Associação Propagadora Esdeva
Centro Universitário Academia – UniAcademia
Curso de Sistemas de Informação
Trabalho de Conclusão de Curso – Artigo

ANÁLISE DO USO DA TECNOLOGIA BLOCKCHAIN NA VALIDAÇÃO DE DIPLOMAS UNIVERSITÁRIOS

Lucas Pinto Monteiro Guimarães[1]
Centro Universitário Academia, Juiz de Fora, MG
Romualdo Monteiro de Resende Costa [2]
Centro Universitário Academia, Juiz de Fora, MG

Linha de Pesquisa: Redes de Computadores e Sistemas Distribuídos

RESUMO

Com o desenvolvimento de novas tecnologias surgem também novos desafios em relação a segurança das inúmeras informações que são geradas constantemente. Este trabalho tem por objetivo investigar como a tecnologia *blockchain* poderia contribuir com uma maior segurança na emissão de diplomas digitais pelas Instituições de Ensino Superior no Brasil. Para isso, foi realizada uma pesquisa bibliográfica para compreender o funcionamento de uma rede *blockchain* e o nível de segurança fornecido por ela. Como resultado, foi escolhida a plataforma EOSIO como uma ferramenta que permite a criação de aplicações descentralizadas. Através disso, este trabalho propõe a criação de uma aplicação que permite a inclusão de um diploma digital na rede *blockchain* EOSIO.

Palavras-chave: Blockchain. Bitcoin. Diploma digital. Ensino superior. EOSIO.

[1] Discente do Curso de Sistemas de Informação do Centro Universitário Academia – UniAcademia. Endereço: Rua Oscar Vidal 459. Centro. Celular: (32)99963-1012. E-mail: lpguimaraes@yahoo.com
[2] Docente do Curso de Sistemas de Informação do Centro Universitário Academia. Orientador.

1 INTRODUÇÃO

Em 2008, um artigo intitulado **Bitcoin: um sistema de dinheiro eletrônico ponto-a-ponto**, escrito por um autor sob o pseudônimo de Satoshi Nakamoto, lança a primeira criptomoeda, o Bitcoin. Nesse artigo, Nakamoto explica como funciona a tecnologia responsável pela segurança no fluxo de armazenamento e troca de dados da moeda, que permitiria transações entre seus usuários sem a necessidade do intermédio de uma entidade central para validar o processo. Nakamoto criou a tecnologia Servidor *Timestamp* (NAKAMOTO, 2008), o que veio a se tornar a *blockchain*, ou cadeia de blocos. Apesar de nascerem juntos, *Bitcoin* e *blockchain* não são a mesma coisa. A *blockchain* é uma tecnologia que fornece os meios necessários para gravar e armazenar transações da criptomoeda *Bitcoin* e esse foi o primeiro caso de uso da arquitetura de *software blockchain*.

Ao longo dos anos, essa tecnologia foi ganhando espaço e sendo aplicada em diversas situações. Um bom exemplo da sua utilização é na validação de diplomas, devido às suas propriedades de segurança e transparência. Os diplomas são usados como um mecanismo de sinalização, apresentando que o indivíduo portador concluiu uma etapa de ensino e agora detém o conhecimento e habilidades de uma determinada área. O diploma se torna muito menos eficiente quando é custoso distinguir o legítimo do fraudulento, como acontece com os diplomas emitidos fisicamente, em papel. Como resultado desse problema, existem casos onde empregadores precisam consultar universidades para que sejam verificados se os diplomas recebidos são legais. Essa verificação pode gerar um processo burocrático resultando em uma carga administrativa extra para as universidades e empregadores.

Nesse contexto, este trabalho tem por objetivo apresentar a *blockchain* como uma possível solução para o problema citado. Para tal, é utilizada a plataforma EOSIO[3], um *software* que introduz uma arquitetura *blockchain* com os recursos necessários para que seja desenvolvido um aplicativo de validação segura de diplomas.

Na seção dois será descrito brevemente o histórico e uma análise geral das principais tecnologias presente nas criptomoedas, seguida pela implementação

[3] https://eos.io/

propriamente dita. Por fim, a última seção estabelece as conclusões e os possíveis trabalhos futuros.

2 BLOCKCHAIN

Em uma lista de discussão de criptografia, Satoshi Nakamoto publicou uma mensagem anunciando sua grande criação, a criptomoeda Bitcoin. Nakamoto surge com uma solução tecnológica que oferece uma maneira de se realizar transações financeiras sem nenhuma autoridade centralizadora, uma tecnologia que se sustenta nos usuários para prover a força computacional para realizar as transações de forma segura.

Vale lembrar que no mesmo ano uma crise financeira assolava a economia mundial. Tal crise foi desencadeada justamente pela quebra de um sistema de crédito baseado em instituições centralizadoras, os bancos. A crise econômica de 2008 teve início nos Estados Unidos, que mantinha uma política de crédito que permitia ampla especulação da população no mercado imobiliário. Financiada pelos bancos, a população se endividava perigosamente até não conseguir quitar as dívidas, levando os bancos à falência. É simbólico que o marco da crise econômica de 2008 seja a quebra do banco americano Lehmann Brothers, mesmo sendo centenário e um dos bancos mais fortes e tradicionais dos EUA (EXAME, 2018) foi vítima da falha financeira de um sistema monetário centralizado.

O que chama a atenção no artigo de Nakamoto é o alicerce do *Bitcoin*, a *blockchain* que, apesar de ser um termo novo, é uma combinação de conceitos já estudados e aplicados pela ciência da computação (Internet, criptografia de chaves e protocolo). Pode-se entender a *blockchain* como uma base de dados de transações distribuídas e compartilhada pelos usuários de um sistema organizado como uma rede *peer-to-peer* (P2P) (Nakamoto, 2008). Nessa rede, cada transação é verificada e validada por um consenso baseado na prova de trabalho. O funcionamento da *blockchain* será discutido na subseção seguinte, onde também é apresentado o conceito de mineração, responsável pela validação da rede.

2.1 MINERAÇÃO

Todas as transações que ocorrem na rede em um determinado espaço de tempo são armazenadas em blocos de dados e, cada novo bloco tem de ser validado para

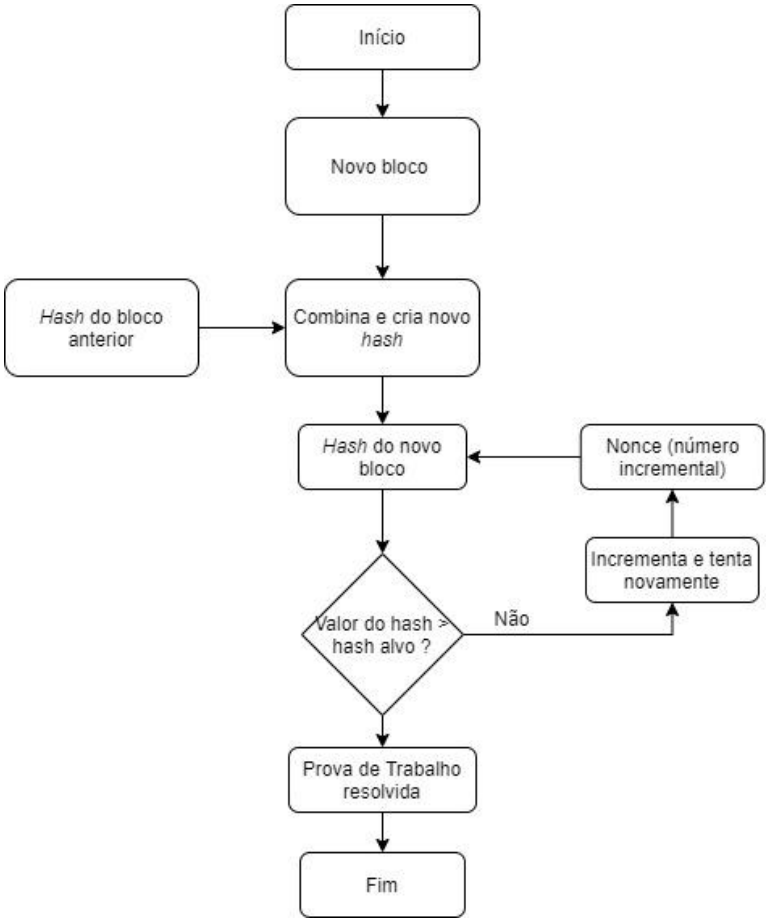
ser considerado como válido e, de fato, fazer parte da cadeia. Essa validação ficou popularmente conhecida como mineração. Um nó (usuário) minerador tem a responsabilidade de autenticar o conteúdo das transações que aguardam em fila para serem incluídas em um bloco e realizar o processo da mineração, que é a maneira em que novos blocos são descobertos. Quando um novo bloco é validado por um minerador, esse bloco é adicionado à rede e todos os nós são atualizados para receber os novos valores, garantindo a sua integridade. Isso garante que nenhum bloco possa ser forjado e adicionado no meio da rede sem que seja imediatamente percebido pelos demais.

Cada nó, mencionado anteriormente, nada mais é do que um usuário conectado à *blockchain*. Os nós guardam uma cópia do registro de todas as transações que já ocorreram na rede. Esse sistema pode ser comparado a um livro-razão, um registro que tem a finalidade de coletar dados cronológicos de todas as transações ocorridas, fornecendo um histórico detalhado de cada transação.

Esse processo de descoberta de um novo bloco que sustenta o consenso por entre a rede se dá através de um algoritmo de prova de trabalho (POW - *Proof of Work*) (NAKAMOTO, 2008). A prova de trabalho é realizada através da busca pelo número aleatório *nonce*[4] até que o *hash* (sequência de bits gerada por um algoritmo) do bloco tenha a quantidade necessária de bits zero. Ou seja, é trabalho do minerador ir incrementando o *nonce* até que se chegue no valor *hash* alvo definido pelo algoritmo do sistema. A Figura 1 exemplifica o processo:

[4] https://en.wikipedia.org/wiki/Cryptographic_nonce

FIGURA 1: Prova de Trabalho.



Fonte: Do Autor (2020)

O valor *hash* do bloco recém minerado é inserido nos dados do bloco subsequente, como apresentado na Figura 1 e, então, todo o processo se repete. Uma vez que um esforço de CPU foi despendido para satisfazer a prova de trabalho, um dado de um bloco não pode ser alterado sem que todo o trabalho seja refeito nele e em todos blocos subsequentes.

Apesar de o mecanismo citado ter revolucionado a maneira com que a troca de informação pode ser feita na Internet, críticos contestam que uns dos problemas gerados por esse mecanismo, vem da demanda de um grande poder computacional necessário para resolver o desafio matemático na criação de novos blocos. Isso faz com que os mineiros que possuem mais *hardware* trabalhando paralelamente detenham mais poder de mineração, além de ainda causar um excessivo consumo de energia elétrica no processo (ALIAGA; HENRIQUES, 2017).

2.2 CONTRATOS INTELIGENTES (SMART CONTRACTS)

Com a ideia de se utilizar da segurança provida pela *blockchain* na elaboração de protocolos mais complexos, indo além do fechado sistema de transações do *Bitcoin*, surgiu a segunda geração de criptomoedas e outras tecnologias. Por exemplo, a possibilidade de explorar conceitos tais como o de contrato inteligente (SZABO, 1994) funcionando dentro da *blockchain*. Que é o que guia a ideia deste trabalho.

No contexto da *blockchain*, os contratos inteligentes funcionam como aplicativos de *software* incorporados à rede que não requerem, necessariamente, de intervenção humana para completar a sua execução. De acordo com Tavares e Teixeira (2018) o funcionamento dos contratos inteligentes é dividido em três etapas. Essas etapas envolvem a codificação do contrato, onde as instruções de execução são estabelecidas, o envio à *blockchain*, que armazena o contrato na rede onde todos os nós da rede têm acesso, e a execução dos contratos por computadores conectados à rede. Os registros do contrato são atualizados com os resultados das execuções.

Essa forma de desenvolvimento de um contrato oferece uma alta confiabilidade e segurança para a validação de diplomas, pois, depois que o código já se encontra em um estado distribuído e descentralizado, não há como controlar sua execução, evitando processos fraudulentos. Igualmente, se torna impossível alterar os resultados da execução do mesmo, já que estão registradas nos blocos da *blockchain*.

A seguir, serão apresentadas as plataformas Ethereum[5], a primeira plataforma de sucesso a possibilitar o desenvolvimento de aplicativos descentralizados e, seguidamente, a plataforma escolhida para este trabalho, a EOSIO.

2.3 ETHEREUM E EOSIO

Atualmente, ocupando o posto de segunda maior rede de *blockchain,* a tecnologia de código aberto Ethereum foi a primeira que surgiu com o objetivo de fornecer uma plataforma de desenvolvimento em *blockchain* generalizada, combinando as noções de consenso do *Bitcoin* com o potencial abstrativo de uma linguagem de

[5] https://ethereum.org/pt-br/

programação alto nível, conhecida como *Solidity*[6]. Dessa forma, foi possível aos desenvolvedores programar aplicações descentralizadas facilmente, sem que fosse necessária a criação de uma nova *blockchain* para cada nova aplicação.

Uma desvantagem da Ethereum são as altas taxas de transação que afetam a rede como um todo. Diferentes aplicações desenvolvidas são impactadas com o mesmo valor de taxa. Um exemplo ocorreu em 2017, com a ampla utilização de um jogo desenvolvido na rede Ethereum denominado *CryptoKitties*[7]. A alta popularidade do jogo ocupou cerca de 10% do tráfego de rede (BBC, 2017). Isto elevou o valor da taxa para todos os usuários, e demonstrou a maior fraqueza da rede, uma escalabilidade insatisfatória.

Como opção, a EOSIO surgiu em 2017 com a proposta de uma nova arquitetura *blockchain* que consegue escalar para até milhões de transações por segundo, proporcionando um tempo menor na confirmação de produção de blocos. Segundo seu criador Larimer (2018), as plataformas *blockchains* existentes enfrentam dificuldades para suportar aplicações descentralizadas funcionais, sendo sobrecarregadas por altas taxas de transações e capacidade computacional limitada, que impedem a adoção em massa da tecnologia *blockchain*. Afirma ainda que, para que essa disseminação seja alcançada, aplicações em *blockchain* necessitam de uma plataforma flexível suficiente para que seja possível atender alguns requisitos básicos que garantem o sucesso de uma aplicação. Tais requisitos como o suporte a milhões de usuários simultâneos combinado com uma baixa latência e o uso gratuito de aplicações, são essenciais para que qualquer aplicação em *blockchain* consiga competir com empresas como por exemplo a Uber[8], Airbnb[9], Facebook[10], Instagram e outros.

Diferentemente da Ethereum, que cobra taxas do usuário para transações em sua rede, a EOS se baseia em um modelo de propriedade, ou seja, o desenvolvedor, através de *tokens* (moedas) adquiridos, se torna dono dos recursos que irá usufruir no processo de desenvolvimento, eliminando a necessidade do usuário final pagar taxas por estar utilizando o serviço. Na Figura 2 é mostrada uma comparação de

---

[6] https://solidity.readthedocs.io/en/v0.6.9/
[7] https://www.cryptokitties.co/
[8] https://www.uber.com/br/pt-br/
[9] https://www.airbnb.com.br/
[10] https://www.facebook.com/

escalabilidade entre algumas *blockchains* existentes atualmente, exibindo a EOSIO em primeiro lugar.

FIGURA 2: Comparação da escalabilidade entre as plataformas.

#	Symbol	Activity 24h	Transaction 24h
1	EOS	76.111.638 Op	3.862.106 Tx
2	TLOS	4.510.899 Op	511.376 Tx
3	XLM	1.750.491 Op	- Tx
4	TRX	1.641.365 Op	1.641.365 Tx
5	KIN	1.413.096 Op	- Tx
6	IOST	1.373.760 Op	1.373.760 Tx
7	ETH	895.324 Op	895.324 Tx
8	BSV	888.251 Op	713.448 Tx
9	BTC	802.673 Op	308.717 Tx

Fonte: Blocktivity (2020)

A coluna *Activity* da Figura 2 exibe a quantidade de transações realizadas em um período de 24 horas. A EOSIO exibe um número de 76.111.638 de transações neste período enquanto a Ethereum realizou 895.324.

2.4 DIPLOMAS DIGITAIS EM BLOCKCHAIN

No Brasil, ao se concluir um curso superior em uma instituição de ensino regulamentada, o aluno tem direito a receber sua certificação, um documento que comprova que uma etapa de sua formação foi finalizada, portanto, tem plena capacidade de exercer sua profissão em todo território nacional. O processo de emissão de diplomas no Brasil fica a cargo da IES, sendo necessário que o respectivo curso seja reconhecido pelo Ministério da Educação (MEC) (BRASIL, 1996), então, emitido o diploma cabe à IES assegurar a sua regularidade.

Ainda que exista todo o controle mencionado na emissão de um diploma, é notória a ineficiência que ainda existe na verificação da autenticidade do mesmo. Casos de uso de diplomas falsos sendo utilizados não são raros. Um exemplo, o

jornal Globo (2013) noticiou um caso de esquema de revalidação de diplomas de medicina no Mato Grosso, onde foram apreendidas 41 pessoas que nem sequer haviam sido alunos do curso.

Em 10 de dezembro de 2019 o MEC anunciou o início da certificação digital no Brasil, que deverá ser implementada nas Instituições de Ensino Superior (IES), privadas e públicas, até o final de 2021. Com o intuito de reduzir as falsificações e possibilitar um fácil acesso pelos alunos, IES, empresas e órgãos governamentais poderiam validar a legitimidade e integridade dos documentos através da Internet. Além disso, para as IES, o diploma digital traz benefícios na redução de custos e riscos, redução da burocracia que envolve a expedição e registro dos documentos, desde o transporte até a entrega para os formandos.

Segundo a nota técnica Nº 13/2019/DIFES/SESU/SESU do Ministério da Educação (2019), as IES ao adotarem o meio digital para expedição de diplomas deverão atender às diretrizes de certificação digital do padrão da infraestrutura de Chaves Públicas Brasileira ICP-Brasil[11]. Essa mesma nota afirma que a utilização da assinatura com certificação digital e carimbo do tempo (*timestamp*) garantem a presunção de integridade, autenticidade e validade dos documentos eletrônicos.

É de se notar semelhanças da nota técnica com o que vem sendo discutindo neste trabalho em relação à *blockchain*. Ambas utilizam de carimbo de tempo *timestamp* e criptografia assimétrica. Porém, há problemáticas acerca da preservação de conteúdo digital que devem ser atentadas.

Apesar de o diploma digital apresentar vantajosas características em contraponto ao diploma físico, preservar um conteúdo digital faz surgir desafios que, até então, não eram enfrentados pelo modo tradicional. Uma alternativa segura de se preservar uma informação é distribuí-la em diversas cópias de conteúdo digital, como servidores (FARIAS; ARAÚJO; EVANGELISTA, 2017). Pensando em uma única IES, se torna infactível que a mesma tenha a infraestrutura computacional necessária, com servidores distribuídos geograficamente e, principalmente, investimentos para operar da forma adequada.

Com isso, surge a alternativa proposta por este trabalho de utilizar diplomas digitais em *blockchain* visto que, segundo Smolenski (2016) a tecnologia *blockchain* é

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

uma infraestrutura ideal para proteger, compartilhar e verificar conquistas adquiridas. Diplomas em uma rede *blockchain* fornecem ao aluno uma credencial segura, assinada por criptografia e descentralizada.

Para tornar possível o desenvolvimento de uma aplicação que permita a criação de um contrato digital em forma de um *smart contract* e, inserir em uma rede *blockchain*, será utilizada a plataforma mencionada anteriormente, a EOSIO. Em uma *blockchain* EOSIO, uma conta identifica um participante da rede, sendo esse participante um indivíduo ou um grupo, e representa também os atores dos contratos, que enviam e recebem ações de outros usuários da rede. Ações que sempre estão contidas nas transações. Teoricamente, uma conta no EOSIO é uma coleção de autorizações guardadas em uma *blockchain*, um par de chaves.

Para que seja possível realizar qualquer transação na EOSIO, é necessária a criação de uma carteira de chaves e em seguida associá-la a uma conta. A aplicação desenvolvida necessita de, no mínimo, duas contas para que seja feito o fluxo complexo de emissão de um diploma. Uma conta da IES, que terá a permissão de interagir com o contrato por meio de ações e incluir um diploma na rede *blockchain*, utilizando-se da chave pública do aluno e uma conta de aluno que irá consultar o contrato. O fluxo desse processo pode ser visto na Figura 3:

FIGURA 3: Fluxo de emissão do diploma em *blockchain* EOSIO.

Fonte: Do Autor (2020)

Na seção seguinte será apresentado como ocorre a emissão do diploma pela IES ocorre e como os usuários na rede podem interagir com o diploma.

3 **METODOLOGIA**

Na elaboração deste trabalho foi utilizada uma carteira de desenvolvimento da EOSIO. Isso é importante devido ao fato de que esta carteira irá realizar todas as configurações necessárias para um ambiente de desenvolvimento funcional. Vale frisar que uma carteira é, na verdade, um repositório de chaves, pública e privada. Com essas chaves da carteira de desenvolvimento, principalmente a privada, serão assinadas as principais ações da aplicação, desde a criação da conta do aluno até a inserção do código do diploma na rede.

A carteira de desenvolvimento é criada utilizando-se da *cleos*[12], uma ferramenta EOSIO de linha de comando que interage com uma API (*Application Programming Interface*), isto é, um conjunto de rotinas e padrões de programação para acesso a um aplicativo de software ou plataforma que, no caso, possui seu acesso baseado na REST[13] (*Representational State Transfer*) que define um conjunto de restrições para que as requisições HTTP atendam as diretrizes definidas na arquitetura. Essa API REST é exposta por um serviço denominado *nodeos*[14], análogo ao mineiro do *Bitcoin*. Esse serviço é fundamental, visto que ele é responsável por processar os contratos, validar transações, produzir e confirmar blocos.

A Instituição de Ensino Superior fará o papel de dona dessa carteira de desenvolvimento citada, visto que, a mesma será responsável pela execução de comandos de emissão do diploma e criação de contas. Ela foi denominada para esse trabalho como conta *master*, e interage com o contrato por meio da *cleos* executando as ações estipuladas no código fonte[15] do projeto. Na subseção seguinte todas as ações são executadas pela IES.

3.1 CONTA ALUNO

[12] https://developers.eos.io/manuals/eos/latest/cleos/index

[13] https://pt.wikipedia.org/wiki/REST

[14] https://eos.io/build-on-eosio/nodeos/

[15]https://github.com/lucasguimaraes/Trabalho-de-Conclusao-de-Curso/blob/master/contracts/diploma/diploma.cpp

Para criar uma conta aluno, é necessário primeiro a criação de uma carteira. Um equívoco comum em relação às carteiras de criptomoedas é que elas armazenam tokens. Na realidade, uma carteira é usada para armazenar chaves privadas para assinar transações em um arquivo criptografado. As carteiras não servem como meio de armazenamento. O armazenamento é realizado nos blocos da cadeia *blockchain*, as chaves são usadas para realizar as transações entre elas.

A criação de uma carteira no EOSIO é feita utilizando-se do *cleos*, mencionado anteriormente. O comando a seguir descreve a criação de uma carteira nomeada Aluno, e a senha dessa carteira será guardada em um arquivo texto denominado passwd. Este processo pode ser visto na Figura 4.

FIGURA 4: Criação da carteira Aluno.

```
lpguimaraes:~$ cleos wallet create -n Aluno -f passwd
Creating wallet: Aluno
Save password to use in the future to unlock this wallet.
Without password imported keys will not be retrievable.
```

Fonte: Do Autor (2020)

A senha gerada é usada para gerenciar a carteira em ações como, por exemplo a geração de uma chave pública. A seguir, na Figura 5, é mostrado o comando de criação de uma chave pública.

FIGURA 5: Criação de chaves para a carteira aluno.

```
lpguimaraes:~$ cleos wallet create_key -n Aluno
Created new private key with a public key of: "EOS8TFMCkzCbYQ516aBufwbQeotwqzMHPnq7R9v3xf3JKGYMiAikg"
```

Fonte: Do Autor (2020)

A chave pública criada é fundamental para realizar posteriormente a criação da conta do aluno. A IES fica responsável pela criação da conta do aluno utilizando a chave pública do mesmo, como visto a seguir na Figura 6:

FIGURA 6: Criação da conta aluno.

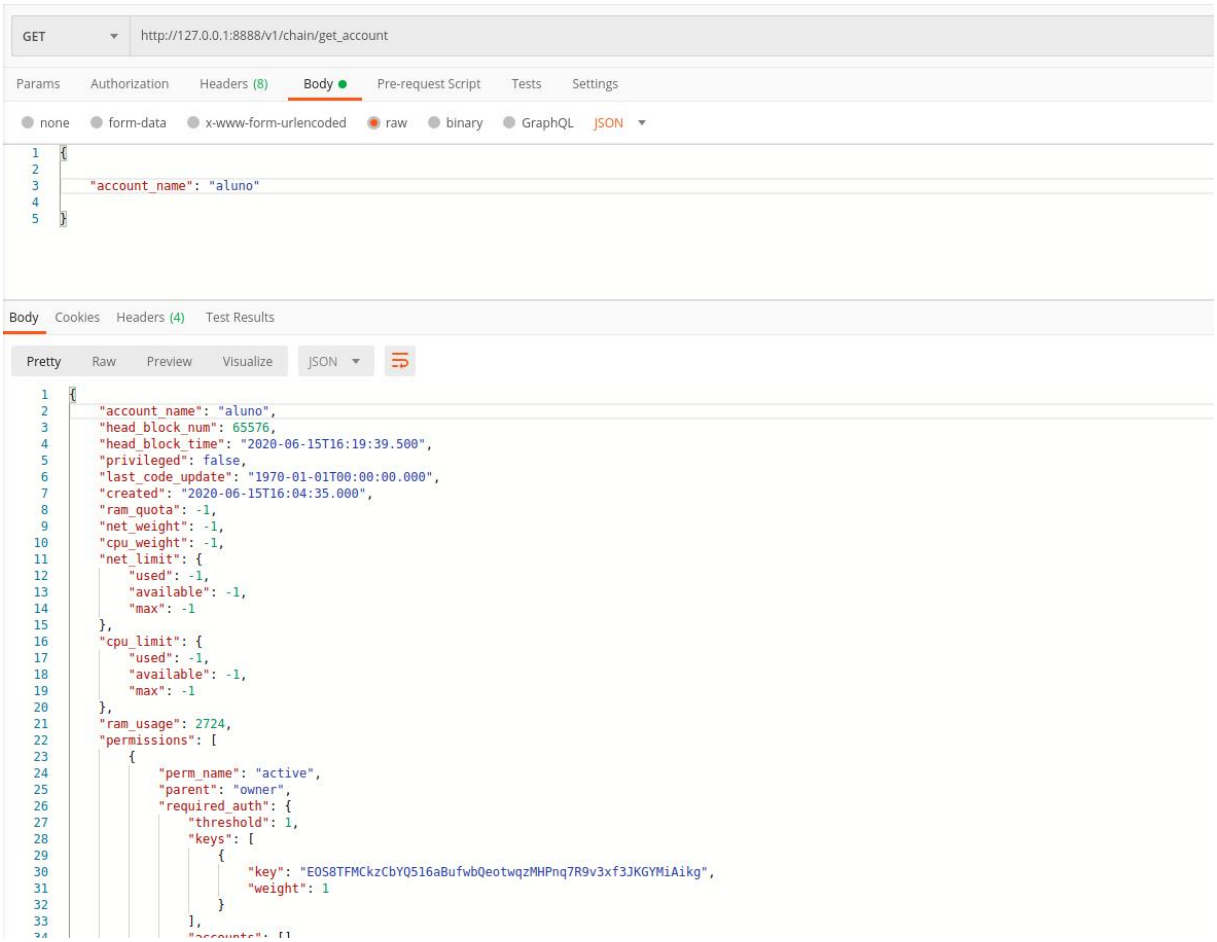
```
lpguimaraes:~$ cleos create account eosio aluno EOS8TFMCkzCbYQ516aBufwbQeotwqzMHPnq7R9
v3xf3JKGYMiAikg
executed transaction: 86b38d544744d5e71e560449de3a7370edf9ec5a1f7ed35f1f30fb3f67098424
  200 bytes  25797 us
#         eosio <= eosio::newaccount           {"creator":"eosio","name":"aluno","own
er":{"threshold":1,"keys":[{"key":"EOS8TFMCkzCbYQ516aBufwbQeot...
warn  2020-06-15T16:04:34.899 cleos     main.cpp:506                print_result war
ning: transaction executed locally, but may not be confirmed by the network yet
```

Fonte: Do Autor (2020)

A conta aluno criada agora pertence à cadeia de blocos do EOSIO e pode ser consultada e verificada por qualquer pessoa na rede. Somente o aluno consegue utilizar sua conta pois somente ele tem a chave privada par da chave pública, utilizada na criação da conta.

Como dito no início desta seção, pelo fato de o *nodeos* expor uma interface API REST, é possível a utilização de ferramentas de teste de serviços REST por meio de requisições HTTP. Foi utilizada a ferramenta *Postman*[16] para realizar essa interação. Na Figura 7 é enviada uma requisição HTTP *GET* para buscar a conta aluno. Os parâmetros da requisição são feitos por objetos JSON (*JavaScript Object Notation* – Notação de objetos JavaScript).

FIGURA 7: Busca pela conta aluno.



[16] https://www.postman.com/

Fonte: Do Autor (2020)

O *endpoint* (endereço que fornece acesso ao serviço) *get_account* é fornecido pelo *nodeos (EOSIO)*, que atua como um servidor. O parâmetro enviado no *body* da requisição, *account_name,* deve conter a conta válida a ser buscada. O retorno do servidor possui diversos parâmetros, a maioria não é importante para o escopo deste trabalho, porém um vale ser mencionada. Na linha 3 da figura 7, é exibida a informação *head_block_num* que demonstra o número *id* do bloco que a conta aluno pertence. Vale lembrar que somente pelo fato de o bloco pertencer à cadeia de blocos, ele já foi validado pelos mineiros e é inalterável. Na situação de ambiente de desenvolvimento deste trabalho, quem faz o papel de mineiro é o *nodeos.*

Com a conta aluno criada, a emissão do diploma agora pode ser feita em seu nome, como será mostrada na subseção seguinte. Porém, é necessário antes atentar para algumas particularidades do contrato desenvolvido.

3.3 CONTRATO DIPLOMA, EMISSÃO E VALIDAÇÃO

As ações implementadas no contrato são responsáveis pela sua definição de comportamento. As ações são definidas no código por meio das anotações [[*eosio*::*action*]], que indicam para o gerador de binário do código o que deve ser incluído no contrato. O contrato desenvolvido neste trabalho é composto por três ações básicas, inclusão, modificação e exclusão.

Um outro atributo essencial para o desenvolvimento de contratos é o [[*eosio::table*]], utilizado para as definições de tabelas. As tabelas são responsáveis por armazenar o estado dos dados do contrato, como em um banco de dados.

Dentro das ações, os métodos são escritos com o passo a passo que cada ação deve executar quando utilizada. No contrato desenvolvido os métodos principais são, *upsert* e *erase*. O método *upsert* inclui ou atualiza os dados do contrato.

O contrato desenvolvido deve ser inserido em uma conta própria para ele. Esta conta é criada da mesma forma que foi criada a conta do aluno. E como o contrato aqui é um diploma, a conta foi denominada **diploma**. Com o contrato

implantado na conta diploma, a IES pode realizar a inclusão dos dados no contrato. O mesmo será atualizado de acordo com o que for incluído.

O comando que se comunica com a ação *upsert* e insere os dados na tabela do contrato diploma, é visto a seguir na figura 8:

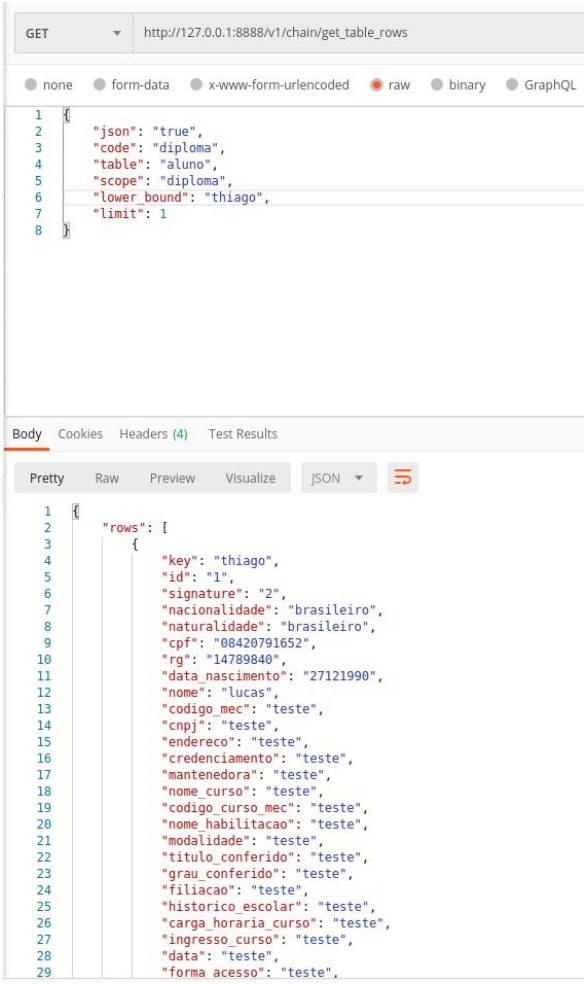
FIGURA 8: Emissão do contrato para o usuário aluno.

Fonte: Do Autor (2020)

O comando *push action* diploma *upsert*, indica que a ação *upsert*, declarada no código, deve ser chamada e realizar a inclusão dos demais parâmetros (definidos no código como variáveis) passados em formato JSON. O primeiro parâmetro aluno, da figura 8, é o nome da conta do aluno. Isso é possível pois no código foi estabelecido que a chave primária da tabela deve ser o nome da conta, e vai ter os dados do diploma gravado em seu nome. Na verdade, a principal função do contrato desenvolvido é acordar que os dados incluídos nele pertencem somente ao aluno.

Agora que os dados do diploma do aluno estão gravados na tabela do contrato, é possível realizar uma consulta como em um banco de dados. Na figura 9 abaixo é mostrado através do *Postman,* o retorno do *endpoint* que busca na tabela os dados de acordo com o que for inserido no parâmetro do corpo da requisição.

FIGURA 9: Busca do contrato utilizando nome da conta aluno.



Fonte: Do Autor (2020)

Para apresentar uma outra exemplificação, foi criada uma segunda conta denominada Thiago. O *endpoint get_table_rows* (EOSIO) da figura 9 recebe os parâmetros utilizados no corpo da requisição, sendo eles os valores: *json:true* (linha 2), que especifica o que deve ser retornado pelo servidor EOSIO seja em formato JSON. *Code:diploma* (linha 3) deve receber o nome do contrato que controla a tabela, este contrato se chama diploma. *Table*:aluno (linha 4) deve receber o nome da tabela a ser pesquisada. *Scope:*diploma recebe o nome da conta a qual o diploma pertence. O parâmetro *lower_bound:*thiago, permite que a busca seja feita por um valor especifico da chave primária da tabela, no caso deste contrato, é o nome do aluno. Desta maneira, pode-se verificar todos os dados do diploma que estão inseridos no contrato por meio desta busca.

Um outro exemplo de utilização seria por um empregador. Dado que o mesmo tenha interesse em realizar uma busca pelo diploma do entrevistado na vaga de um emprego. Realizando então uma busca pelo nome do aluno, como mostrado na figura 9, o empregador se certificaria que os dados contidos ali só podem ter sido emitidos pela IES. Garantindo a integridade do diploma e a certeza de imutabilidade inerente a uma rede *blockchain*.

4 CONSIDERAÇÕES FINAIS

A construção da aplicação foi elaborada de maneira que a IES exerça o papel principal na emissão do diploma para qualquer usuário criada por ela. Uma validação extra foi adicionada no código fonte para que nenhum usuário, sem permissão da IES, consiga realizar a operação de inserção de dados em um diploma.

Porém, cabe um ponto de atenção. Se porventura a senha da carteira da IES vier a ser perdida, seria anulada toda a possibilidade de interação com a rede *blockchain*. Nessa questão, um trabalho futuro seria o estudo e implementação da *multisig*[17]. Essencialmente, a *multisig* abre a possibilidade de múltiplas partes possuírem permissão para assinar ou aprovar as ações que ocorrem na rede.

Um exemplo de cenário seria as autoridades centrais de uma IES, por meio da *multisig*, terem controle de voto para aprovar ou não uma transação. Ou seja, nesse caso, mais de um usuário teria a permissão de emissão. Com essa transferência de autoridade, caso uma venha a se perder, não comprometeria toda a rede.

Um trabalho futuro também relevante seria na construção de uma *interface web* que realize as requisições que foram exemplificadas pelo *Postman*. Permitindo uma maior adoção e facilidade do usuário para interagir com a rede *blockchain* EOSIO.

Este trabalho não teve como objetivo abordar questões socioeconômicas e legais que provavelmente impediriam a curto e longo prazo a implementação de uma rede *blockchain* pública em todo o Brasil. Na prática, as Instituições de Ensino Superior certamente enfrentariam problemas complexos na implementação desta tecnologia, que ainda é recente e com poucos casos de uso. No entanto, a preocupação aqui foi apresentar as vantagens de segurança e baixo custo intrínsecas a esta tecnologia.

Utilizando-se da plataforma EOSIO, que fornece uma arquitetura escalável proposta por Larimer (2018), foi desenvolvida uma aplicação *back-end* que permite a inserção de dados de um diploma digital em forma de um *smart contract*. Com isso, o contrato pode ser inserido na rede descentralizada e irá perdurar enquanto houver *blockchain*.

ABSTRACT, RÉSUMÉ ou RESUMEN

With the emergence of Bitcoin in 2008, it has long been discussed about the potential use of the technology behind this cryptocurrency. This work aims to investigate how Blockchain technology could contribute to ensuring greater security in the issuance of

[17]https://steemit.com/eos/@genereos/eos-multisig-tutorial

digital diplomas by Universities in Brazil. For this, a bibliographic search was carried out to understand the functioning of a blockchain network and the level of security provided by it. The EOSIO platform is explored in a practical and direct way as a tool that helps and allows the creation of decentralized applications and, with that, it was applied in this work to create an application that allows the inclusion of a digital diploma in the blockchain network.

REFERÊNCIAS

ALIAGA, Yoshitomi; HENRIQUES, Marco (Coord.). **Uma comparação de mecanismos de consenso em blockchains**. FEEC - UNICAMP. Campinas, 2017. Disponível em: https://bit.ly/3hrc0r8. Acesso em: 5 Jun. 2020.

BBC. **CryptoKitties craze slows down transactions on Ethereum**. 2017. Disponível em: https://bbc.in/2ACjXct. Acesso em: 13 Jun. 2020.

Blocktivity. **The Real Value of Blockchains.** Blocktivity.info. Disponível em: https://blocktivity.info/. Acesso em: 10 Jun. 2020.

Brasil. **LEI Nº 9.394, DE 20 DE DEZEMBRO DE 1996**. Brasília, 1996. Disponível em: https://bit.ly/2YCIEhb. Acesso em: 7 Jun. 2020.

EOSIO. **Chain API**. Disponível em:https://developers.eos.io/manuals/eos/latest/nodeos/plugins/chain_api_plugin/api-reference/index. Acesso em: 9 Jun. 2020.

Exame. **Há 10 anos, Lehman Brothers quebrou e mudou a economia global**. Exame. 2018. Disponível em: https://bit.ly/3flp6o4. Acesso em: 20 Mai. 2020.

FARIAS, Juliana; ARAÚJO, Luiza; EVANGELISTA, Raimunda. **Percepções da importância da preservação digital**. BRAPCI. 2017. Disponível em: https://bit.ly/2AzmXXc. Acesso em: 7 Jun. 2020.

Globo. **Esquema de revalidação de diploma de medicina é desarticulado pela PF**. G1. Mato Grosso, 2013. Disponível em: https://glo.bo/3cYuDPJ. Acesso em: 7 Jun. 2020.

LARIMER, Daniel. **EOS.IO Technical White Paper v2**. 2018. Disponível em: https://bit.ly/3hqbzxt. Acesso em: 5 Jun. 2020.

Ministério da Educação. **Diploma Digital**. portal.mec. 2019. Disponível em: https://bit.ly/37uBGPl . Acesso em: 2 Jun. 2020.

NAKAMOTO, Satoshi. **Bitcoin**: **A Peer-to-Peer Electronic Cash System**. Bitcoin. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 12 Fev. 2020.

SZABO, Nick. **Smart Contracts**. Phonetic Sciences. Amsterdam, 1994. Disponível em: https://bit.ly/3hqb4DB . Acesso em: 30 Abr. 2020.

TAVARES, João; TEIXEIRA, Luiz. **BLOCKCHAIN: DOS CONCEITOS ÀS POSSÍVEIS APLICAÇÕES**. ResearchGate. Belo Horizonte, 2018. Disponível em: https://bit.ly/37sjA0h. Acesso em: 6 Jun. 2020.