necessidade de verificação de um documento acadêmico emitido pela universidade emissora e para o aluno. Esta necessidade existe a partir de uma candidatura a uma vaga de emprego por parte do aluno. Neste cenário, é necessário que o aluno comprove ter as competências e formações necessárias para realizar as funções de determinado cargo. A empresa então recebe do próprio candidato, que é responsável pelos seus dados e tem posse de seus dados acadêmicos, o diploma que comprova estas informações.

Um ponto importante é que uma universidade também pode desempenhar o papel aqui definido como Empresa. Em casos onde uma universidade precise validar a emissão de um documento de outra universidade ou até mesmo seu, ela torna-se este ator aqui descrito. A universidade pode ter a necessidade de verificação de documentos para contratação de novos docentes e ingresso de alunos em cursos de pós graduação.

4.2 Artefatos

Em artefatos são descritos todos os documentos e recursos que compõem o modelo proposto.

4.2.1 Diploma

O diploma utilizado no modelo proposto é um espelho virtual fidedigno ao documento físico. Isso significa que o diploma possui as mesmas informações do diploma de papel. Por meio deste documento digital é possível gerar uma versão passível de impressão, caso o dono do documento assim deseje.

4.2.2 Certificado Digital

O Certificado digital é um arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica, que proporciona garantia e proteção às informações trocadas. A certificação digital neste modelo é utilizada para assinatura dos diplomas e dos lotes de diplomas emitidos pela universidade, garantindo assim a integridade destas informações (POOJA; YA- DAV, 2018). No modelo proposto somente a Universidade possui Certificação Digital e este é utilizado como o primeiro fator de verificação do documento acadêmico.

4.3 Modelo de dados

Devido a importância das informações que serão utilizadas na construção do espelho virtual dos documentos acadêmicos, esta seção visa mostrar todos os campos previstos para constarem no documento digital. Não são abordados aqui formatos necessários para armazenamento destas informações e sim quais informações são necessárias. A Tabela 3 mostra a lista de informações que constam no documento emitido pelo modelo. O atributo Lista de disciplinas é uma lista de todas as disciplinas cursadas e suas respectivas informações cujo detalhamento é mostrado na Tabela 4.

4.4 Plataformas

Nesta seção são descritas as plataformas utilizadas no modelo e sua importância

4.4.1 Blockchain

Blockchain aqui trata-se da plataforma a ser utilizada para gravação das informações referentes ao lote de certificados emitidos pela universidade. A plataforma é o ponto central de

Tabela 3: Dados do Diploma

Dado	Descrição
Descrição do diploma	Descrição do diploma
Titulação	Título conferido
Titular do Diploma	Nome do Aluno
Data de Nascimento	Data de nascimento do aluno
Naturalidade	Cidade e estado de nascimento do aluno
Documento de Identificação	Registro Geral do Aluno
UF documento	UF de emissão do Registro Geral do Aluno
Data da Titulação	Data da titulação do aluno
Responsáveis pela emissão	Pessoas responsáveis pela titulação na universidade
Dados legais	Dados obrigatórios do documento (Portarias e leis)
Dados Registro Acadêmico	Informações do registro do documento na universidade
Responsáveis Registro Acadêmico	Pessoas responsáveis pelo Registro Acadêmico
Data Emissão	Data de emissão do documento
Competências	Competências do curso
Carga horária	Carga horária do curso
Lista de disciplinas	Lista de disciplinas cursadas

Fonte: Elaborado pelo autor

Tabela 4: Dados de disciplinas

Dado	Descrição
Ano	Ano em que a disciplina foi cursada
Semestre	Semestre em que a disciplina foi cursada
Disciplina	Nome da disciplina
Ementa	Ementa da disciplina
Carga horária	Carga horária total da disciplina
Nota	Nota final da disciplina
Resultado	Resultado final da disciplina

Fonte: Elaborado pelo autor

garantia quanto à veracidade das informações apresentadas pelo aluno à empresa. Por meio dela é possível certificar que o documento em questão é de fato o mesmo documento gerado pela universidade no momento da emissão. O seu uso é detalhado nas seções seguintes e esta é utilizada como segundo fator de verificação do documento acadêmico.

4.4.2 Plataforma Pública da Universidade

A plataforma pública da universidade aqui é tratada como a API que permite a empresa obter um terceiro fator de verificação de um documento. Esta plataforma permite a universidade manter uma lista de diplomas revogados e seus motivos. Uma vez que um dado gravado na blockchain não pode ser alterado (TSILIDOU; FOROGLOU, 2015), um diploma digital emitido pela plataforma seria virtualmente irrevogável e para isso este recurso existe. A plataforma é

operada e mantida pela própria universidade e segue um padrão estipulado, não divulgando quaisquer informações que possam servir para identificação do aluno, somente o *fingerprint* do seu diploma.

4.5 Processos

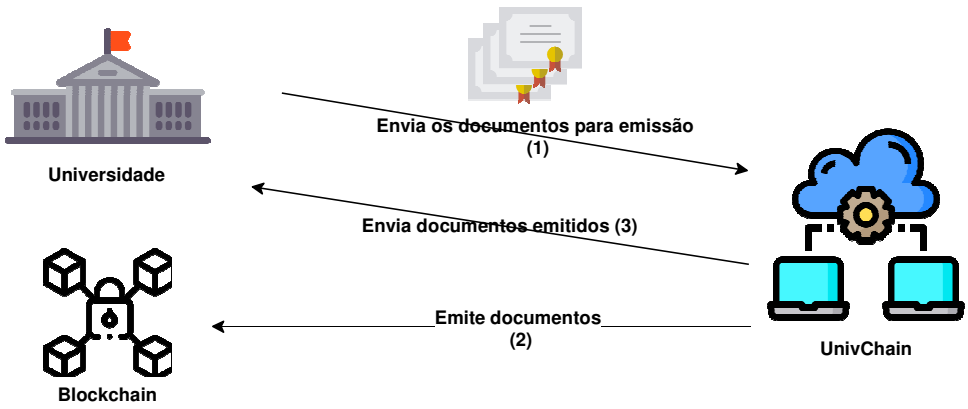
Nesta seção são descritos os processos cobertos pelo modelo e suas integrações com os atores, artefatos e plataformas descritas na seção anterior. Para facilitar o entendimento, cada processo possui seu próprio diagrama.

4.5.1 Emissão do diploma

O processo de emissão de um diploma, certificado de conclusão e histórico do curso está demonstrado na Figura 12. Do ponto de vista da entidade emissora, os documentos já no formato correto são enviados via API para o UnivChain (1), que por sua vez, realiza o processo de emissão e armazenamento das informações necessárias na blockchain (2). Os documentos são então disponibilizados para a universidade (3).

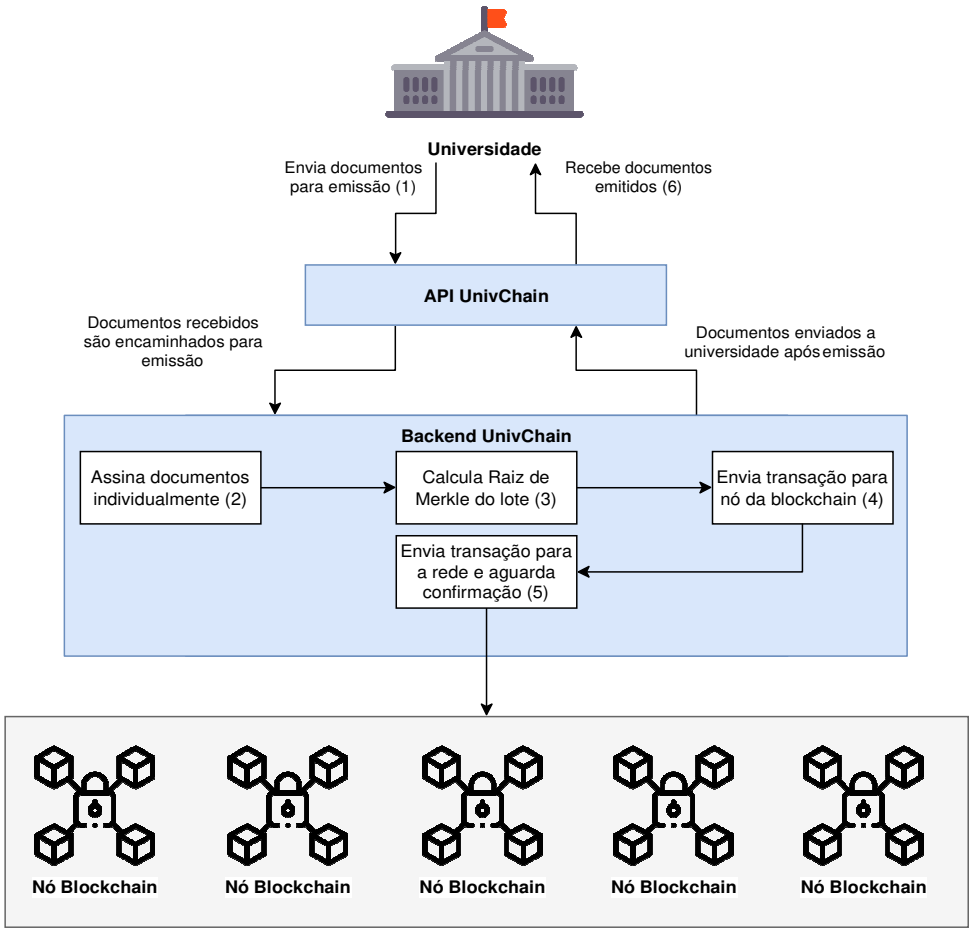
Ao final deste processo a universidade possui os documentos assinados digitalmente, verificáveis e gravados na blockchain, podendo ser enviados aos seus respectivos alunos. A Figura 13 mostra os processos internos realizados pelo modelo para realizar a emissão dos documentos. Recebendo os documentos para emissão através da API (1), os documentos são encaminhados inicialmente para a assinatura individual (2). Finalizada a assinatura, os documentos já assinados são enviados para o c cálculo da raiz de Merkle (3), que em seguida será incluído em uma transação não financeira e enviado ao nó da blockchain (4). O nó da blockchain faz o envio da transação aos demais nós da rede e aguarda o número mínimo de confirmações (5). Após a confirmação os documentos são enviados à universidade (6).

Figura 12: Visão processual da emissão de um documento acadêmico através do modelo UnivChain



Fonte: Elaborado pelo autor

Figura 13: Processos executados pelo modelo para emissão dos documentos acadêmicos recebidos



Fonte: Elaborado pelo autor

4.5.2 Validação do Diploma

O processo ilustrado na Figura 14 diz respeito ao processo realizado de forma independente pela parte interessada, ou seja, cada um dos processos necessários é realizado sem utilizar a plataforma UnivChain. Isso demonstra que é possível que estes processos sejam integrados a soluções comerciais diversas, uma vez que os processos de validação são amplamente conhecidos.

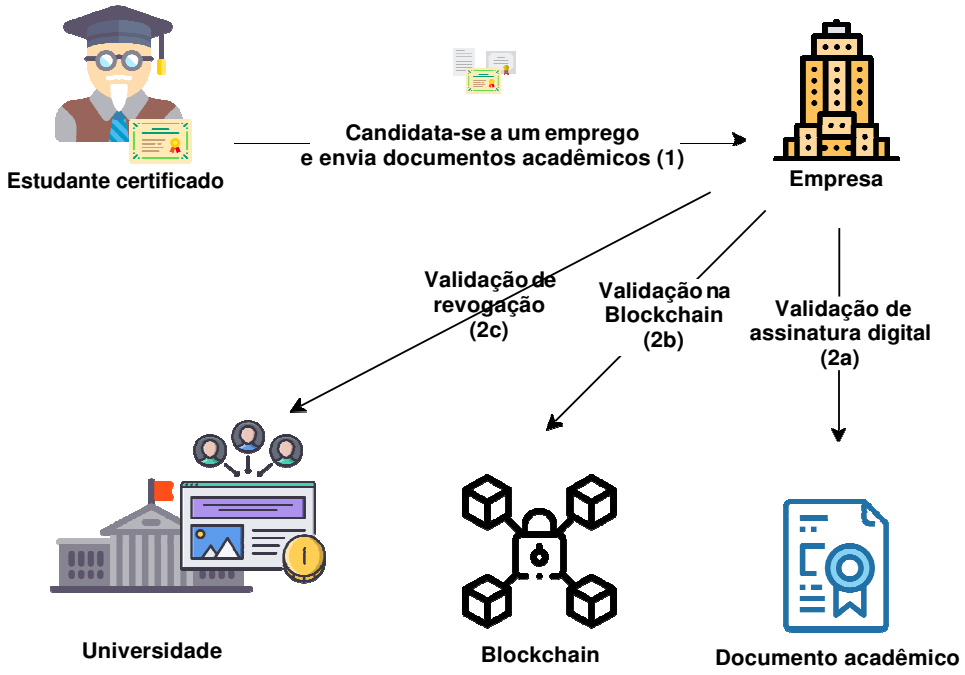
O processo de verificação pode ser dividido em três etapas:

- Verificação da Assinatura Digital
- Verificação do diploma na blockchain
- Verificação de revogação

O processo de verificação de assinatura digital é o processo realizado para checagem se a assinatura é realmente da instituição que o documento apresenta (2a) (ZHENG et al., 2018).

Este passo visa verificar a instituição que realizou a emissão do diploma. O segundo processo de verificação consiste em usar os documentos assinados para realizar a mesma operação criptográfica realizada em sua emissão. Tratando-se de uma operação determinística, o resultado deve ser o mesmo gravado na blockchain no momento da emissão (2b). Por fim, a última etapa é a verificação quanto a revogação de um certificado (2c). Devido a característica imutável da blockchain, é necessário implementar um controle externo para revogar um certificado, o que é feito através da plataforma mantida pela universidade, citada anteriormente. Um fluxo de verificação de um documento deste o envio por parte do aluno até a verificação da empresa pode ser visualizado também na Figura 15.

Figura 14: Visão geral do processo de verificação de documentos realizados fora do ambiente UnivChain



Fonte: Elaborado pelo autor

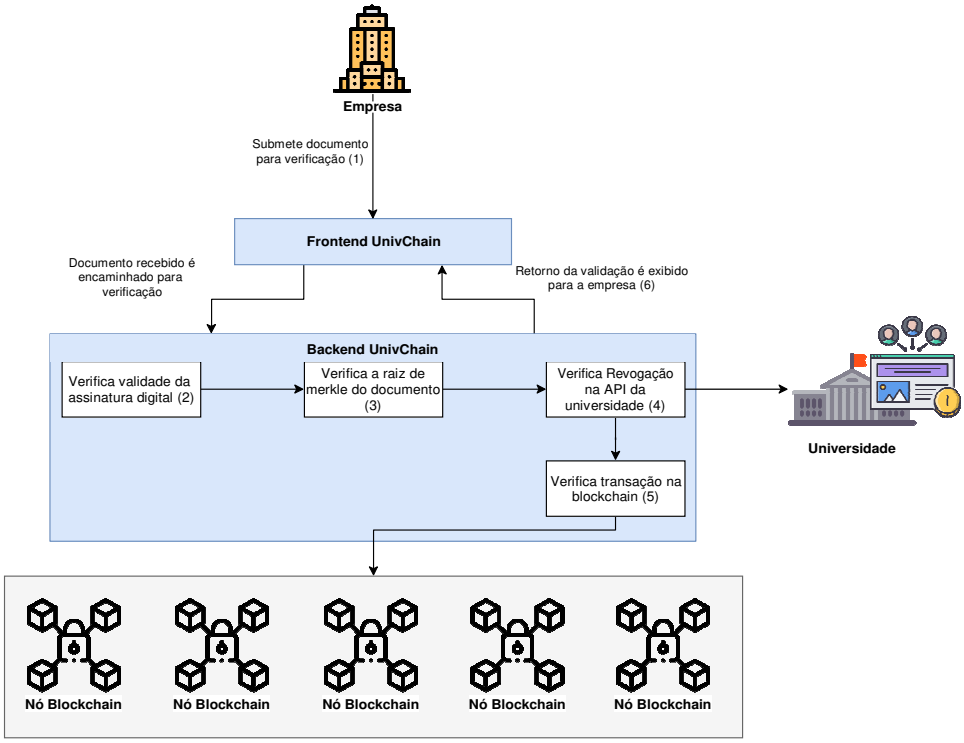
4.5.3 Revogação do Diploma

O processo de revogação do diploma é realizado através da inserção do identificador do documento e do motivo da revogação na API disponibilizada pela universidade. Neste caso, o processo de verificação destacado na Figura 15, item 4, apresentará esta informação a quem estiver verificando o documento. É importante salientar que este processo fica a cargo da universidade, bem como a manutenção da API de consulta a revogações.

4.6 Considerações preliminares

Uma análise preliminar do modelo proposto mostra que ele torna o processo mais confiável do ponto de vista da empresa, que pode efetivamente validar um documento de forma rápida,

Figura 15: Processos executados pelo modelo para verificação de um documento



Fonte: Elaborado pelo autor

que coloca o aluno como dono de suas informações, permitindo a ele realizar diversas cópias de seus dados sem a necessidade de recorrer novamente à universidade. Além disso, a universidade ganha o recurso de revogação de diplomas, algo difícil de ser executado com a emissão em papel atual.

É possível colocar uma outra universidade no papel de empresa empregadora, o que faz com que ela utilize todos estes recursos na validação dos dados de seus novos professores e demais profissionais. Este tipo de recurso pode e deve ser utilizado também para análise curricular de alunos que ingressam em uma segunda graduação ou até mesmo em programas de pós-graduação.

5 METODOLOGIA

Este capítulo é dedicado a descrever a metodologia de avaliação deste trabalho. Inicialmente é descrita a forma como se deu a concepção do modelo seguida da forma como o modelo deverá ser implementado. Por fim, é apresentada a metodologia de avaliação quanto ao atingimento dos objetivos propostos.

5.1 Concepção do modelo

A definição da questão de pesquisa, aliada às análises já feitas dos trabalhos relacionados e suas comparações foram a base para as principais decisões durante a concepção do modelo. Além destas informações, a concepção também utilizou o modelo atual de diplomação, mostrado na Figura 1. O modo atual de emissão de diplomas serviu para comparação com o modelo proposto de forma a permitir uma análise de coerência entre os objetivos do trabalho e proposta propriamente dita. Para proposição do modelo, inicialmente, não foram levadas em consideração questões técnicas específicas, a fim de mantê-lo o mais conceitual possível, permitindo assim maior flexibilidade na implementação do mesmo.

5.2 Implementação do protótipo

Analisando a Tabela 2 é possível compreender que a implementação do protótipo possui cada um dos itens comparados como premissas, ou seja, o protótipo é pensado para atender ao proposto. Tendo em vista a interoperabilidade do protótipo e sua extensibilidade para ambientes baseados em Web Services, optou-se pela utilização da linguagem PHP para seu desenvolvimento.

A fim de facilitar a construção do modelo escolheu-se evitar a reescrita de bibliotecas e soluções já existentes. Pensando nisso, como forma de manter o modelo de dados dos documentos abertos, para que possam ser facilmente estudados e melhorados, será utilizado o padrão Open- Badges (OPEN BADGES FOR LIFELONG LEARNING, 2010). Este padrão já amplamente utilizado será estendido a fim de manter compatibilidade com o mesmo e para facilitar o uso pela sociedade. Utilizar este padrão se mostra uma vantagem uma vez que o mesmo é mantido por um consórcio de empresas e originalmente proposto pela Fundação Mozilla[1], tornando-o assim um candidato forte a se tornar o padrão deste tipo de projeto.

Outra tecnologia a ser adotada é a suíte de aplicações do BlockCerts (CERTIFICATES, RE- PUTATION, AND THE BLOCKCHAIN, 2017). As aplicações já existentes do BlockCerts são de código aberto pela licença MIT (DIGITAL CERTIFICATES PROJECT, 2017) e permite seu uso irrestrito inclusive para alterações. Com os aplicativos para assinatura e verificação dos documentos existentes, é possível estendê-los para suportar o padrão

proposto neste trabalho.

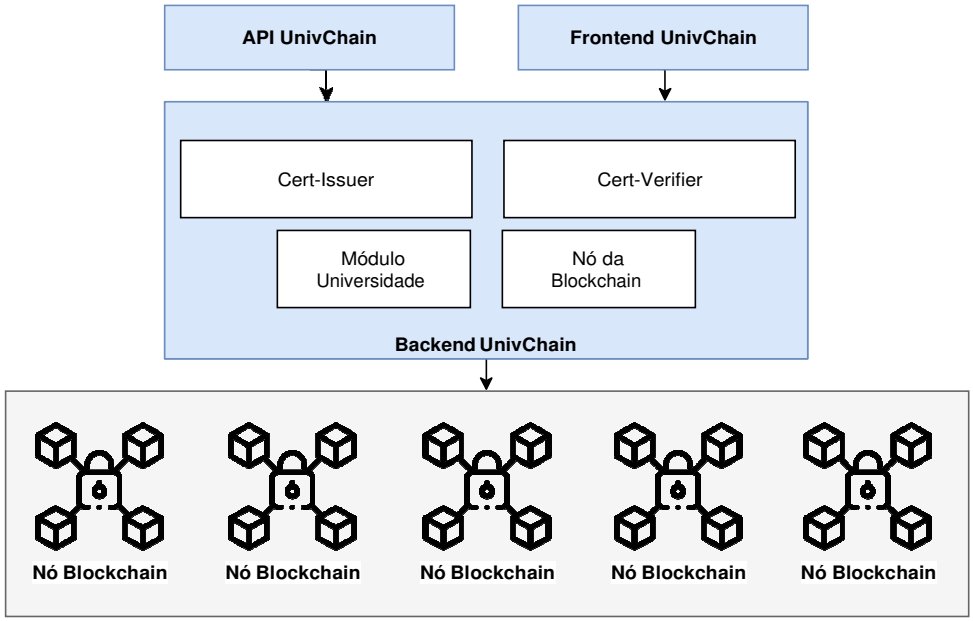
[1]https://foundation.mozilla.org/en/

Há ganho no uso destas aplicações também devido ao uso do padrão Open Badges no projeto BlockCerts. Em particular, o projeto BlockCerts fornece aplicações prontas para assinatura e validação de documentos seguindo os padrões adotados no protótipo.

A interface de comunicação para emissão dos documentos será construída através de uma partição montada, onde os documentos serão colocados. Esta mesma partição será utilizada para retorno dos documentos emitidos pelo UnivChain. A consulta de documentos revogados será realizada através da construção de um Client HTTP capaz de processar chamadas REST.

A plataforma Blockchain pública a ser utilizada será a Bitcoin, por se tratar da mais utilizada globalmente (ZHENG et al., 2018). A plataforma citada conta com rede de teste, o que viabiliza a execução de cenários de teste sem nenhum ônus financeiro. A Figura 16 ilustra a arquitetura proposta para o modelo considerando as decisões de implementação descritas.

Figura 16: Arquitetura geral com as definições deste capítulo



Fonte: Elaborado pelo autor

A primeira etapa da implementação do modelo foi a configuração da blockchain do Bitcoin em sua versão testnet. Para execução de um único nó da blockchain, o mínimo recomendado de memória RAM é 2 GB [2]. Para fins de teste, todos os componentes aqui descritos serão executados em uma mesma máquina virtual. Então, foi utilizada uma configuração com 8 GB de memória a fim de garantir os recursos necessários a todos os componentes. A máquina virtual foi provisionada na empresa DigitalOcean[3]. A Tabela 5 sumariza as configurações do ambiente utilizado para a execução dos experimentos.

Com o provisionamento da máquina virtual, o próximo passo foi a configuração do nó da blockchain. A configuração inicial do nó foi baseada em um processo disponibilizado pela

[2]https://bitcoin.org/en/full-node#minimum-requirements
[3]https://www.digitalocean.com/

Tabela 5: Máquina virtual utilizada na concepção do modelo

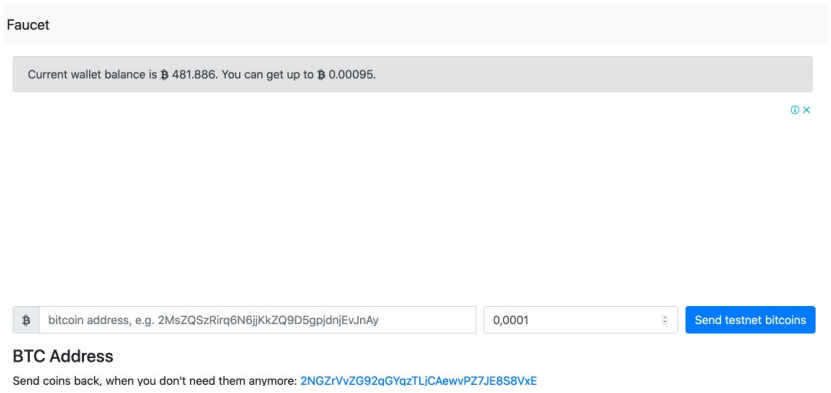
Componente	Valor
Sistema Operacional	Ubuntu 18.04.3 (LTS) x64
Memória RAM	8 GB
CPU	4 CPUS
Disco Rígido	160 GB SSD
Transferência	5 TB

Fonte: Elaborado pelo autor

comunidade de desenvolvedores, e requer o download dos blocos iniciais da rede Blockchain (aproximadamente 20 GB na data em que os experimentos foram realizados).

Neste momento o protótipo conta com uma máquina virtual e um nó Bitcoin corretamente configurados. A próxima etapa é a geração de uma carteira Bitcoin, para que seja possível realizar as transações com os dados dos diplomas. Essa operação é realizada através de um único comando e após a criação da carteira ela já está configurada para ser utilizada, bastando que ela possua fundos. Na rede testnet existem ferramentas chamadas Faucet, como o mostrado na Figura 17. A Figura 18 exibe o resultado de uma consulta quanto ao saldo existente na carteira gerada para este experimento.

Figura 17: Faucet do Bitcoin



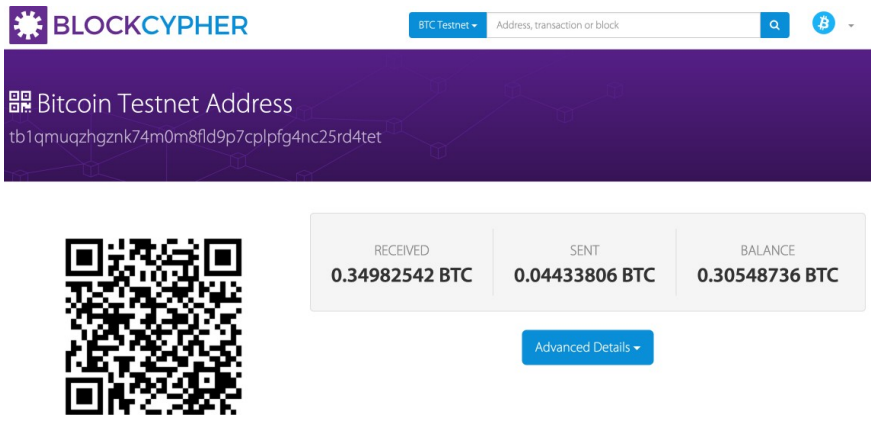
Fonte: Elaborado pelo autor

A próxima etapa foi prover uma API para que os documentos acadêmicos pudessem ser coletados e emitidos. Assim, foi mapeada uma unidade de disco no sistema operacional, uma pasta, onde os documentos são postados e posteriormente são lidos pelo UnivChain. Para este protótipo, não foi realizado um controle de acesso a esta pasta.

Os documentos lidos pelo UnivChain são primeiramente assinados digitalmente, necessitando assim de um par de chaves pública e privada que possa simular o processo realizado por uma assinatura digital. Para isso, foi utilizado o utilitário LibreSSL[4] em sua versão 2.8.3. Este utilitário é utilizado no ambiente corporativo e sua escolha se deu por sua relevância no

[4]https://www.libressl.org/

Figura 18: Consulta à carteira criada na rede Testenet3 do Bitcoin



Fonte: Elaborado pelo autor

mercado.

Para que os diplomas emitidos conforme o padrão proposto neste trabalho possam ser emitidos, é necessário que exista um JSON-LD específico e que ele seja vinculado ao documento. A adição de um novo JSON-LD permite que o documento herde características, campos e tipos não presentes no contexto original. É possível vincular múltiplos formatos para permitir que um documento tenha as características e formato desejados.

Neste trabalho foi criado um arquivo JSON-LD adicionando novos tipos de campos que serão utilizados para diplomas emitidos em território brasileiro. Este padrão será oresponsável por tornar possível que os arquivos possuam os campos necessários para sua correta emissão. Este padrão também serve como garantia de que um arquivo contém os dados e tipos corretos. O arquivo criado pode ser visualizado na Figura 19

Conforme descrito no Capítulo 4, foram gerados um total de 1791 diplomas, seguindo os padrões de dados descritos no conjunto de dados da UFRGS. Com base nesses padrões foram gerados valores aleatórios para os campos de todos os certificados emitidos durante os experimentos. Nesse sentido, desenvolveu-se um script responsável por gerar sequencialmente os 1791 documentos. A Figura 21 ilustra um trecho de um dos diplomas gerados, ainda não publicado através da blockchain.

5.2.1 Configuração do Blockcerts

O ecossistema Blockcerts é composto por uma série de componentes isolados e que em teoria devem ser independentes, permitindo a sua evolução individual. No contexto deste trabalho, os seguintes componentes foram necessários.

- **cert-core**: contém classes comuns e de modelagem
- **cert-issuer**: responsável por fazer a assinatura do documento e registro na Blockchain

Figura 19: JSON-LD schema utilizado para adicionar novos tipos aos arquivos

```
{
  "@context": {
    "schema": "https://schema.org/",
    "brazilianRecipientProfile": {
      "@id": "https://example.com/univchain#brazilianRecipientProfile",
      "@type": "@id"
    },
    "name": "schema:name",
    "birthDate": "schema:birthDate",
    "birthPlace": "schema:birthPlace",
    "document": {
      "@id": "https://example.com/univchain#document",
      "@type": "schema:Text"
    },
    "uf": {
      "@id": "https://example.com/univchain#state",
      "@type": "schema:Text"
    },
    "brazilianBadge": {
      "@id": "https://example.com/univchain#brazilianBadge",
      "@type": "@id"
    },
    "legalIssuerResponsible": {
      "@id": "https://example.com/univchain#legalIssuerResponsible",
      "@type": "schema:name"
    },
    "legalData": {
      "@id": "https://example.com/univchain#legalData",
      "@type": "schema:Text"
    },
    [...]
  }
}
```

Fonte: Elaborado pelo Autor

- **cert-schema**: definições dos *schemas* dos documentos a serem assinados

- **cert-verifier**: responsável pela verificação dos documentos emitidos, para checar a sua veracidade e validade

5.2.1.1 Execução do ecossistema Blockcerts

Com a instância pronta para uso, os repositórios dos projetos do Blockcerts foram clonados nela. Todos os componentes estão disponíveis no GitHub[5]. Neste primeiro momento, nenhum parâmetro foi alterado e as instruções foram seguidas tal qual disponível na documentação. Para a primeira checagem quanto ao funcionamento dos componentes, foi executado um teste de emissão de diploma utilizando o exemplo disponibilizado pelo próprio repositório *cert-issuer*. A verificação do diploma emitido foi feita por meio do repositório *cert-verifier* e ocorreu com sucesso, mostrando assim que o ambiente estava corretamente configurado.

[5]https://github.com/blockchain-certificates/

Figura 20: Trecho do diploma criado mas ainda não assinado


```
{
  "brazilianRecipientProfile": {
    "name": "Emílio Leon",
    "birthDate": "1972-11-25",
    "birthPlace": "Santa Alonso/SC",
    "document": "53.078.213-8",
    "uf": "CE"
  },
  "brazilianBadge": {
    "legalIssuerResponsible": "Isabella Caldeira",
    "legalData": "Ea dolorem deserunt veritatis. Nemo sed hic tenetur enim qui odit veritatis.",
    "academicRecord": "Natus explicabo ducimus blanditiis. Dolores doloremque est doloremque
pariatur.",
    "legalAcademicRecordResponsible": "Simon Casanova",
    "degreeTimeLoad": 1314,
    "transcript": [
      {
        "year": "1975",
        "semester": 1,
        "subject": "Magni qui vitae necessitatibus est maiores.",
        "summary": "Est corporis et iste eius. Deleniti non nihil quis voluptatem molestias fugiat
minima.",
        "subjectTimeLoad": 71,
        "grade": 3,
        "result": "fail"
      },
      ...
    ]
  }
}
```


Fonte: Elaborado pelo Autor

5.2.1.2 Problemas enfrentados

Com o ecossistema em execução, configurado e testado com o padrão próprio do Blockcerts, os arquivos foram adicionados ao projeto *cert-issuer* para que fossem emitidos. O sistema possui uma pasta específica onde todos os arquivos que ali se encontram e obedecem ao padrão estabelecido, são automaticamente emitidos. A emissão é feita de forma sequencial, conforme o nome do arquivo.

Para este teste inicial, um arquivo emitido conforme o Algoritmo **??** foi adicionado na pasta específica do Blockcerts e aguardou-se a emissão do mesmo. Apesar de o documento seguir um padrão válido, o componente utilizado não conseguiu realizar o registro dos documentos de forma correta. Para que o *cert-issuer* reconhecesse o novo formato, foi necessário modificar o software e desacoplá-lo do formato padrão do Blockcerts.

Após esta modificação tentou-se novamente realizar a emissão dos documentos, porém, o software se mostrou inconsistente em suas emissões. Em alguns dos casos o documento não era emitido alegando erro no formato. Utilizando o validador externo disponível na W3C, porém, o documento acusava padrão correto.

Seguiu-se análise do componente *cert-issuer* na tentativa de solucionar a inconsistência na emissão. A inconsistência foi mapeada, porém, o esforço exigido para a adequação do pacote supera o esforço esperado de construção de um componente próprio. Apesar de componentes separados, o ecossistema possui múltiplas dependências entre si, entre elas o modelo de dados utilizado. Neste caso, o experimento com Blockcerts foi encerrado e foi iniciado o novo protótipo com comunicação direta e total desacoplamento do modelo de dados dos documentos.

5.2.2 Desenvolvimento dos módulos adicionais

Com os problemas enfrentados na realização dos testes com Blockcerts, seguiu-se em uma abordagem de comunicação direta, evitando assim possíveis interferências de pacotes de terceiros. Com esta nova abordagem, a comunicação com a Blockchain é feita através da API padrão do Bitcoin, acessada diretamente. A assinatura dos documentos e sua gravação na Blockchain é feita através de um software próprio e escrito exclusivamente para este fim. O nó do Bitcoin, a carteira, os diplomas gerados e as chaves pública e privada foram reaproveitadas no protótipo seguinte. A remoção das bibliotecas do Blockcerts não impacta na arquitetura. Porém, é necessário desenvolver o módulo de cálculo da raiz de Merkle e comunicação com a API do Bitcoin, conforme mostrado na Figura 11.

Após o documento ser adicionado à pasta de leitura do UnivChain, a assinatura digital de cada documento é a primeira etapa e um dos dois pontos que pode ser feito de forma paralela pois independe dos outros documentos. A Assinatura utilizada aqui foi a Assinatura digital com Referência Básica (AD-RB). A assinatura é realizada utilizando a chave privada e a biblioteca LibreSSL. O resultado do comando é um hash criptográfico, que é adicionado ao documento em um campo chamado *SignatureValue*.

Com os documentos já assinados, a próxima etapa é o cálculo da raiz de Merkle e inserção destas informações nos documentos. Cada um dos documentos tem o seu hash individual gerado utilizando um método criptográfico. Neste caso o utilizado foi um duplo hash SHA2[6] de 256 bits. Este é o algoritmo padrão utilizado pela maioria das Blockchains. Os *hashes* de documentos são agrupados em pares e cada par de hash dará origem a um novo hash, através do mesmo processo criptográfico que o criou.

O processo segue até que restem somente dois *hashes*, que darão origem à Raiz de Merkle. Esta informação é armazenada em cada um dos documentos gerados, juntamente com todos os hashes necessários para validação, conforme mostrado na Figura 30. O campo *merkleRoot* mostra o hash final, enquanto o campo *merkleTree* mostra a árvore de hashes necessária para validação do documento.

A raiz de Merkle gerada para o lote deve então ser enviada à blockchain. Para isso é necessário adicionar a informação a uma transação não financeira. Cada transação do bitcoin é composta por entradas e saídas, sendo entradas os bitcoins recebidos e saídas os endereços e valores para onde serão enviados os mesmos. Por se tratar de uma transação não financeira, ela será enviada para um endereço da mesma carteira emissora, ou seja, uma transação do UnivChain para o próprio UnivChain. Para isso, é necessário que uma das saídas seja um endereço válido da própria carteira.

Outro ponto fundamental para geração da transação é o valor da taxa, que neste protótipo foi definida em 0.0000163 bitcoins. O Algoritmo 1 mostra o algoritmo utilizado para gerar e enviar a transação para a rede. Na linha 1 está definido o valor da taxa para a transação, já

[6]https://pt.wikipedia.org/wiki/SHA-2

Figura 21: Trecho do diploma com a raiz de merkle já adicionada


```
"signature": {
    "merkleRoot": "5e558250f06a4779895095bcf39bca7af6ed3896d576107ac17da9538632e99f",
    "merkleTree": [
        "c0f69bf25b2feebc4a59a6fb3a847f1e227cca0de42480075108fc7778165fda",
        "dfbc3484370522f97988ad7ff875dbb3a0e713dcc2b6161261baa7a7db7e2c68",
        "271b2abd63c9c815fe171f18104413b6e03446f951f0eb8954cf5f17fcbf05f9",
        "a450b01485219d895e403a15e04f6d79ed88bafbe8daef2aaa178c369c391aba",
        "c7eb87092753b9239abc508c318c35cf3d623051b8f327238dbfcc1a39571fb5",
        "f602155f537cd76b37f68db01ada97e58c60adbfc6ff5674176f8cff49738d57",
        "5f2ef3a82c0fb6c1cdc391e39751cde372d8629e2b79008490abfd1884fe723d",
        "e0f8e406e2ad8752699a79d143c634755a9a16b00dad1aea993bae70524fabe4",
        "bb30b4039be25569a20758eb5b19cacc6760656feb149cb20a571ad67971d83a",
        "04d6875ba6b8ce72cdf932fdefd7706de62775c99733a83d6d05bad15ddda531"
    ]
}
```


Fonte: Elaborado pelo Autor

a linha 10 evidencia o ponto do algoritmo onde o endereço de destino é gerado. O algoritmo busca uma transação ainda não gasta cujo valor seja superior ao valor da taxa mínima. Com o identificador desta entrada, uma transação é gerada, assinada e enviada à blockchain. Após o envio, o mesmo algoritmo realiza o monitoramento da transação até que ela obtenha o número mínimo de confirmações, neste caso 6, valor utilizado no mercado.

Algorithm 1: Geração da transação na blockchain do Bitcoin

```
Input: merkle_root_hash
transaction_fee = 0.0000163
transaction_index = 0
transaction_input = []
merkle_root = merkle_root_hash
transaction_input = get_transaction_unspent(transaction_index)
transaction_index++
while transaction_input[amount] < transaction_fee do
    transaction_input = get_transaction_unspent(transaction_index)
    transaction_index++
end
transaction = get_transaction_status(transaction_id)
while transaction[confirmations] < 6 do
    sleep(60000)
    transaction = get_transaction_status(transaction_id)
end
update_diplomas(merkle_root, transaction[blockhash])
```

Finalizada a emissão, o hash do bloco é então armazenado também no documento emitido, permitindo a sua posterior verificação. Encerrando assim o processo de emissão do documento. A Figura 22 mostra a assinatura completa do documento, já com o hash do bloco do Bitcoin, que agora pode ser publicamente verificado. A Figura 23 mostra a consulta da transação realizada através de uma ferramenta pública. Nessa tela podem ser identificados a raiz de Merkle e o hash do bloco iguais aos dados armazenados em cada documento do lote de diplomas.

Figura 22: Trecho da assinatura do diploma com a raiz de Merkle já salva na blockchain


```
"signature": {
    "signatureValue":
"eTD2eORizcq5PbcgjNisqNeAGqyu9RtXtPlYwxQB1uJcNTDbTWHuPmISSTg8qkC/dWrzCwhVKjJJMwpMjbAdlfcxfPESLvBvpjA+bt
65dUoY/cJUqvFNpJ11sWr8mSS1kO6nF1r0lnnMuUr
/OCahZtJJ+TylKGCl8BMPqxcYn99odaVR4pqTv8BAhdDn0QcxpbxU7ZvYZ55gtJhoyyQ1mFRq5oXQwGi0cTsdZ
/J4H1cxJWN8SJTJ+thQT50F6ykCZyZmEb4m2FYkgKGWV/HtVlZKfVnwhtGZeqOBtXHWLSMmdZwX35ur
/K4MnEonDMcRSasJjiENPTn1bD1EKMuDZRXUscPNaNsNUkKy1evkUsbnC6ka3VMpG34aD1AQsDkOViU8zRmQCIWAPyr6+Xvi5SUU1Ze
Ng+aVVw27UXwFhz3fRxuUWBOANiHRsaTCgIwgmkBtUinM6LIw7cRzFUWzfcs0wvATzGX3hfj4Kc7LdEaao4nXHXK3bxIDn9
/hWfAAB+SwdHQqOxfIO+SnaL2IaCvYNEUOzZwJAnjQVfpC2QYk0xkZmnvGnVmEUQhQFNJt5yOtvoCedJXdKrWxYMYcnatMfe7ul+QdT
hegsgXWOQHGbx4/GLZ5T+LxSLW7n+km67+pVmpncosDoeYeueouYAcGsc5WQ2bnzLpuVrhWYXc=",
    "merkleRoot": "5e558250f06a4779895095bcf39bca7af6ed3896d576107ac17da9538632e99f",
    "merkleTree": [
        "c0f69bf25b2feebc4a59a6fb3a847f1e227cca0de42480075108fc7778165fda",
        "dfbc3484370522f97988ad7ff875dbb3a0e713dcc2b6161261baa7a7db7e2c68",
        "271b2abd63c9c815fe171f18104413b6e03446f951f0eb8954cf5f17fcbf05f9",
        "a450b01485219d895e403a15e04f6d79ed88bafbe8daef2aaa178c369c391aba",
        "c7eb87092753b9239abc508c318c35cf3d623051b8f327238dbfcc1a39571fb5",
        "f602155f537cd76b37f68db01ada97e58c60adbfc6ff5674176f8cff49738d57",
        "5f2ef3a82c0fb6c1cdc391e39751cde372d8629e2b79008490abfd1884fe723d",
        "e0f8e406e2ad8752699a79d143c634755a9a16b00dad1aea993bae70524fabe4",
        "bb30b4039be25569a20758eb5b19cacc6760656feb149cb20a571ad67971d83a",
        "04d6875ba6b8ce72cdf932fdefd7706de62775c99733a83d6d05bad15ddda531"
    ],
    "anchors": [
        {
            "sourceId": "0000000000002cc5a28716c47556a8be1c1d1e43a7d525f93605bc4f4f924fbe",
                "type": "BTCOpReturn",
                "chain": "bitcoinTestnet3"
        }
    ]
}
```


Fonte: Elaborado pelo Autor

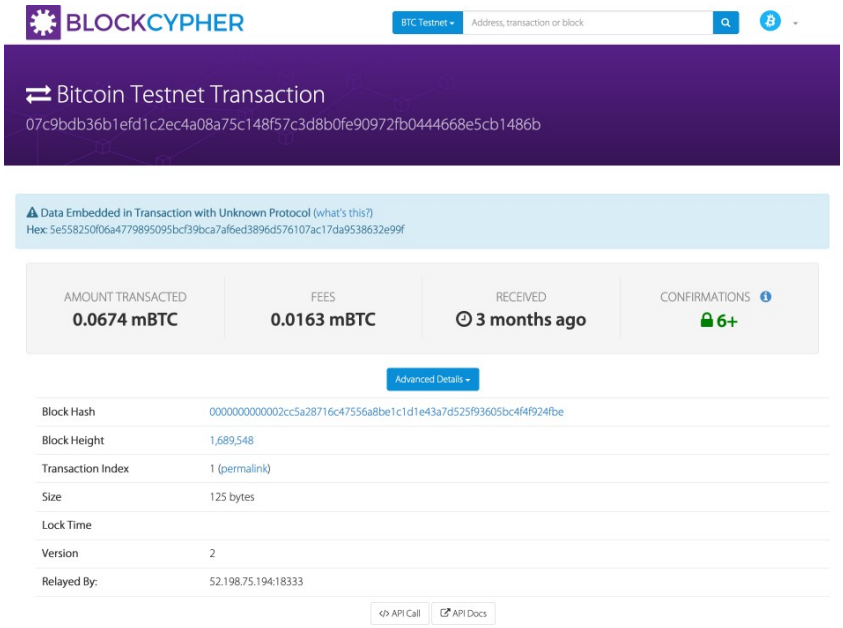
Com a emissão dos documentos completa, a próxima etapa construída foi a API de revogação de documentos. Esta API foi construída utilizando a linguagem PHP e um único endereço, o qual é responsável por disponibilizar um retorno em formato JSON com os documentos revogados e suas eventuais justificativas. Esta etapa é de responsabilidade da instituição emissora. A Figura 24 mostra um exemplo do retorno esperado para API de revogação.

A interface web, chamada de Frontend UnivChain foi o último módulo a ser construído e é o responsável pela verificação do documento. Esta interface permite o *upload* do diploma emitido e faz todas as validações necessárias, exibindo o resultado das validações na tela. O Algoritmo 2 elucida a ordem das checagens realizada pelo UnivChain.

A primeira verificação é quanto ao formato do documento, que deve obedecer aos parâmetros estabelecidos nos arquivos JSON-LD. O próximo passo é a extração das informações necessárias do documento, seguindo das validações de assinatura, árvore de Merkle, bloco do Bitcoin e revogação do documento. Caso alguma delas esteja incorreta, a tela do módulo exibirá uma mensagem de erro informando ao usuário a condição em desacordo. A Figura 25 apresenta a tela após uma verificação bem sucedida do documento. Já as Figuras 26 e 27 apresentam mensagens alertando sobre a impossibilidade de checar a revogação e a de um documento revogado pela universidade, respectivamente.

O protótipo desenvolvido neste capítulo foi utilizado na realização dos experimentos definidos como estudo de caso para avaliação do modelo proposto. O próximo capítulo descreve os resultados e conclusões obtidas.

Figura 23: Consulta pública da transação de emissão do lote de diplomas



Fonte: Elaborado pelo Autor

Figura 24: Retorno da API mostrando a identificação e a razão da revogação


```
[
    {
        "id": "003cf563-30e8-31f6-ac88-7ef658da55ed",
        "revocationReason": "Magni qui vitae necessitatibus est maiores"
    }
]
```


Fonte: Elaborado pelo Autor

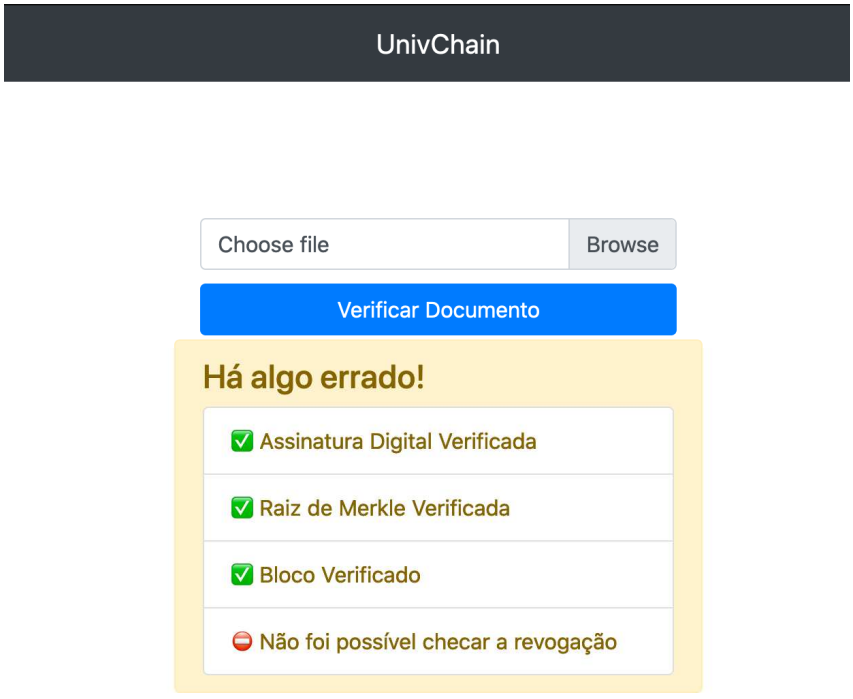


Figura 26: API de revogação indisponível

Algorithm 2: Verificação do documento emitido

```
Input: document_uploaded
Output: errors
if check_document_format(document_uploaded) == false then
    return invalid_document
end
raw_document = extract_raw_document(document_uploaded)
public_key = extract_public_key(document_uploaded)
signature = extract_signature_value(document_uploaded)
revoked_list = extract_revoked_list_url(document_uploaded);
errors = []
if check_document_signature(raw_document, public_key) == false then
    errors[] = invalid_signature
end
if check_merkle_tree(raw_document, signature) == false then
    errors[] = invalid_merkle_tree
end
if check_bitcoin_block(raw_document, signature) == false then
    errors[] = invalid_bitcoin_block
end
if check_revogation(raw_document, revoked_list) == false then
    errors[] = revoked_document
end
return errors
```

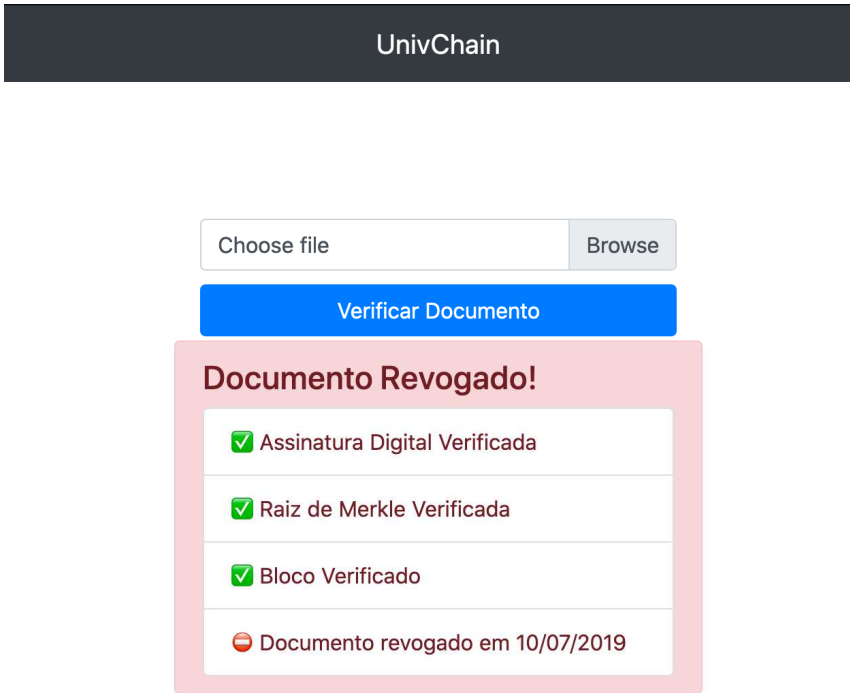


Figura 27: Verificação de um documento revogado

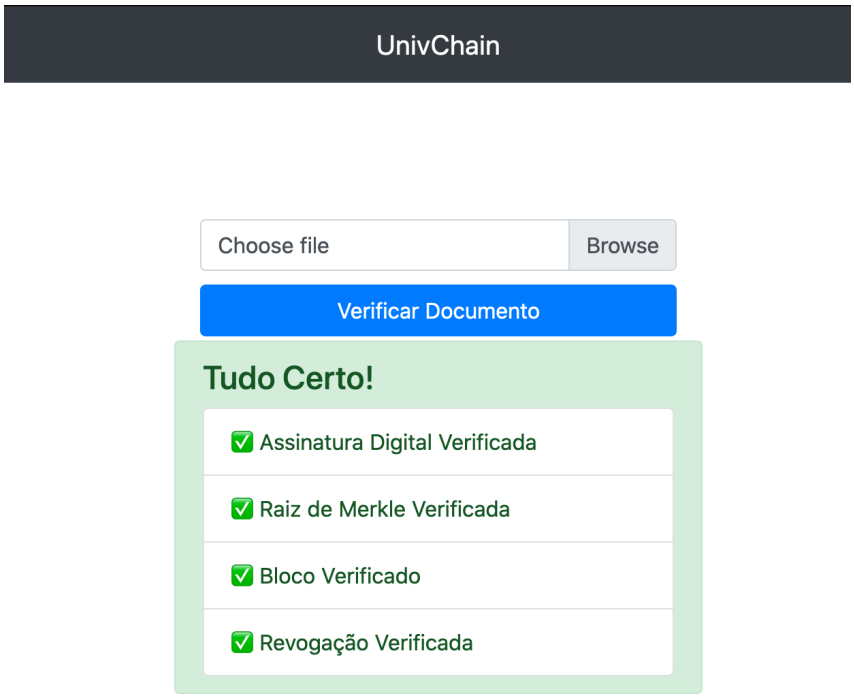


Figura 25: Documento corretamente verificado

5.3 Metodologia de Avaliação

A avaliação da proposta tem como foco os objetivos principais e secundários definidos para o trabalho. Ela será baseada em um caso de uso utilizando um conjunto de dados real, disponibilizado publicamente pela Universidade Federal do Rio Grande do Sul (UFRGS).

5.3.1 Caso de Estudo

A UFRGS dispõe de painel de dados aberto e atualizado, onde expõe informações quanto ao número de alunos diplomados semestralmente[7]. Através deste painel foi possível saber que são diplomados em média 1791 alunos por semestre[8] na universidade. Com este número foi possível definir um caso de uso com quantidade de documentos mais próximo do real.

Por outro lado, não existe um índice que defina o número de documentos cancelados ou revogados no Brasil. Sem este parâmetro é difícil inferir um número base para realização do segundo caso de testes. Sendo assim, a fim de determinar o correto emprego das revogações no modelo proposto, cada um dos lotes terá 5% dos seus diplomas revogados.

Para a correta avaliação do modelo será necessária a geração de documentos simulados de diploma. Além disso, será necessária a geração de um par de chaves pública e privada a fim de simularem o processo de assinatura de cada diploma. Com a inexistência da API pública da

[7]https://www1.ufrgs.br/paineldedados
[8]Dados disponíveis a partir de 01/2017

universidade, uma API será construída e utilizada nos testes de revogação do caso de uso. A versão da blockchain do Bitcoin será a testnet, que não possui valor real, mas simula fielmente o comportamento da versão principal da blockchain.

5.3.2 Análise de Desempenho

O caso de estudo descrito anteriormente permite que o modelo seja avaliado quanto às suas funcionalidades de emissão, revogação e verificação. Para análise quanto a sua viabilidade técnica serão coletados os tempos utilizados para emissão dos documentos, permitindo que o modelo possa ser analisado quanto a possibilidade de uso em um ambiente real de emissão de diplomas. O tempo gasto na emissão dos documentos é fator determinante para a viabilidade técnica do modelo UnivChain, uma vez que um alto tempo na emissão pode tornar o processo incompatível com os atuais processos das universidades.

Serão coletados também os dados relacionados ao uso de recursos de memória RAM no ambiente de execução do UnivChain. O objetivo neste caso é prover maiores informações que possam servir de base para projeção de gastos com este tipo de recurso. Com estas informações será possível avaliar o modelo quanto a todos os objetivos propostos e utilizar estes mesmos dados para projeções de gastos com as diplomações.

6 RESULTADOS E DISCUSSÃO

Este capítulo trata da exibição e análise dos resultados obtidos após a execução do caso de estudo. Os dados a seguir viabilizam uma análise quanto ao atendimento dos objetivos principal e secundários propostos. Após, segue-se uma análise de desempenho, exibindo o tempo gasto e o custo de memória de cada etapa do processo de emissão dos documentos.

6.1 Processo de emissão

A primeira parte do objetivo principal deste trabalho é prover a emissão de documentos acadêmicos através de uma infraestrutura baseada em blockchain. Entende-se que o processo consiste na assinatura digital dos documentos, na inserção em um lote, através da raiz de Merkle e gravação deste mesmo dado em um bloco da blockchain. Estas informações devem constar no documento emitido, tornando-o assim, verificável e autocontido, ou seja, todas as informações necessárias estão no próprio documento.

Além disso, o processo de emissão também contempla a existência de todas as informações necessárias no documento, definidas na Tabela 3 e parcialmente exibidos na Figura 20. A garantia de que as informações constantes no documento são válidas fica a cargo do documento JSON-LD, consultado e utilizado na validação do formato antes mesmo da emissão da assinatura do diploma.

A análise da emissão dos diplomas mostrou que o protótipo conseguiu atender a este objetivo, sendo o documento corretamente emitido. O documento foi corretamente validado quanto ao formato JSON-LD, garantindo que as informações coincidem com tipos de dados existentes no mesmo. Todas as informações necessárias para a correta verificação do documento também se encontram presentes no arquivo: raiz de Merkle, árvore de Merkle, hash do bloco e chave pública do emissor. Todas estas informações, aliadas a existência dos dados detalhados na Tabela 3 dão esta etapa como cumprida e operacional.

6.2 Processo de verificação

O processo de verificação de um diploma é definido como o processo onde se faz a análise dos requisitos de segurança do documento. Como detalhado no modelo, cada documento deve conter todas as informações necessárias que permitam sua correta verificação. O primeiro fator de verificação é a assinatura digital, através de um processo criptográfico. O segundo fator diz respeito a raiz de Merkle, gravada em um bloco público da blockchain. O terceiro fator é a lista de revogações disponibilizada através de uma API pública pela universidade.

Com todos os documentos emitidos, estes foram testados utilizando o Algoritmo 2 a fim de analisar o resultado quanto a todos os fatores de segurança existentes. Todos os 1791 documentos foram validados corretamente, indicando que assim como o processo de emissão, a

verificação dos documentos válidos ocorre com sucesso. Esta etapa mostra que todas as informações necessárias para verificação do documento puderam ser corretamente utilizadas, desde a assinatura digital até a lista de revogação.

6.3 Processo de revogação

Como abordado no Capítulo de Metodologia, após a emissão, 5% dos documentos de cada lote foram revogados de forma aleatória. O objetivo desta etapa é verificar se os documentos revogados são corretamente identificados como tal e se os demais documentos do lote ainda são verificáveis e válidos. O processo de revogação consistiu no sorteio aleatório de 89 documentos de cada lote e inserção dos identificados de cada documento na API de revogação detalhada no Capítulo de Implementação.

Para avaliar o correto uso da lista de revogação, todos os 89 documentos passaram novamente pelo processo de verificação. O processo se mostrou consistente e todos os 89 documentos foram identificados como revogados. Isso demonstra que tendo acesso à API de revogações, o protótipo foi plenamente capaz de realizar a verificação. Na impossibilidade de acesso a esta mesma API, o documento não é apresentado como revogado, porém, o protótipo exibe um alerta informando que não foi possível realizar a consulta.

Com o comportamento descrito acima, é possível dizer com segurança que o protótipo cumpre a última etapa do objetivo principal, a de fornecer a revogação dos documentos emitidos pelo UnivChain. O protótipo pode ainda identificar pontos de atenção, como por exemplo a não disponibilidade da API com os certificados revogados. Outro ponto positivo é o fato de a revogação de um documento ser independente, não impactando na validade dos demais diplomas.

6.4 Análise de Desempenho

O tempo de geração dos documentos para emissão consiste na geração dos arquivos JSON dos 1791 documentos, sem assinatura alguma e pronto para iniciar o seu processo de registro na Blockchain. Houve pouca variação de valores entre as 10 execuções do caso de teste, sendo o maior tempo de 27,66 segundos, enquanto o menor, de 24,28. Esta etapa do processo levou em média 25,92 segundos, com um desvio padrão calculado em 1,14 segundos. A Figura 28 traz um comparativo de todos os tempos utilizados nesta etapa.

A assinatura dos documentos compreende o tempo gasto entre assinar o arquivo e adicionar, ao próprio, o hash da assinatura. Para a assinatura foi utilizado uma mesma chave privada de 4096 bits, padrão recomendado de assinatura. O tempo médio gasto nesta etapa ficou em 63,61 segundos, sendo o menor 60,70 e o maior 67,12. A Figura 29 demonstra todos os tempos de assinatura coletados. O desvio padrão calculado para esta etapa foi de 2,34 segundos, pouco maior que o encontrado na etapa anterior, mas ainda assim baixo. Isso demonstra que a assinatura foi um processo homogêneo durante todos as execuções.

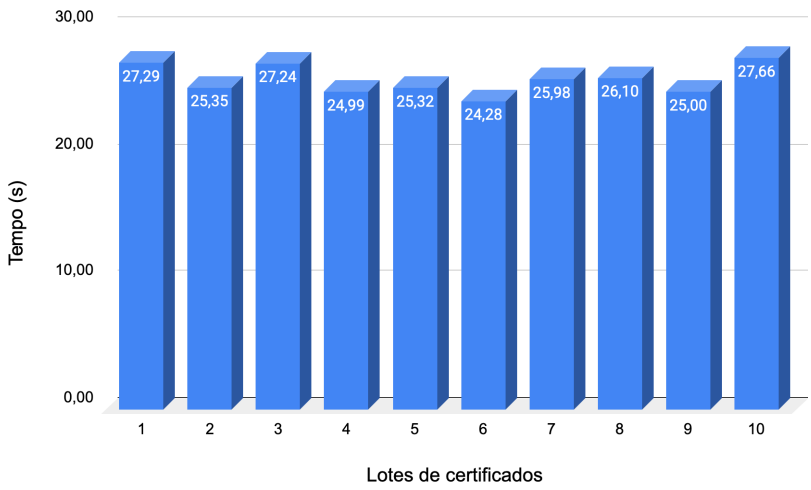


Figura 28: Tempo gasto na geração dos documentos para emissão

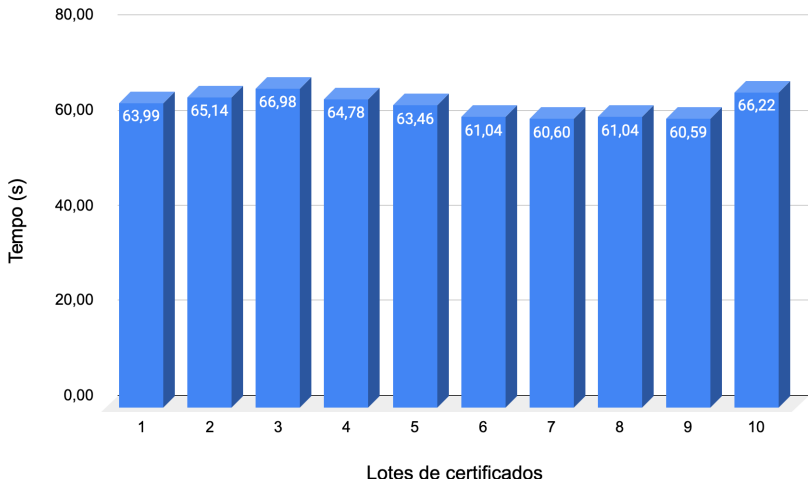


Figura 29: Tempo gasto na assinatura digital dos documentos para emissão

O processo seguinte, de cálculo da Raiz de Merkle, que envolve todos os documentos do lote, foi o tempo que apresentou menor variação nos tempos coletados. Isso se deve pelo fato de o número de documentos ser sempre o mesmo em todos os cenários executados. A amplitude entre o menor e o maior tempo para o cálculo é de apenas 0,18 segundos, com um média de 2,09 segundos de execução total. Esta etapa do processo é a que obteve o menor desvio padrão, calculado em 0,07 segundos, e todos os resultados estão condensados na Figura 30.

A última etapa analisada foi o tempo gasto para criação de uma transação não financeira, contendo a Raiz de Merkle calculada anteriormente, e a espera pela confirmação definitiva da Blockchain do Bitcoin. Conforme detalhado anteriormente, após a inserção de uma informação em um bloco, espera-se a adição de pelo menos outros 6 blocos posteriores. Isso garante que a transação não será desfeita. É importante salientar que este é o único processo que não está sob total controle do modelo, uma vez que ele é dependente dos mineradores vinculados àcadeia.

Figura 30: Tempo gasto no cálculo da Raiz de Merkle antes da emissão dos documentos

Este processo foi o que demonstrou maior variação entre as execuções, alcançando um desvio padrão de 165,39 segundos. A amplitude entre o menor e maior tempo foi de 599,24 segundos, praticamente 10 minutos. A menor medida foi realizada no lote 9, com 120,89 segundos, e a maior no lote 7 com 720,13. A média registrada foi de 330,36 segundos e a Figura 31 deixa clara as diferenças nos tempos de cada um dos lotes.

Figura 31: Tempo gasto aguardando a confirmação do bloco na Blockchain do Bitcoin

Os dados apresentados na Figura 32 mostram o tempo total gasto de todas as etapas agrupadas por lote executado. A diferenciação de cada etapa por cores deixa evidente quais processos mais impactam na completa emissão dos documentos. Como pode ser evidenciado nas análises individuais das etapas, o lote 7 foi aquele que levou o maior tempo para ter sua emissão finalizada, isso em função da espera pela confirmação do bloco. Esta etapa ocupa, em média, 75% do tempo necessário para finalização de um lote de diplomas ou, em média três vezes mais tempo que as outras etapas somadas. A assinatura dos documentos foi o segundo processo mais

custoso consumindo em média 17% do tempo total.

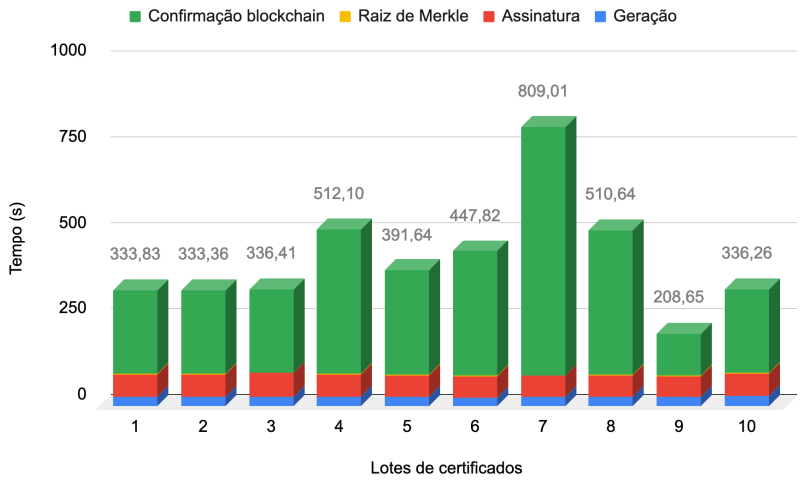


Figura 32: Tempo de registro de certificados em lote

Na Figura 32 foram utilizados todos os tempos individuais de emissão de um documento. Para isso foram computados o tempo de geração do documento sem assinatura, a assinatura do documento e a geração da árvore de Merkle do bloco onde ele está inserido. Na Figura 33 são apresentados os limites identificados, de 122 e 422 segundos, com algumas execuções fora destes parâmetros chegando a 724 segundos. É possível identificar também que 75% dos documentos emitidos levam até 422 segundos para estarem prontos, em lote, para gravação na blockchain. Destes, um terço leva até 242 segundos para atingirem o mesmo status.

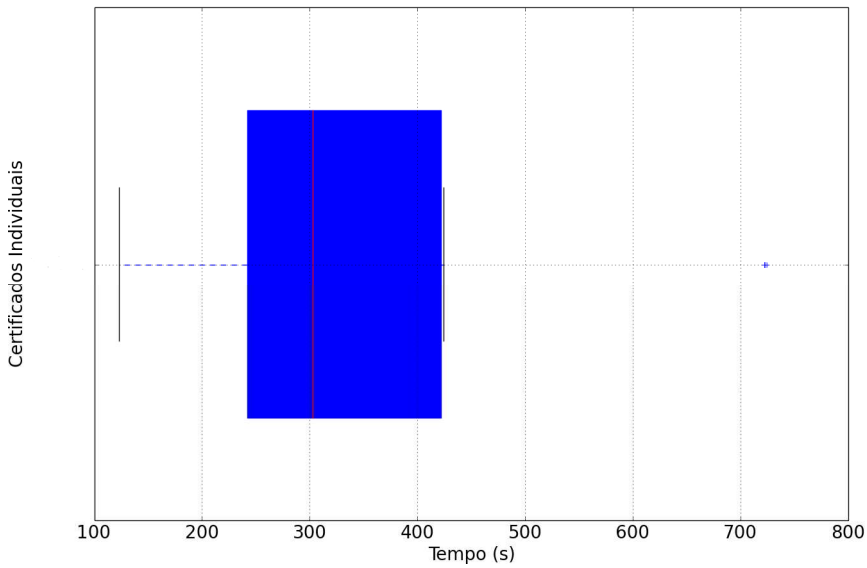


Figura 33: Tempo de processamento individual dos certificados

A Figura 34 apresenta o gasto médio de memória de cada um dos processos realizados, a geração dos documentos, assinatura individual, cálculo da raiz de Merkle e geração da transação

na blockchain. Como pode ser percebido, o impacto do ponto de vista de recursos gastos é baixo, mesmo operando com um número de diplomas emitido em um semestre inteiro. O maior custo registrado é o relacionado a geração dos documentos para emissão, seguido pelo cálculo da raiz de Merkle. Os demais processos utilizam 2 MB de memória para finalizarem suas tarefas.

A máquina virtual utilizada para realização dos cenários mostrou-se superdimensionada após a análise destes resultados. Uma máquina virtual com metade da capacidade seria capaz de executar os mesmos cenários de testes mesmo com a execução de um nó da blockchain rodando paralelamente. O baixo consumo de recursos é um ponto positivo, já que indicam menores custos de infraestrutura necessária para manter uma instância do UnivChain operacional.

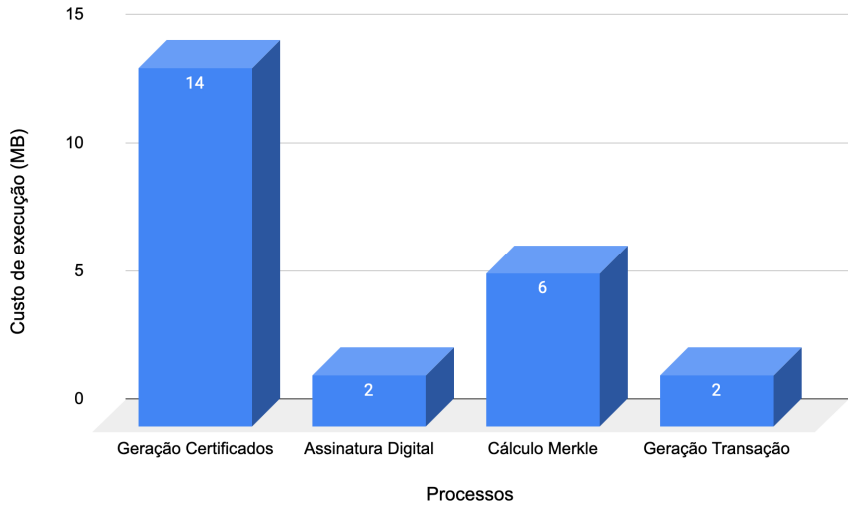


Figura 34: Custo de memória para execução de cada um dos processos

Analisando as informações coletadas é possível afirmar que o modelo proposto possui viabilidade técnica. Os tempos registrados para emissão dos documentos foi muito inferior ao tempo médio de emissão de um documento físico, que hoje leva cerca de 90 dias, segundo dados do próprio MEC. Outro ponto relevante é o fato de a emissão ser feita em lotes e, portanto, mais eficiente. Em cerca de 13 minutos é possível realizar a emissão de 1791 diplomas, assinados digitalmente, gravados permanentemente da Blockchain e verificáveis por entidades terceiras.

O protótipo foi validado utilizando como base os dados médios de diplomações semestrais da UFRGS e a emissão realizada por meio de um único lote. Com isso, o custo médio da gravação do bloco na Blockchain do Bitcoin é de US$ 2,96[1], o que equivale a US$ 0,16 por diploma. O custo das emissões escalará conforme a quantidade de lotes emitidos pela universidade.

[1]Consultado em abril de 2020

6.5 Discussão

Os resultados detalhados anteriormente demonstram que o modelo atende ao objetivo principal, que foi definido como o de *desenvolver um modelo para emissão, verificação e revogação de documentos acadêmicos, utilizando processos independentes através de uma plataforma baseada em blockchain*. Os três processos foram analisados individualmente e atendem ao pro- posto após a implementação do protótipo.

Além disso foram definidos também objetivos secundários relacionados a avaliação dos documentos sem terceiros, prover plenos direitos sob os documentos ao aluno e permitir o uso de assinatura digital em padrão reconhecido no Brasil. Estes objetivos também são considerados atendidos pelo modelo. Não é necessária a existência de uma entidade terceira para verificação dos documentos, já que cada documento possui todas as informações necessárias para sua verificação. Por se tratar de um documento digital, entende-se que o estudante tem plenos poderes sobre o seu diploma emitido, podendo realizar backup e distribuí-lo livremente. A assinatura digital utilizada no protótipo evidencia que o modelo consegue fazer uso deste recurso, atendendo ao último dos objetivos secundários.

Com a coleta de informações relacionadas a tempo e uso de memória dos processos, a análise de desempenho mostra que o protótipo desenvolvido apresenta uma baixa demanda por recursos computacionais. O uso de recursos foi inferior a 20 MB em todos os processos, mesmo com um lote de 1791 documentos a emitir. Para fins de comparação, uma máquina virtual com metade dos recursos da máquina utilizada no protótipo custa US$ 20 na mesma provedora de recursos. Como os trabalhos relacionados não possuem valores em seus artigos, não é possível realizar a comparação de custos de infraestrutura, porém, entende-se que o custo aqui apresentado torna o modelo viável para as universidades brasileiras. Os demais espectros comparados são discutidos abaixo.

O protótipo do UnivChain foi desenvolvido para suportar a alteração do módulo de blockchain, o que o torna adaptável a outras cadeias existentes. Essa característica pode ser percebida somente no modelo de (GHAZALI; SALEH, 2018), todos os outros implementam arquiteturas permissionadas, próprias ou atreladas a *smart contracts*. Além do UnivChain, somente o modelo de (GRäTHER et al., 2018) aplica também um modelo extensível de dados, tornando o reaproveitamento dos modelos mais simples. A utilização de um modelo de dados aberto e extensível faz com que novas versões destes modelos possam surgir e reutilizar a arquitetura aqui proposta para outros experimentos.

A requisição de algum tipo de permissão do estudante para a emissão de um documento torna o processo vulnerável quanto ao tempo empregado. Os modelos de (HAN et al., 2018), (GRäTHER et al., 2018), (GRESCH et al., 2019) e o próprio UnivChain são aqueles onde o documento acadêmico pode ser emitido livremente, sem a necessidade de nenhuma ação extra do estudante, fazendo com que os tempos aqui coletados possam de fato ser executados. A emissão por lotes é um recurso que auxilia as universidades a reduzir as despesas com a emissão

dos documentos, uma vez que uma blockchain pública possui custos. Como os documentos são emitidos em um único lote é necessária uma única transação para os emitir. Neste ponto, os modelos de (HAN et al., 2018) e (HUYNH et al., 2018) também preveem este comportamento.

O histórico completo é uma forma de centralizar as informações de notas, ementas e aproveitamento das disciplinas em um único documento. Estes dados podem servir como base para análises mais aprofundadas de currículos. Neste ponto, os modelos de (HAN et al., 2018) e (GRESCH et al., 2019) contemplam estes recursos. No caso do modelo de (GRESCH et al., 2019), são utilizados documentos PDF para a emissão dos diplomas, o que em teoria viabiliza a geração com histórico completo. Pelo uso de uma blockchain pública, é necessário realizar o pagamento de taxas por transação. Neste caso, os modelos apresentados por (HAN et al., 2018) e (ARENAS; FERNANDEZ, 2018) são os únicos que não utilizam quaisquer criptomoedas para viabilizar a emissão dos documentos, por utilizarem estruturas próprias.

7 CONSIDERAÇÕES FINAIS

A constante evolução tecnológica é também um desafio para a própria tecnologia. Da mesma forma como novos meios de segurança surgem, novos meios de burlar a segurança também. O aumento do poder computacional pode em breve levar a obsolescência de inúmeros algoritmos criptográficos existentes. Blockchain é uma tecnologia que se apoia no uso de criptografia e no uso de computação distribuída para garantir segurança às transações realiza- das através dela. Além disso, sua característica imutável, torna tudo o que estiver gravado em uma transação, permanente. Isso tem feito com que inúmeros projetos tenham surgido apoiados nessa tecnologia, principalmente no que diz respeito a garantia de integridade de um documento.

Este trabalho visou explorar o uso das características da blockchain para prover um ambiente onde documentos acadêmicos possam ser emitidos, verificados e revogados sem a necessidade de contato presencial entre as partes. O processo de emissão pode ser feito pela universidade e o aluno pode receber seus documentos digitais sem necessidade de comparecer a instituição. A comprovação de qualificação para processos seletivos pode ser simplificada, uma vez que o processo de checagem dos documentos do candidato pode ser verificado de forma automatizada e rápida. Além disso, o diploma emitido neste trabalho contém todas as informações que constam no diploma físico, podendo esse ser considerado um espelho virtual.

7.1 Contribuições

Os objetivos deste trabalho se apoiaram nas lacunas deixadas pelos trabalhos relacionados. Com base nisso, destacam-se as seguintes contribuições científicas:

- Com o objetivo de prover um método seguro para emissão de documentos, este trabalho apresentou um modelo composto por um triplo fator de verificação: assinatura digital, raiz de Merkle e bloco da blockchain e lista de revogação de documentos mantida pela universidade. Todos os métodos de verificação são independentes, permitindo suas checagens individuais;

- Este trabalho apresenta um método de revogação de documentos acadêmicos, que dá a entidade emissora a possibilidade de corrigir possíveis erros ou fraude na emissão dos documentos acadêmicos;

- O modelo construído com tecnologias amplamente utilizadas e validadas pelo mercado, faz com que os documentos gerados possam ser verificados inclusive por entidades internacionais. Esta contribuição abre importante porta para integração com entidades de qualquer parte do mundo;

7.2 Limitações

Nesta Seção são descritas algumas das limitações do modelo apresentado.

- É necessário que a universidade possua uma Assinatura Digital válida e que esta esteja disponível para uso pelo UnivChain;
- Os diplomas precisam ser enviados já no formato correto e aceito pelo UnivChain, incluindo os novos campos definidos através dos padrões JSON-LD;
- Os custos por transação possuem valor flutuante, podendo ser mais caros ou baratos do que o descrito ao longo deste trabalho;

7.3 Trabalhos Futuros

Dando sequência ao trabalho aqui descrito, o modelo UnivChain pode ser evoluído quanto a forma como lida com o acesso às revogações de documentos. No formato aqui apresentado, o modelo está sujeito a um ataque de rede, que poderia burlar a verificação, caso o atacante tenha acesso a rede do usuário que está verificando. É possível realizar novos estudos sobre este tema e identificar um modo ainda mais seguro de realizar esta etapa. O modelo também pode ser expandido para suportar o novo padrão de diplomação digital, proposto pelo MEC em 2019[1]. Este padrão regulamenta o uso de arquivos XML[2] em formato específico e assinados digitalmente pela universidade. O suporte a este modelo pode ser integrado como um novo formato aceito bem como um formato final, tornando o JSON um documento intermediário. Como possibilidade adicional de trabalhos futuros, os limites desse modelo podem ser explorados, elevando o número de documentos e determinando qual o máximo de documentos a serem emitidos por um mesmo lote.

[1] http://portal.mec.gov.br/diplomadigital/
[2] https://www.w3.org/XML/

REFERÊNCIAS

ANDROULAKI, E.; MANEVICH, Y.; MURALIDHARAN, S.; MURTHY, C.; NGUYEN, B.; SETHI, M.; SINGH, G.; SMITH, K.; SORNIOTTI, A.; STATHAKOPOULOU, C.; VUKOLIć, M.; BARGER, A.; WEED COCCO, S.; YELLICK, J.; BORTNIKOV, V.; CACHIN, C.; CHRISTIDIS, K.; DE CARO, A.; ENYEART, D.; LAVENTMAN, G. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: 2018. **Anais. . .** [S.l.: s.n.], 2018. p. 1–15.

ARENAS, R.; FERNANDEZ, P. CredenceLedger: a permissioned blockchain forverifiable academic credentials. In: 2018, Stuttgart, Germany. **Anais. . .** [S.l.: s.n.], 2018.

BARTOLETTI, M.; POMPIANU, L. An analysis of Bitcoin OP*RETURN*metadata. **Lecture Notes in Computer Science**, [*S.l.*], 02 2017.

CERTIFICATES, Reputation, and the Blockchain. 2017.

CHENG, J.-C.; LEE, N.-Y.; CHI, C.; CHEN, Y.-H. Blockchain and smart contract for digital certificate. In: 2018. **Anais. . .** [S.l.: s.n.], 2018. p. 1046–1051.

DANG, Q. H. **Secure Hash Standard**. [S.l.]: National Institute of Standards and Technology, 2015.

Data elements and interchange formats — Information interchange — Representation of dates and times. Geneva, CH: International Organization for Standardization, 2004. Standard.

DIGITAL Certificates Project. 2017.

E. PECK, M. Blockchains: how they work and why they'll change the world. **IEEE Spectrum**, [S.l.], v. 54, p. 26–35, 10 2017.

GARWE, E. Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. **Critical Studies in Education**, [S.l.], v. 5, p. 119–135, 05 2015.

GHAZALI, O.; SALEH, O. S. A Graduation Certificate Verification Model via Utilization of the Blockchain Technology. **Journal of Telecommunication, Electronic and Computer Engineering**, Malaysia, v. 10, n. 3-2, p. 29–34, 2018.

GRECH, a.; CAMILLERI, A. **Blockchain in Education**. 2017.

GRESCH, J.; RODRIGUES, B.; SCHEID, E.; KANHERE, S. S.; STILLER, B. The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling. In: 2019, Switzerland. **Anais. . .** [S.l.: s.n.], 2019. v. 339, p. 185–196.

GRäTHER, W.; KOLVENBACH, S.; RULAND, R.; SCHüTTE, J.; TORRES, C.; WENDLAND, F. Blockchain for Education: lifelong learning passport. In: ERCIM BLOCKCHAIN WORKSHOP 2018, 1., 2018, Amsterdam, Netherlands. **Proceedings. . .** [S.l.: s.n.], 2018. v. 2, n. 10.

HAN, M.; LI, Z.; HE, J. S.; WU, D.; XIE, Y.; BABA, A. A Novel Blockchain-based Education Records Verification Solution. In: OF 1ST , 2018, Fort Lauderdale, FL, USA. **Anais. . .** [S.l.: s.n.], 2018. p. 178–183.

HUYNH, T.; HUYNH, T.; PHAM, D.; NGO, A. Issuing and Verifying Digital Certificates with Blockchain. In: 2018. **Anais. . .** [S.l.: s.n.], 2018. p. 332–336.

IANSITI, M.; LAKHANI, K. The Truth About Blockchain:. **Harvard business review**, [S.l.], v. 95, p. 118–127, 01 2017.

KELLOGG, G.; CHAMPIN, P.-A.; LONGLEY, D. **JSON-LD 1.1 – A JSON-based Serialization for Linked Data**. [S.l.]: W3C, 2019. Technical Report.

LI, X.; JIANG, P.; CHEN, T.; LUO, X.; WEN, Q. A Survey on the Security of Blockchain Systems. **Future Generation Computer Systems**, [S.l.], 08 2017.

Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: IEEE/ACM INTERNATIONAL SYMPOSIUM ON CLUSTER, CLOUD AND GRID COMPUTING (CCGRID), 2017., 2017. **Anais. . .** [S.l.: s.n.], 2017. p. 468–477.

M. BACH, L.; MIHALJEVIC, B.; ZAGAR, M. Comparative analysis of blockchain consensus algorithms. In: 2017 17TH , 2018. **Anais. . .** [S.l.: s.n.], 2018. p. 1545–1550.

M. JONES, T.; WICKS, A.; FREEMAN, R. Stakeholder Theory: the state of the art. In: _____. . [S.l.: s.n.], 2017. p. 17–37.

MERKLE, R. C. A Digital Signature Based on a Conventional Encryption Function. In: ADVANCES IN CRYPTOLOGY — CRYPTO '87, 1988, Berlin, Heidelberg. **Anais. . .** Springer Berlin Heidelberg, 1988. p. 369–378.

NAKAMOTO, S. Bitcoin: a peer-to-peer electronic cash system. **Cryptography Mailing list at https://metzdowd.com**, [S.l.], 03 2009.

OPEN Badges for Lifelong Learning. 2010.

POOJA; YADAV, M. Digital Signature. **International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)**, [S.l.], v. 3, n. 6, p. 71–75, jul 2018.

REN, F.; YANG, X.; ZHENG, D. A QC-LDPC Code Based Digital Signature Algorithm. In: SPRINGER BERLIN HEIDELBERG, 2018. **Anais. . .** [S.l.: s.n.], 2018. p. 257–262.

RESHEF KERA, D. Sandboxes and Testnets as "Trading Zones" for Blockchain Governance. In: BLOCKCHAIN AND APPLICATIONS, 2020, Cham. **Anais. . .** Springer International Publishing, 2020. p. 3–12.

SINGHAL, A.; S. PAVITHR, R. Degree Certificate Authentication using QR Code and Smartphone. **International Journal of Computer Applications**, [S.l.], v. 120, p. 38–43, 06 2015.

SPORNY, M.; KELLOGG, G.; LANTHALER, M. JSON-LD 1.0 - A JSON-based Serialization for Linked Data. **W3C Recommendation**, [S.l.], 01 2014.

Swan, M. Blockchain Thinking : the brain as a decentralized autonomous corporation [commentary]. **IEEE Technology and Society Magazine**, [S.l.], v. 34, n. 4, p. 41–52, Dec 2015.

TSILIDOU, A.; FOROGLOU, G. Further applications of the blockchain. In: SPRINGER INTERNATIONAL PUBLISHING, 2015. **Anais. . .** [S.l.: s.n.], 2015.

WARASART, M.; KUACHAROEN, P. Paper-based Document Authentication using Digital Signature and QR Code. , [S.l.], 07 2019.

YANG, R.; WAKEFIELD, R.; LYU, S.; JAYASURIYA, S.; FENGLING, H.; YI, X.; YANG, X.; AMARASINGHE, G.; CHEN, S. Public and private blockchain in construction business process and information integration. **Automation in Construction**, [S.l.], v. 118, 10 2020.

YU, M.; SAHRAEI, S.; LI, S.; AVESTIMEHR, S.; KANNAN, S.; VISWANATH, P. Coded Merkle Tree: solving data availability attacks in blockchains. In: FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 2020, Cham. **Anais. . .** Springer International Publishing, 2020. p. 114–134.

ZHANG, R.; XUE, R.; LIU, L. Security and Privacy on Blockchain. **ACM Computing Surveys**, [S.l.], v. 52, p. 1–34, 07 2019.

ZHENG, Z.; XIE, S.; DAI, H.-N.; CHEN, X.; WANG, H. Blockchain challenges and opportunities: a survey. **International Journal of Web and Grid Services**, [S.l.], v. 14, p. 352, 10 2018.

APÊNDICE A EXEMPLOS DE DIPLOMAS EMITIDOS PELO PROTÓTIPO

A.1 Diploma emitido pelo protótipo UnivChain


```
{
  "@context": [
      "https://w3id.org/openbadges/v2",
      "https://w3id.org/blockcerts/v2",
      "http://138.68.226.195/univchain.json"
  ],
  "type": "Assertion",
  "id": "https://www.unisinos.br/badge/uuid/003cf563-30e8-31f6-ac88-7
   ef658da55ed",
  "issuedOn": "2013-04-02T18:57:16-03:00",
  "recipient": {
    "type": "email",
    "identity": "samuel.queiros@example.com"
  },
  "brazilianRecipientProfile": {
    "name": "Emlio Leon",
    "birthDate": "1972-11-25",
    "birthPlace": "Santa Alonso/SC",
    "document": "53.078.213-8",
    "uf": "CE"
  },
  "badge": {
    "issuer": {
      "url": "https://www.unisinos.br",
        "name": "Universidade do Vale do Rio dos Sinos - UNISINOS",
        "email": "contato@unisinos.br",
        "type": "Profile",
        "id": "https://www.unisinos.br/univchain/v1",
        "image": "data:image/png;base64",
          "revocationList":
    "https://www.unisinos.br/univchain/v1/revocation ",
          "publicKeyPem": "-----BEGIN PUBLIC KEY -------\
    nMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAr2KmCctv1acm1O/cUsdb\nVSZF
    /1VIQznPGVVVpgP2ttSVazJELR/WeEhz+2qKNH7ja5j1JfUqNbWlPyZX0T8e\nVY1QvWWF
    +60844fDYRspFduNaTom3YNivn6d+8WftEbfRf4PDnvbL5/HS33AQSID\npSI1EeMKxT/
    rqfXgcxThm33lm4cyvdssCeJt1RrwSoUAcJ7wkvNLS1Yo4hvVDhER\
    nfj5F1YAChRipAvLW9mVQVRTFqH32kQ56NUt3pXjMq37J7MHva4LuRXDxqXF9u7gz\
    nosq3YXppq3Vf2Jr8Nt/bJXvqCz9cAJReTd01t68G3u4T859dxp2NZeGKSfvqLkcO\
    nP3DBPyIW0TaKkQ6mx1XlNMPo/KxZ/rwOO1S38plfGIAZBDHPexhpXUj66pNEQKKl\
    n9DzHy3DN4ZUgk05zUNV+fQ7GGjBfdd0bKn/8ENw6gTul60auAsBw0G2Sik2jgxNl\
    ncK5m202GTH3KlS+UP7cGjvvakvGYtZMaK76P5kQRicj3xsMdgnnipZZTAeUZE8pt\
```

```
    nlt7aAdGlPKrQkia3Frq5RLnk1DzhW7pIZmZ7AnXFQBbGcZgfQ3jlXWZeEh4zsBZa\
    n71vvDQlAHelSrsfQKJDlC/HvInn28aA/y4CWsa/OKX4kl6T5lsdOE49oqyDSFTfP\
    nEHEECbAGBSGIgwET5uQPzKMCAwEAAQ==\n-----END PUBLIC KEY---------\n"
31   },
32     "name": "Bacharelado em Ci ncia da Computa  o",
33     "type": "BadgeClass",
34   "criteria": {
35     "narrative": "Provident esse quibusdam repudiandae debitis aliquam
    quo enim inventore. Consequatur nihil deserunt aspernatur id."
36   },
37   "image": "  data:image/png;base64",
38   "id": "https://www.unisinos.br/badge/uuid/64522624-572f-11ea-82b4-0242
    ac130003",
39   "description": "Pigeon went on, 'you throw."
40 },
41 "brazilianBadge": {
42   "legalIssuerResponsible": "Isabella Caldeira",
43       "legalData": "Ea dolorem deserunt veritatis. Nemo sed hic tenetur
    enim qui odit veritatis.",
44       "academicRecord": "Natus explicabo ducimus blanditiis.
    Dolores doloremque est doloremque pariatur.",
45   "legalAcademicRecordResponsible": "Simon Casanova",
46   "degreeTimeLoad": 1314,
47   "transcript": [
48     {
49       "year": "1975",
50       "semester": 1,
51       "subject": "Magni qui vitae necessitatibus est maiores.",
52       "summary": "Est corporis et iste eius. Deleniti non nihil quis
    voluptatem molestias fugiat minima.",
53       "subjectTimeLoad": 71,
54       "grade": 3,
55       "result": "fail"
56     },
57     [...]
58   ]
59 },
60 "signature": {
61       "signatureValue": "
    eTD2eORizcq5PbcgjNisqNeAGqyu9RtXtPlYwxQB1uJcNTDbTWHuPmISSTg8qkC/
62   dWrzCwhVKjJJMwpMjbAdlfcxfPESLvBvpjA+bt65dUoY/cJUqvFNpJ11sWr8mSS1k
63   O6nF1r0lnnMuUr/OCahZtJJ+TylKGCl8BMPqxcYn99odaVR4pqTv8BAhdDn0Qcxpb
64   xU7ZvYZ55gtJhoyyQ1mFRq5oXQwGi0cTsdZ/J4H1cxJWN8SJTJ+thQT50F6ykCZyZ
65   mEb4m2FYkgKGWV/HtVlZKfVnwhtGZeqOBtXHWLSMmdZwX35ur/K4MnEonDMcRSasJ
66   jiENPTn1bD1EKMuDZRXUscPNaNsNUkKy1evkUsbnC6ka3VMpG34aD1AQsDkOViU8z
67   RmQCIWAPyr6+Xvi5SUU1ZeNg+aVVw27UXwFhz3fRxuUWBOANiHRsaTCgIwgmkBtUi
68   nM6LIw7cRzFUWzfcs0wvATzGX3hfj4Kc7LdEaao4nXHXK3bxIDn9/hWfAAB+SwdHQ
```

```
69      qOxfIO+SnaL2IaCvYNEUOzZwJAnjQVfpC2QYk0xkZmnvGnVmEUQhQFNJt5yOtvoCe
70      dJXdKrWxYMYcnatMfe7ul+QdThegsgXWOQHGbx4/GLZ5T+LxSLW7n+km67+pVmpnc
71      osDoeYeueouYAcGsc5WQ2bnzLpuVrhWYXc=",
72            "merkleRoot": "5
    e558250f06a4779895095bcf39bca7af6ed3896d576107ac17da9538632e99f",
73      "merkleTree": [
74        "c0f69bf25b2feebc4a59a6fb3a847f1e227cca0de42480075108fc7778165fda",
75        "dfbc3484370522f97988ad7ff875dbb3a0e713dcc2b6161261baa7a7db7e2c68",
76        "271b2abd63c9c815fe171f18104413b6e03446f951f0eb8954cf5f17fcbf05f9",
77        "a450b01485219d895e403a15e04f6d79ed88bafbe8daef2aaa178c369c391aba",
78        "c7eb87092753b9239abc508c318c35cf3d623051b8f327238dbfcc1a39571fb5",
79        "f602155f537cd76b37f68db01ada97e58c60adbfc6ff5674176f8cff49738d57",
80        "5f2ef3a82c0fb6c1cdc391e39751cde372d8629e2b79008490abfd1884fe723d",
81        "e0f8e406e2ad8752699a79d143c634755a9a16b00dad1aea993bae70524fabe4",
82        "bb30b4039be25569a20758eb5b19cacc6760656feb149cb20a571ad67971d83a",
83        "04d6875ba6b8ce72cdf932fdefd7706de62775c99733a83d6d05bad15ddda531"
84      ],
85      "anchors": [
86        {
87          "sourceId": "0000000000002
    cc5a28716c47556a8be1c1d1e43a7d525f93605bc4f4f924fbe",
88          "type": "BTCOpReturn",
89          "chain": "bitcoinTestnet3"
90        }
91      ]
92    }
93 }
```


Código A.1: Diploma emitido pelo protótipo UnivChain com alguns trechos ocultados e/ou reduzidos.

APÊNDICE B ARQUIVOS ESPECIFICADOS COM PADRÃO JSON-LD

B.1 JSON-LD completo utilizado no protótipo

```
{
    "@context": {
        "schema": "https://schema.org/",
        "brazilianRecipientProfile": {
            "@id": "https://m2sdigital.com/univchain#brazilianRecipientProfile",
            "@type": "@id"
        },
        "name": "schema:name",
        "birthDate": "schema:birthDate",
        "birthPlace": "schema:birthPlace",
        "document": {
            "@id": "https://m2sdigital.com/univchain#document",
            "@type": "schema:Text"
        },
        "uf": {
            "@id": "https://m2sdigital.com/univchain#state",
            "@type": "schema:Text"
        },
        "brazilianBadge": {
            "@id": "https://m2sdigital.com/univchain#brazilianBadge",
            "@type": "@id"
        },
        "legalIssuerResponsible": {
            "@id": "https://m2sdigital.com/univchain#legalIssuerResponsible",
            "@type": "schema:name"
        },
        "legalData": {
            "@id": "https://m2sdigital.com/univchain#legalData",
            "@type": "schema:Text"
        },
        "academicRecords": {
            "@id": "https://m2sdigital.com/univchain#academicRecords",
            "@type": "schema:Text"
        },
        "legalAcademicRecordResponsible": {
            "@id": "https://m2sdigital.com/univchain#legalAcademicRecordResponsible",
            "@type": "schema:name"
        },
```

```
        "degreeTimeLoad": {
            "@id": "https://m2sdigital.com/univchain#timeLoad",
            "@type": "schema:Number"
        },
        "transcript": {
            "@id": "https://m2sdigital.com/univchain#transcript",
            "@type": "@id"
        },
        "year": {
            "@id": "https://m2sdigital.com/univchain#year",
            "@type": "schema:Number"
        },
        "semester": {
            "@id": "https://m2sdigital.com/univchain#semester",
            "@type": "schema:Number"
        },
        "subject": {
            "@id": "https://m2sdigital.com/univchain#subject",
            "@type": "schema:Text"
        },
        "summary": {
            "@id": "https://m2sdigital.com/univchain#summary",
            "@type": "schema:Text"
        },
        "subjectTimeLoad": {
            "@id": "https://m2sdigital.com/univchain#subjectTimeLoad",
            "@type": "schema:Number"
        },
        "grade": {
            "@id": "https://m2sdigital.com/univchain#grade",
            "@type": "schema:Text"
        },
        "result": {
            "@id": "https://m2sdigital.com/univchain#result",
            "@type": "schema:Text"
        },
        "chain": {
            "@id": "https://m2sdigital.com/univchain#chain",
            "@type": "schema:Text"
        },
        "signatureValue": {
            "@id": "https://m2sdigital.com/univchain#signatureValue",
            "@type": "schema:Text"
        },
        "merkleTree": {
            "@id": "https://m2sdigital.com/univchain#merkleTree",
            "@type": "schema:Text"
```

```
86                }
87        }
88 }
```

Código B.1: JSON-LD schema completo utilizado no protótipo