# Utilização de blockchain para certificação de sistema de gestão de processos e documentos eletrônicos

**Thales Junior de Souza Gomes**[1], **Ewerton R. Andrade**[1]

[1]Grupo de Pesquisa em Segurança, Algoritmos, Computação e Inovação (SACI)
Departamento Acadêmico de Ciência da Computação (DACC)
Fundação Universidade Federal de Rondônia (UNIR)
Porto Velho/RO – Brasil.

thales3238junior@gmail.com, ewerton.andrade@unir.br

***Resumo.*** *A utilização de sistemas de gestão de processos e documentos eletrônicos é uma realidade. Contudo, na maioria das vezes, esses sistemas baseiam-se em modelos centralizados, onde seus administradores possuem privilégios elevados. Neste sentido, este trabalho busca desenvolver uma blockchain com API padronizada e integrável; visando coibir ataques de gestores mal intencionados e descentralizar o armazenamento e manipulação dos processos e documentos eletrônicos, porém, mantendo as proteções de cada sistema e adicionando novos mecanismos de segurança. Para demonstrar a viabilidade da proposta, desenvolveu-se uma blockchain privada, utilizando-se uma API-REST com todas funcionalidades necessárias para realizar as transações.*

## 1. Introdução

Com o crescente aumento na produção de informações, os documentos "tradicionais", normalmente disponibilizados em papel, não atendem mais às necessidades de agilidade na circulação das informações; sendo evidentes suas limitações no que se refere à simples conservação, capacidade de transmissão e segurança [Gandini et al. 2002].

De fato, ao longo dos últimos anos, identifica-se uma forte tendência de que o uso de documentos em papel seja substituído por documentos eletrônicos. Neste sentido, as organizações tendem a aderir cada vez mais as tecnologias relacionadas aos documentos eletrônicos seguros [Leal and De Rolt 2013].

Assim, para arquivar documentos, principalmente aqueles que registram fatos que necessitam de comprovações e garantias, são realizadas certificações digitais utilizando criptografia e sistemas de segurança que garantam que determinado documento é válido [Correa et al. 2018]. Sendo que a certificação digital é a tecnologia que busca prover os mecanismos de segurança capazes de propiciar uma gestão documental de qualidade, pois ela fornecerá serviços de confidencialidade, autenticidade e integridade aos documentos nas trocas eletrônicas de informação [Correa et al. 2018].

No Brasil, este arquivamento e manuseio de documentos digitais vem se popularizando pela utilização de sistemas como o sistema de Gestão online de conteúdo e-Clic [e-Clic 2020], e, especialmente, o Sistema Eletrônico de Informações – SEI [TRF4 2020], que é utilizado na maioria das instituições públicas do país.

Todavia, usualmente estes sistemas baseiam-se em um modelo centralizado, onde um único ponto da rede (servidor) é responsável por armazenar todos documentos, e seus administradores possuem privilégios elevados quanto ao acesso a estas informações.

Desta forma, caso este ponto central seja atacado ou mal utilizado, poderão ocorrer problemas de segurança que comprometam a auditabilidade ou promovam a exclusão, adulteração ou inserção de documentos; principalmente se o ataque partir de um usuário com privilégios elevados. Apesar de parecer conservador, proteger-se de administradores do sistema vem se tornando prática cada vez mais recomendada, uma vez que a literatura especializada indica que um número substancial de falhas de segurança são causadas por este tipo de atacante [Verizon 2019].

Existem diversas abordagens para proteger-se deste tipo de vulnerabilidade em sistemas deste tipo, contudo, por não necessitar de grandes alterações nos sistemas já existentes, acredita-se que a utilização de uma blockchain (ou cadeia de blocos) com uma API padronizada (*Application Programming Interface*) seja a abordagem mais adequada devido sua versatilidade, praticidade e, sobretudo, segurança [Do and Ng 2017].

Isto porque a blockchain é um ambiente seguro para registro de transações de qualquer natureza, sejam transações financeiras, registros genéricos ou tipos de dados abstratos, uma vez que não há exclusão e nem modificação dos registros já realizados. Além disso, qualquer cadeia de blocos é mantida simultaneamente por todos os nós da rede, não existindo local principal ou preferencial para armazenamento de uma base de dados original. Com isto, todo nó tem a sua réplica da base de dados, e todas elas são mantidas íntegras, consistentes e sincronizadas pelos protocolos de consenso [Braga et al. 2017]. Logo, não há a possibilidade de exclusão, adulteração ou inserção de documentos, e a auditabilidade sempre será mantida.

### 1.1. Objetivo deste trabalho

Neste contexto, este trabalho busca desenvolver uma blockchain com API padronizada, para comunicação com qualquer sistema de gestão de processos e documentos eletrônicos que realize requisições no formato JSON (*JavaScript Object Notation*).

## 2. Descrição do método e da solução proposta

Levando em consideração as características tecnológicas, principalmente quanto às blockchains e sua eficiência, optou-se pelo desenvolvimento de uma Blockchain Privada sem a utilização de nenhum framework de blockchains. A não utilização de um framework nos deu a possibilidade de planejar e configurar todos os detalhes da blockchain, desta forma, temos um domínio maior para planejar a escalabilidade da rede, além disso, aplicado aos órgãos públicos, não é interessante depender de um componente externo dentro da aplicação. Conjecturou-se que desta forma seja possível adaptar a rede blockchain proposta ao sistema de processos e documentos eletrônicos atualmente utilizado na Universidade Federal de Rondônia (o Sistema Eletrônico de Informações – SEI), para que, assim, o usuário final não sofra nenhum impacto negativo no processo de migração/implantação.

Quanto ao processo de engenharia de software, destaca-se que foram utilizados Diagramas UML (*Unified Modeling Language*) para modelagem e estruturação do sistema, e Metodologias Ágeis para o desenvolvimento do software.

### 2.1. Prova de conceito desenvolvida e discussões relacionadas

Para desenvolvimento da prova de conceito, foi utilizado como modelo de estudo de viabilidade o Núcleo de Tecnologia da Fundação Universidade Federal de Rondônia e seus departamentos associados: Departamento Acadêmico de Ciência da Computação (DACC),

Departamento Acadêmico de Engenharia Civil (DECIV) e Departamento Acadêmico de Engenharia Elétrica (DEE). Formando, assim, uma rede privada de 4 (quatro) nós em uma blockchain. Resumidamente, desenvolveu-se esta rede composta por 4 (quatro) nós em que todos possuem conexões entre si, o que possibilita a transferência de dados de forma direta e sem uma autoridade central. Assim, é possível estabelecer uma rede de transações P2P (*Peer-to-Peer*) em que tem todos os nós participam da rede como certificadores e mantenedores dos processos e documentos eletrônicos.

Em em cenário real, estes nós poderiam ser diferentes instituições (*e.g.*, outras universidade, institutos, tribunais, etc...), com diferentes sistemas de gestão de processos e documentos eletrônicos; bastando que eles se comuniquem através da API criada. Desta forma, cada instituição funcionaria como um validador dos documentos registrados na rede, funcionando como uma grande estrutura confederada de sistema de gestão de processos e documentos eletrônicos. Destaca-se aqui, que como em qualquer blockchain, um nó não poderá alterar ou excluir o documento inserido por terceiro, contudo, agirá como validador de cada informação contida na rede.

Tratando especificamente do software desenvolvido, utilizou-se a linguagem Python 3.7 em conjunto com o microframework Flask 1.1.2, e as bibliotecas UUID4, PyPDF2 e hashlib, fazendo uso do algoritmo criptográfico SHA256, além de HTML5 e o framework Bootstrap. Além disso, como o SEI da Universidade Federal de Rondônia ainda não pode ser adaptado para comunicar-se com a solução desenvolvida neste trabalho, desenvolveu-se uma página web simulando um sistema básico de envio de processos e documentos eletrônicos.

Através desta página, ou qualquer outra aplicação que se comunique utilizando a API padronizada, cada nó participante poderá enviar um novo documento, que por sua vez passará a constar na rede como uma nova transação. Em seguida, após sua confirmação, será adicionada a um bloco em construção. E por fim, após o bloco receber um número determinado de transações, ele será minerado e propagado por toda rede.

### 2.2. Estruturas de dados utilizadas

Para formar a rede com conexão P2P(*Peer-to-Peer*), são cadastrados em cada nó da rede uma lista com o endereço de IP (*Internet Protocol*) de todos os nós participantes da rede.

Conforme abordado anteriormente, a cada documento adicionado é criada uma transação, em seguida, estas transações são armazenadas em uma lista que se mantêm atualizada em todos os nós (lista de documentos não minerados). Para garantir a integridade e a busca de um documento, todas transações possuem as informações necessárias para sua certificação (como o seu hash e informações do usuário). Um exemplo desta lista de documentos (transações) pode ser observada na Figura 1.

Tratando especificamente da lista de transações, têm-se que cada atributo do objeto JSON significa: *document*: hash criptográfico do documento transacionado; *id*: código identificador único do usuário que cadastrou o documento ou processo; *index*: índice da transação na lista; *name*: nome do usuário que realizou a transação; *node address*: identificador único universal do nó que realizou a transação, gerado pela biblioteca UUID4; *process*: número do processo correspondente ao documento; *receiver*: nó responsável pelo recebimento do documento; *sender*: nó responsável pelo envio do documento; *timestamp*: carimbo de tempo da transação.

```
{ "length": 2,
  "transactions": [ {
     "document": "8ee37a9ae5c6cdc03acd6ab0234d0737e03f88e221d6bed4e0677be4a4b1155c",
     "id": "34442",
     "index": 1,
     "name": "Ada Lovelace",
     "node_address": "0e9c5531-e6aa-42ea-bb34-f312cb69b8bb",
     "process": "33334",
     "receiver": "DEE",
     "sender": "NT",
     "timestamp": "2020-06-18 15:39:00.147613" },
    { "document": "0bf272944fdd23bc52ea809570f1539d5d6413196f19de4bfdc14d6bd53250b4",
     "id": "34442",
     "index": 2,
     "name": "Noam Chomsky",
     "node_address": "cd5aa021-917f-412b-87b3-237c44b3f5d6",
     "process": "33334",
     "receiver": "DACC",
     "sender": "DECIV",
     "timestamp": "2020-06-18 15:40:27.680481" } ] }
```


**Figura 1. Exemplo de estrutura contendo a lista de documentos enviados para a rede da blockchain (transações não mineradas).**

É importante destacar que, assim como nas requisições, as transações, blocos e demais estruturas da blockchain são representadas como dados em formato JSON. Pois, com este formato, a leitura dos dados é simplificada em todos os níveis, inclusive em possíveis auditorias realizadas por humanos. Além disso, vale destacar que, apesar da possível sobrecarga que a utilização destas estruturas pode trazer, existem diversas estratégias e bibliotecas para aprimorar o seu desempenho [Vanura and Kriz 2018].

No processo da adição de uma nova transação, o nó responsável pelo envio do documento tem que verificar se um novo bloco deve ser minerado, se não for necessário, a transação entrará em processo de propagação, para que a lista de transações seja atualizada. Porém, caso seja necessário, o algoritmo de consenso é executado até que seja encontrado um número único (*i.e.*, o NONCE) e o bloco seja adicionado a blockchain.

Na prova de conceito, por se tratar de uma blockchain privada onde somente instituições ou departamentos pré autorizados participam, a dificuldade do *Proof of Work* (PoW) foi definida como mínima para não haver desperdício de poder computacional ao se realizar estas operações. É importante esclarecer que, a escolha algoritmo de consenso deste trabalho baseou-se na abrangência, diversidade e segurança das aplicações que o método PoW é utilizado atualmente; assim, obtêm-se uma maior facilidade de entendimento e integração no processo de construção da blockchain para a prova de conceito.

A verificação para saber se um novo bloco deve ser minerado ocorre com a verificação da quantidade de transações na lista; ficando definida como 2 (dois) o número de transações por bloco nesta primeira versão da prova de conceito. Desta forma, têm-se o controle exato de quantas transações cada bloco possui. Além disso, ressalta-se que a pequena quantidade de transações por bloco é proposital, pois desta forma a criação de blocos se torna praticamente constante e sem tempo de espera.

Tratando de outra estrutura da blockchain, na Figura 2 está representado o bloco gênesis (primeiro bloco gerado) da blockchain, onde hash apresentado nele corresponde a uma frase de Thomas Edison - *"Eu aprendi muito mais com meus erros do que com meus acertos"*. Como ocorre em toda blockchain, este bloco não possui transações, pois é gerado automaticamente pela estrutura da rede, para representar o início da sua utilização.

Agora, tratando especificamente dos blocos, têm-se que cada atributo do objeto JSON significa: *hash*: hash criptográfico do bloco; *index*: índice do bloco na blockchain; *node address*: identificador único universal do nó que realizou a transação, gerado pela

```
{"chain": [  {
        "hash": "95ac5b008aaffb00537f7a3cdc11eeec65dc2aa7db83bfcea26901f4ad7537c3",
        "index": 1,
        "node_address": "bdfe0e4e-6cdb-434c-ad7c-8fc6ae16b51b",
        "nonce": 0,
        "previous_hash": "0",
        "timestamp": "2020-06-18 15:42:30.698149",
        "transactions": []
      } ], "length": 1  }
```


**Figura 2. Conteúdo do bloco gênesis.**

biblioteca UUID4; *nonce*: é uma abreviação de "*number only used once*", refere-se ao número que um minerador da blockchain precisa descobrir antes de criar um novo bloco; *previous hash*: hash de ligação do bloco com o seu bloco antecessor. (O bloco gênesis possui previous hash = "0" por ser o bloco inicial); *timestamp*: carimbo de tempo da criação do bloco; *transactions*: lista de transações pertencente ao bloco (o bloco gênesis possui a lista de transações vazia por ser o bloco inicial).

Diferentemente do bloco gênesis, todos os demais blocos posteriores possuirão dados como: o hash do antecessor (*previous hash*); os dados do nó que realizou a sua mineração; e os dados de cada transação armazenada e certificada pelo bloco.

## 3. Resultados

O desenvolvimento deste trabalho focou na implementação de uma blockchain que responda a requisições de uma API REST (*REpresentational State Transfer*). Com esta abordagem, foi possível criar uma prova de conceito por meio da utilização de um sistema web simples para realizar tais requisições. Assim, além de mostrar a viabilidade da solução, também foi possível evidenciar sua interoperabilidade com sistemas de gestão de processos e documentos eletrônicos já existentes, desde que eles realizem requisições no formato estabelecido.

Além das características próprias do trabalho desenvolvido, vale destacar novamente algumas vantagens do armazenamento de documentos em uma blockchain. Vantagens como: disponibilidade, integridade, armazenamento confiável, e outras características positivas inerentes a tecnologia. Por outro lado, não se pode deixar de citar possíveis desvantagens, como: redundância desnecessária, sobrecarga na rede e ineficiência nos mecanismos de busca. Contudo, ressalta-se que tais desvantagens podem ser contornadas com abordagens mais modernas para o armazenamento de documentos em blockchain [Do and Ng 2017], sistemas de arquivos distribuídos em rede mais eficientes [Huang et al. 2013], e gerenciadores e indexadores de busca mais adequados as tecnologias utilizadas [Truica et al. 2013]. Apesar de não ser trivial, estas modificações podem ser vistas como importantes aprimoramentos e próximos passos.

Outro aspecto que pode causar preocupação em usuários menos habituados com a tecnologia blockchain é o fato de terceiros possuírem acesso a seus documentos. Todavia, o fato de cada nó possuir uma cópia dos documentos enviados a rede não incorre em quebra de sigilo, uma vez que todo documento "privado" ou "restrito" pode ser cifrado antes de ser enviado a blockchain através de JSONs. Desta forma, a rede armazenará os bytes do arquivo protegido, não sendo possível a nenhum nó da rede decifrá-lo sem o conhecimento da chave correta. Logo, vale destacar que esta funcionalidade também encontra-se desenvolvida na prova de conceito implementada.

Por fim, infere-se que a utilização de uma blockchain integrada a sistema de gestão

de processos e documentos eletrônicos fornece uma "camada extra" de proteção, adicionando mecanismos de segurança contra administradores de sistema mal intencionados. Possibilitando, assim, que as informações permaneçam íntegras, autênticas, imutáveis, irretratáveis e auditáveis.

## 4. Considerações Finais

A principal contribuição desse trabalho foi desenvolver uma blockchain com API padronizada e integrável a sistemas de gestão de processos e documentos eletrônicos que realizem requisições utilizando JSON. Destaca-se que, para validação da solução, criou-se um sistema web para comunicação simulada e realização de testes, deixando de forma clara que as implementações desenvolvidas foram utilizadas apenas para prova de conceito. Além disso, por se tratar de um extrato de um Trabalho de Conclusão de Curso (TCC), frisa-se que todo levantamento conceitual e metodológico possibilitou o entendimento da viabilidade para utilizar-se blockchain na certificação de processos e documentos.

Todavia, em virtude de alguns aspectos inerentes a tecnologia utilizada, acredita-se que este trabalho possa ser continuado integrando-se o sistema de gestão de processos e documentos eletrônicos utilizado na Universidade; através de adaptações nativas ou criando-se extensões para navegadores web. Ou, ainda, realizando-se testes de desempenho, escalabilidade e sobrecarga, para propositura de eventuais otimizações.

## Referências


Braga, A., Marino, F., and dos Santos, R. (2017). Segurança de aplicaçoes blockchain além das criptomoedas. *Livro-texto dos minicursos SBSeg*, pages 99–148.

Correa, O. A. et al. (2018). Estudo da aplicação de estrutura blockchain com proof of stake para arquivamento de documentos com registro no tempo. *TCC – UFSC*.

Do, H. G. and Ng, W. K. (2017). Blockchain-based system for secure data storage with private keyword search. In *2017 IEEE World Congress on Services (SERVICES)*.

e-Clic (2020). Gestão online de conteúdo e-Clic. `https://www.e-clic.net`.

Gandini, J. A. D., Salomão, D. P. d. S., and Jacob, C. B. (2002). A segurança dos documentos digitais. *Ajuris*.

Huang, C., Hu, W., Chia-Chun Shih, Bo-Ting Lin, and Chien-Wei Cheng (2013). The improvement of auto-scaling mechanism for distributed database - A case study for MongoDB. In *15th Asia-Pacific Network Operations and Management Symposium*.

Leal, K. A. F. and De Rolt, C. R. (2013). Impactos para adoção de documento eletrônico seguro nas transações de compras eletrônicas.

TRF4 (2020). Sistema Eletrônico de Informações. `https://www.trf4.jus.br/`.

Truica, C.-O., Boicea, A., and Trifan, I. (2013). CRUD Operations in MongoDB. In *Proceedings of ICACSEI 2013*, pages 347–350. Atlantis Press.

Vanura, J. and Kriz, P. (2018). Perfomance Evaluation of Java, JavaScript and PHP Serialization Libraries for XML, JSON and Binary Formats. In Ferreira, J. E., Spanoudakis, G., Ma, Y., and Zhang, L.-J., editors, *SCC 2018*, Cham. Springer.

Verizon (2019). 2019 data breach investigations report. Technical report, Verizon – Business ready. `https://vz.to/2RuRHNU`.