

# UnivChain: um modelo para autenticação de documentos acadêmicos baseado em blockchain

Mateus Schmitz da Silveira<sup>1</sup>, Rodolfo Stoffel Antunes<sup>1</sup>, Cristiano André da Costa<sup>1</sup>

<sup>1</sup>PPGCA - Programa de Pós-graduação em Computação Aplicada (UNISINOS)  
São Leopoldo – RS – Brasil

**Abstract.** *Amid constant technological advances, academic document validation remains a challenge for universities, students, and the labor market. The current model does not provide simple and robust method for storage, distribution, and authenticity verification to third parties. This work presents a blockchain-based model for authenticity verification of documents without requiring intermediaries or proof from the issuing entity. The proposed model uses a public blockchain for broad access, applicability, and cost reduction.*

**Resumo.** *Em meio ao constante avanço tecnológico, a validação de documentos acadêmicos segue sendo um desafio para universidades, alunos e o mercado de trabalho. O modelo atual não oferece um método simples e robusto para verificação de autenticidade, armazenamento, e distribuição. Este trabalho apresenta um modelo baseado em blockchain para a validação 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 permite amplo acesso, aplicabilidade e redução de custos.*

## 1. Introdução

Em um mundo em constante avanço tecnológico, ainda existem muitas dificuldades em autenticar documentos acadêmicos. Estas dificuldades vão desde os meios disponíveis até a quantidade de trabalhos manuais necessários [Singhal and S. Pavithr 2015], o que é exacerbado no caso da verificação de um grande número de documentos de uma só vez. Tal autenticação é um processo fundamental quando o recipiente de um documento deseja utilizá-lo para se candidatar a uma vaga de emprego ou reingressar na universidade e, portanto, precisa comprovar suas qualificações.

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 (Ministério da Educação). 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 digitais de verificação. Entretanto, tais serviços normalmente se aplicam a documentos de uso único como comprovantes de matrícula e frequência.

O estudante certificado precisa realizar então a guarda dos documentos de forma segura [Han et al. 2018]. A perda, extravio, ou 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, e requer a assinatura manual do estudante. Outro ponto crucial é o fato de o aluno possuir apenas este tipo

de documento 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 como prova.

É ponto relevante também o fato de a falsificação de documentos acadêmicos causar prejuízos na casa dos milhões de dólares [Børresen et al. 2020]. 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.

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 [Zheng et al. 2018]. A proposta deste trabalho visa a utilizar as características da blockchain para resolver os problemas de custo, emissão, armazenamento, e verificação de documentos acadêmicos, permitindo a consulta à sua autenticidade de forma rápida, segura, e transparente.

A principal contribuição deste trabalho é desenvolver um modelo que permita a emissão e verificação de documentos acadêmicos através de uma estrutura distribuída baseada em blockchain. Com o seu uso, a universidade pode emitir um espelho virtual do diploma, que possui as mesmas informações do documento físico. Este arquivo é assinado digitalmente pela entidade emissora e, após isso, passa por um processo criptográfico. O resultado deste processo é enviado para inclusão em uma blockchain. Neste momento, a emissão do diploma está concluída e o aluno recebe o espelho virtual, ou seja, o arquivo do seu diploma. Este processo não é excludente, podendo ser realizado de forma concomitante com a emissão do documento físico tradicional. Outra contribuição deste trabalho é a análise da viabilidade do modelo proposto através de experimentos realizados com uma prova de conceito.

O restante do artigo está organizado da seguinte forma. Na Seção 2 são apresentados os trabalhos relacionados, seguido pelo modelo UnivChain na Seção 3. A Seção 4 apresenta o estudo de caso para avaliação da proposta e os resultados obtidos. Por fim, a Seção 5 apresenta as considerações finais.

## **2. Trabalhos Relacionados**

Esta Seção apresenta estudos que possuem similaridades com o trabalho aqui proposto, por envolverem blockchain aplicada à validação de documentos acadêmicos. As principais características dos estudos avaliados são sumarizadas e comparadas na Tabela 1, apresentada ao final da seção.

O modelo teórico apresentado por [Ghazali and Saleh 2018] é dividido em dois processos: A emissão do certificado e a verificação do mesmo. O estudo utiliza blockchain mas não deixa claro o real benefício do seu uso, já que não faz uso dos dados salvos na rede. [Han et al. 2018] propõe um ambiente onde os indivíduos sejam donos de seus respectivos registros acadêmicos oficiais e consigam compartilhá-los. A arquitetura proposta transforma as entidades emissoras, alunos, e demais interessados em validar documentos acadêmicos, em nós da plataforma. Além disso, a plataforma mantém o conceito de nó minerador<sup>1</sup> em aplicações de blockchain atuais, o qual executa o mesmo trabalho

---

<sup>1</sup><https://bitcoin.org/en/vocabulary#mining>

feito em outras plataformas blockchain.

O trabalho de [Gräther et al. 2018] define uma estrutura de entidades autorizadas e autoridades para emissão de documentos. 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. Os certificados são responsáveis pela emissão dos diplomas em si. O modelo CredenceLedger, proposto por [Arenas and Fernandez 2018], utiliza uma blockchain permissionada para armazenar provas de veracidade de documentos acadêmicos. A proposta 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.

O modelo de [Gresch et al. 2019] parte do levantamento de requisitos feito com os *stakeholders* [Freeman et al. 2010] do projeto na University of Zurich (UZH). O projeto toma como base entrevistas feitas com as partes interessadas, e os requisitos levantados nestas entrevistas, para a definição do modelo. O modelo pode ser dividido em três partes. A primeira cobre os requisitos 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.

O projeto de [Cheng et al. 2018] apresenta um modelo baseado em *Smart Contracts* rodando na plataforma Ethereum. São definidos 4 grupos de usuários, sendo eles: escolas ou unidades de certificação, estudantes ou companhias, provedores de serviço, e plataforma Ethereum. O modelo apresentado por [Huynh et al. 2018], denominado Unicert, é baseado no Unicoin, uma criptomoeda desenvolvida sobre a tecnologia blockchain. O modelo apresentado pode 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, utilizando o mesmo tipo de algoritmo de consenso, o *Proof of Work*.

A proposta apresentada neste artigo atende cinco dos seis requisitos relacionados na Tabela 1, 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 uma arquitetura que possa ser constantemente melhorada e estendida, o modelo de dados utilizado é Open Source. Visando a facilidade e menor modificação do processo 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, resultando na economia em sua emissão e permitindo 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

**Tabela 1. Tabela Comparativa**

	Adaptável a Blockchain	Dados extensíveis	Ação do estudante	Lotes	Histórico completo	cripto moeda
[Ghazali and Saleh 2018]	Sim	Não	Sim	Não	Não	Sim
[Han et al. 2018]	Não	Não	Não	Sim	Sim	Não
[Gräther et al. 2018]	Não <sup>a</sup>	Sim	Não <sup>b</sup>	Não	Não	Sim
[Arenas and Fernandez 2018]	Não	Não	Sim	Não	Não	Não
[Gresch et al. 2019]	Não	Não	Não	Não	Sim <sup>c</sup>	Sim
[Cheng et al. 2018]	Não	Não	Sim	Não	Não	Sim
[Huynh et al. 2018]	Não	Não	Não	Não	Não	Não
UnivChain	Sim	Sim	Não	Sim	Sim	Não

<sup>a</sup>Suportado apenas em plataformas que implementem contratos inteligentes.

<sup>b</sup>Necessário caso estudante queira manter um portfólio na plataforma.

<sup>c</sup>Plataforma usa documento digital em formato PDF, permitindo o armazenamento do histórico.

que permita a utilização das maiores plataformas atuais, Bitcoin e Ethereum<sup>2</sup>, 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.

### 3. UnivChain

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.

A visão geral do modelo mostrada na Figura 1 evidencia todas as operações mapeadas e suportadas pela plataforma. Por meio da análise da visão geral é possível perceber a existência de três atores independentes e que juntos compõem o modelo proposto. Cada ator e seus respectivos papéis são detalhados abaixo.

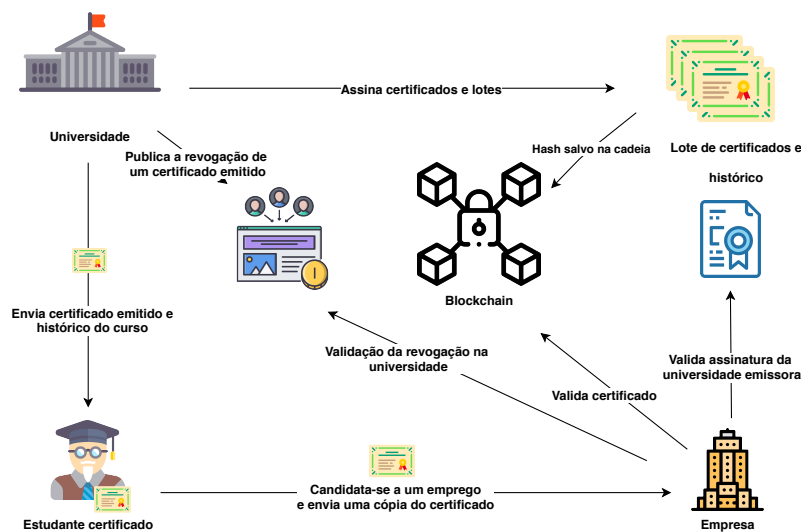
#### 3.1. Atores

O modelo UnivChain é composto por três atores que desempenham diferentes papéis no ciclo de vida da emissão e verificação de um documento acadêmico. A **universidade** aqui é considerada qualquer entidade acadêmica oficialmente licenciada pelo MEC e capacitada para oferecer cursos de ensino superior. Ela também é a responsável por manter os dados de seus estudantes e conseqüentemente de suas formações. A universidade é a responsável por prover todas as informações a respeito do diploma, do certificado de conclusão, do histórico do curso e do aluno ao qual se refere.

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

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

<sup>2</sup><https://www.coindesk.com/>



**Figura 1. Visão geral do modelo proposto**

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. Um ponto importante é que uma universidade também pode desempenhar o papel aqui definido como empresa.

### 3.2. Artefatos

O modelo UnivChain tem dois artefatos, que são recursos utilizados para a plataforma: Diploma e Certificado Digital. 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.

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 and Yadav 2018].

### 3.3. Plataformas

O modelo UnivChain utiliza como base duas plataformas externas em seu funcionamento. Uma delas é a Blockchain e outra a plataforma de revogação, mantida pela entidade emissora do diploma. A Blockchain é utilizada para gravação das informações referentes ao lote de certificados emitidos pela universidade. Ela é o ponto central de garantia quanto à veracidade das informações apresentadas pelo aluno à empresa. Por sua vez, a plataforma de revogação é uma plataforma pública da universidade que permite a manutenção de uma lista de diplomas revogados e sua respectiva motivação.

### 3.4. Processos

O modelo proposto constitui-se de dois processos distintos, a emissão do documento acadêmico e sua verificação após emitido. O processo de **emissão** constitui-se da geração

do arquivo base, assinatura digital do mesmo, cálculo da Raiz de Merkle do lote, e gravação na blockchain. Após estas etapas o documento é enviado ao aluno.

O processo de validação do diploma emitido pode ser dividido em três etapas de verificação: (i) verificação da assinatura digital; (ii) verificação do diploma na blockchain; (iii) verificação da revogação. A verificação de assinatura digital é o processo realizado para checagem se a assinatura é realmente da instituição que o documento apresenta [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. Por fim, a última etapa é a verificação quanto a revogação de um certificado. 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.

## **4. Avaliação**

Nesta Seção são detalhados o caso de estudo e a análise de desempenho utilizados para avaliar a proposta. Também são descritos e analisados os resultados obtidos da realização das avaliações do modelo.

A avaliação foi realizada utilizando um protótipo da arquitetura proposta, implementado utilizando a linguagem PHP. A comunicação com a Blockchain foi implementada por meio de conexão via API HTTP utilizando o padrão RPC. A assinatura dos documentos é feita pelo mesmo software, o qual usa a biblioteca OpenSSL. Com a assinatura dos documentos, as informações são inseridas no próprio arquivo assinado.

### **4.1. Caso de Estudo**

A análise do modelo foi realizada através de um estudo de caso especificado com base em dados reais públicos, disponibilizados pela Universidade Federal do Rio Grande do Sul. Através destes dados foi possível saber que são diplomados em média 1791 alunos por semestre<sup>3</sup> na universidade. Com este número foi possível definir um cenário 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. Sendo assim, foi escolhido um número arbitrário de 5% dos documentos emitidos. Na prática, isso quer dizer que o segundo caso de testes fará a revogação de 89 documentos escolhidos aleatoriamente no lote.

Com a execução dos testes serão realizadas as medições de tempo gasto na emissão e a quantidade de recursos computacionais empregados em suas emissões. O tempo gasto tem como objetivo realizar a comparação com o processo atual e manual de diplomação. A coleta do uso de recursos computacionais, mais especificamente a coleta de recursos de memória, tem como objetivo analisar a viabilidade técnica para execução do protótipo em um ambiente acadêmico.

### **4.2. Resultados**

A análise de desempenho foi conduzida levando em consideração o tempo necessário para processamento e emissão de todos os documentos. Para fins de coleta das métricas,

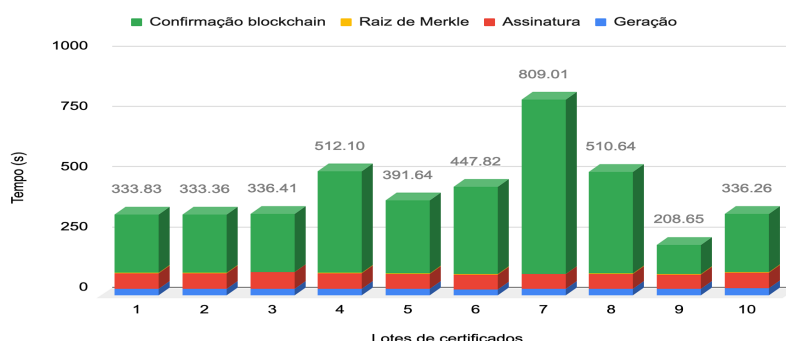
---

<sup>3</sup>Dados disponíveis a partir de 01/2017

foram realizadas 10 rodadas de execução de testes. Cada uma das execuções consistiu na geração dos 1791 documentos, assinaturas individuais, cálculo da Raiz de Merkle e gravação na blockchain pública. Cada uma das execuções resultou em um lote de diplomas que tiveram a raiz de Merkle armazenada em um bloco da Blockchain.

O cenário proposto foi executado com sucesso, realizando a correta emissão dos diplomas que constavam nos 10 lotes gerados. Todos os diplomas receberam corretamente as suas informações da raiz de Merkle e seu respectivo bloco da cadeia. Com a emissão dos documentos finalizada, foi realizada a revogação dos 89 documentos, equivalente a 5% dos documentos emitidos. Finalizada a revogação, a verificação dos documentos foi realizada também com sucesso, onde todos os documentos ainda válidos foram identificados como corretos e os inválidos acusaram erro de verificação. Conclui-se com este caso de estudo que o modelo apresentado consegue emitir, validar e revogar um documento acadêmico na forma como se propõe durante a descrição deste trabalho.

Quando analisado o tempo gasto para emissão de cada lote de diplomas, é possível perceber em todas as execuções que a maior parte do tempo é gasta aguardando a confirmação da blockchain. Na Figura 2 evidencia-se que o maior tempo de espera para gravação foi de 720,13 segundos, enquanto o menor foi de 120,89. 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. Na média, o tempo empregado para gravação de um lote na blockchain foi de 330,36 segundos. 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.



**Figura 2. Tempo de registro de certificados em lote**

A etapa de assinatura dos diplomas é realizada individualmente e consome em média 63,61 segundos por lote de documentos. Este processo registrou seu menor tempo quando levou 60,70 segundos e o maior levando 67,12 segundos. O desvio padrão calculado para esta etapa foi de 2,34 segundos, pouco maior que o encontrado na etapa de geração dos documentos. No geral, esta etapa consumiu em média 17% do tempo total empregado na geração de cada lote de documentos.

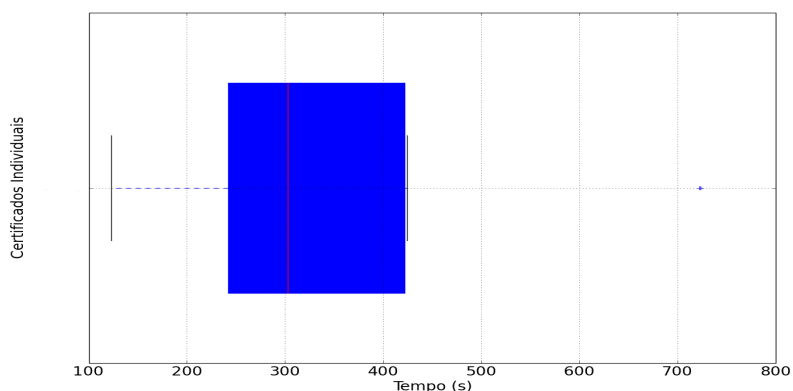
O tempo médio para geração dos documentos iniciais, ainda não assinados, foi de 25,92 segundos. O menor tempo registrado foi de 24,28 segundos e o maior 27,66 segundos, tendo um desvio padrão calculado em 1,14 segundos. Este é o tempo registrado para geração dos 1791 documentos de cada lote. A geração dos documentos iniciais, não assinados, consumiu em média 7% do tempo total de emissão do lote.

O processo menos custoso do ponto de vista de tempo gasto é o registrado para

cálculo da raiz de Merkle. O tempo empregado foi de 2 segundos em média, resultando em pouco impacto no tempo total de geração dos documentos. Como pode ser percebido através da Figura 2, o melhor resultado do ponto de vista do tempo foi a execução 9, onde o processo todo levou 208,65 segundos para ser concluído. Já o pior cenário foi o observado na execução 7 onde o tempo empregado foi de 809,01 segundos.

De forma geral, observa-se que existe pouca variação entre os tempos medidos, onde somente um deles superou a barreira dos 800 segundos, estando os demais abaixo do limiar de 520 segundos. Como relatado anteriormente, uma das execuções alcançou tempos melhores, conseguindo finalizar a execução em 208 segundos. Estas informações mostram que o protótipo apresenta resultados consistentes e com pouca variação, sendo o maior gasto o de espera pelo bloco.

A Figura 3 apresenta uma análise do tempo médio para o processamento dos certificados individuais, conforme observado durante os experimentos. 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. Os resultados mostram que os limites identificados foram 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 260 segundos para atingirem o mesmo status.



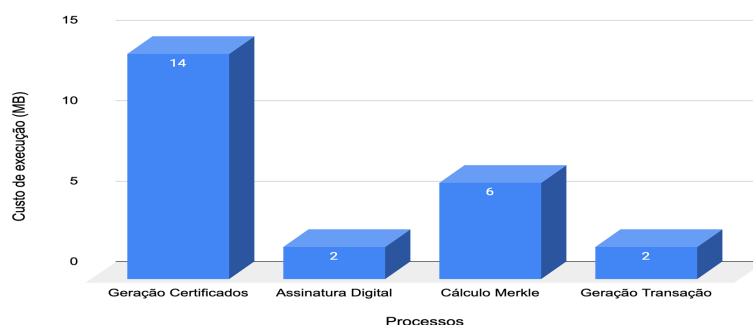
**Figura 3. Tempo de processamento individual dos certificados**

A Figura 4 apresenta o gasto médio de memória de cada um dos processos realizados, sendo estes: 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.

## 5. Conclusão

Este artigo apresentou e avaliou um protótipo do modelo UnivChain. Por meio de um caso de estudo e da análise de desempenho foi possível perceber que o protótipo consegue atender ao proposto como objetivo para o trabalho. É possível realizar a emissão de documentos acadêmicos, revogá-los e validá-lo de forma consistente, sem a necessi-





**Figura 4. Memória gasta no processamento de cada etapa**

dade de terceiros envolvidos no processo. Além disso, o aluno torna-se dono das suas informações acadêmicas, tendo liberdade para armazenamento e distribuição do arquivo.

Além disso, percebe-se que o modelo pode ser implementado com baixo custo do ponto de vista de hardware, podendo ser executado mesmo em servidores com baixa capacidade computacional. 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. O custo estimado com o uso de uma blockchain pública como a do Bitcoin é de US\$ 2.96<sup>4</sup>, o que equivale a US\$ 0.16 por diploma.

Com a execução do cenário de avaliação pode-se perceber que o modelo apresentado possui oportunidades de melhoria. Através de alterações na rede do usuário ou na máquina que executa as validações do documento, evitar que a consulta de revogação chegue ao servidor da entidade emissora. Neste cenário é possível inclusive forjar a resposta, levando a aplicação a acreditar que o documento está válido quando na verdade não foi possível checar a sua revogação.

Como trabalhos futuros, o UnivChain pode melhorar a forma como lida com as revogações de documentos pela universidade emissora, apresentando uma possível solução para o evidenciado no parágrafo anterior. Em termos de tempo de execução, é possível estudar alternativas para uma gravação mais rápida na blockchain. Por fim, o modelo pode ser expandido para suportar o novo padrão de diplomas digitais proposto pelo MEC em 2019<sup>5</sup>. Este padrão regulamenta o uso de arquivos XML<sup>6</sup> em formato específico e assinados digitalmente pela universidade. O suporte a estes arquivos é uma boa expansão do modelo UnivChain.

Finalizados os experimentos, é possível perceber pelo descrito anteriormente que o baixo consumo de recursos de memória aliado ao cumprimento dos objetivos proposto, torna o protótipo e o modelo viáveis. Outros ganhos apresentados como a emissão dos documentos em lotes, o baixo custo financeiro para emissão destes documentos e a re-

<sup>4</sup>Consultado em abril de 2020

<sup>5</sup><http://portal.mec.gov.br/diplomadigital/>

<sup>6</sup><https://www.w3.org/XML/>

siliência das informações armazenadas na blockchain, tornam o UnivChain um excelente candidato à solução de diplomação acadêmica.

## Agradecimentos

Este trabalho foi desenvolvido no contexto do projeto financiado pela FAPERGS, edital ARD 04/2019, termo 19/2551-0001340-0. Os autores também gostariam de agradecer à Capes e ao CNPq pelo suporte ao trabalho desenvolvido.

## Referências

- Arenas, R. and Fernandez, P. (2018). Credenceledger: A permissioned blockchain for verifiable academic credentials. In *IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC 2018)*, Stuttgart, Germany.
- Børresen, L. J., Meier, E., and Skjerven, S. A. (2020). *Corruption in Higher Education: Global Challenges and Responses*, volume 46, pages 102–107. Brill / Sense.
- Cheng, J.-C., Lee, N.-Y., Chi, C., and Chen, Y.-H. (2018). Blockchain and smart contract for digital certificate. In *IEEE International Conference on Applied System Invention (ICASI 2018)*, pages 1046–1051.
- Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., and de Colle, S. (2010). *Stakeholder Theory: The State of the Art*, pages 17–37. Cambridge University Press.
- Ghazali, O. and Saleh, O. S. (2018). A graduation certificate verification model via utilization of the blockchain technology. *Journal of Telecommunication, Electronic and Computer Engineering*, 10(3-2):29–34.
- Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S. S., and Stiller, B. (2019). The proposal of a blockchain-based architecture for transparent certificate handling. In *Business Information Systems Workshops (BIS 2018)*, volume 339, pages 185–196, Switzerland.
- Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., and Wendland, F. (2018). Blockchain for education: Lifelong learning passport. *Reports of the European Society for Socially Embedded Technologies*, 2(10):1–8.
- Han, M., Li, Z., He, J. S., Wu, D., Xie, Y., and Baba, A. (2018). A novel blockchain-based education records verification solution. In *19th Annual Conference on Information Technology Education (SIGITE 2018)*, pages 178–183, Fort Lauderdale, FL, USA.
- Huynh, T., Huynh, T., Pham, D., and Ngo, A. (2018). Issuing and verifying digital certificates with blockchain. In *International Conference on Advanced Technologies for Communications (ATC 2018)*, pages 332–336.
- Pooja and Yadav, M. (2018). Digital signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, 3(6):71–75.
- Singhal, A. and S. Pavithr, R. (2015). Degree certificate authentication using qr code and smartphone. *International Journal of Computer Applications*, 120:38–43.
- Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14:352.