Construção de uma Blockchain utilizando a linguagem Java

ADSTON OLIVEIRA PEREIRA[1], MARIO T. SHIMANUKI[2]

[1]Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas, IFSP, Campus Caraguatatuba, adstonoliveira@bol.com.br.
[2]Professor Doutor do curso de Análise e Desenvolvimento de Sistemas, Mario T. Shimanuki, IFSP, Campus Caraguatatuba, mario.shimanuki@gmail.com.
Área de conhecimento (Tabela CNPq): Arquitetura de Sistemas de Computação – 1.03.04.02-9.

RESUMO: Este estudo tem como objetivo a construção de uma *Blockchain* utilizando a linguagem de programação JAVA. Esta é uma tecnologia relativamente nova que vem sendo considerada como revolucionária por diversos setores em todo mundo. Seu potencial disruptivo é alvo de grande incentivo e seu crescimento estimulado por uma parte das grandes empresas. Trata-se de um sistema transparente, pois todo participante pode consultar as transações já realizadas e registradas; confiável, pois a validação se dá por intermédio de métodos de criptografia e consenso entre os membros; e de alta disponibilidade: pois opera em uma rede ponto-a-ponto com um banco de dados distribuído entre os nós. Além disto, suas características ainda provêem os pilares da segurança da informação. Desta forma, surge como grande aliada como complemento de confiança na apuração dos resultados em uma urna eletrônica educacional. Durante os testes foi possível identificar as alterações de integridade das informações. O presente trabalho apresenta: 1) uma introdução da tecnologia; 2) os conceitos básicos da blockchain; 3) as ferramentas e os métodos necessários para sua criação; e finalmente 4) os resultados obtidos e conclusões finais.

PALAVRAS-CHAVE: *Blockchain* Java; Rede *Peer-to-Peer*; Rede Descentralizada; Segurança da Informação.

1 INTRODUÇÃO

A *Blockchain* é uma tecnologia desenvolvida juntamente a criptomoeda *Bitcoin*, em 2008. É relativamente nova, e promete mudar até mesmo a forma como internet funciona, descentralizando seus bancos de dados e servidores e distribuindo-os nos dispositivos conectados. A isto se dá o nome de Web 3.0. Diversas empresas estão investindo em seu crescimento e aperfeiçoamento, algumas conhecidas mundialmente, como: a IBM, Microsoft, Oracle, a AWS dentre outras. (LAMOUNIER, 2019). De acordo com o *Gartner Trend*, a tecnologia deve criar um mercado de aproximadamente de 10 milhões de dólares em 2022 podendo atingir em 2030, cerca de 3,1 trilhões de dólares. (GARTNER, 2017).

No Brasil, por se tratar de uma tecnologia segura com potencial de permear todo um mercado, 75% dentre os 20 maiores bancos em operação no país, investiram no seu desenvolvimento e aprimoramento apenas em 2018. (FEBRABAN, 2018)

De forma simplista e resumida, pode-se dizer que ela é um grande livro-razão público, distribuído em nós de uma rede P*eer-to-Peer* (P2P) e que possui acesso aberto a todos os participantes. Sendo o fato mais interessante é que o consenso entre os membros da rede é o que define o que deve ser escrito, de forma que todos os nós podem acessar os registros anotados. (TAVARES e TEIXEIRA, 2016)

Suas maiores características, e o que a destaca frente a outras tecnologias, são: a *descentralização*: não necessita de uma entidade intermediária confiável; *disponibilidade* e *integridade*: os dados são disponibilizados em todos os participantes; *transparência* e *auditabilidade*: todas as transações são públicas, podendo ser consultadas a qualquer momento; *imutabilidade* e *irrefutabilidade:* são escritas em forma de Resumo Criptográfico de mão-única; *privacidade* e *autenticidade*: garantidas com a remoção de terceiros e o uso de certificados

digitais público e privados; e por fim a *cooperação* entre os nós conectados: onde há a necessidade do consenso para aprovação de cada transação. (ABIJAUDE et. al., 2018)

Para que um único dado seja alterado após sua inclusão na rede, se faz necessário que se altere toda à cadeia subsequente. Assim, quanto maior o número de blocos já adicionados, mais difícil torna-se sua adulteração. Soma-se ao fato de que a rede é atualizada em todos os nós com os mesmos dados e em curtos períodos de tempo, a viabilidade técnica e de hardware torna impraticável a sua adulteração.

2 TEORIA

No ano de 2008, Satoshi Nakamoto pseudônimo utilizado pela pessoa, ou grupo de pessoas, publicou seu artigo "*Bitcoin: A Peer-to-Peer Eletronic Cash System*". Nele, sugeriu uma nova forma de se realizar transações financeiras via Internet com o uso de uma moeda eletrônica, chamada de Bitcoin. Esta operaria sem intermediários, em uma rede Ponto-a-Ponto, utilizando um banco de dados descentralizado. Já em 2009, foi apresentado no grupo de discussões "*The Cryptographic Mailing"* e entrou em operação. Esta inovação daria origem a *Blockchain*. Em 2016, estimava-se mais de 16 milhões de *Bitcoins* em circulação no mundo. (BRAGA, FILHO e LEAL, 2017)

Após o crescente desenvolvimento das *criptomoedas*, vários especialistas observaram que as propriedades implícitas na *Blockchain* como segurança, resiliência, inviolabilidade e imutabilidade poderiam ser empregadas em outras aplicações, e assim a plataforma evoluiu. (BRAGA, FILHO e LEAL, 2017). Atualmente existem três modelos de *Blockchain*: o modelo 1.0 é caracterizado pelo *Bitcoin* e pelas *criptomoedas* que surgiram a seguir. O modelo 2.0 surgiu com o Projeto *Ethereum*, agregando o conceito de contratos inteligentes e possibilitando a instalação de aplicações descentralizadas e autônomas. A versão atual é a 3.0, que é identificada pela adoção da tecnologia em benefício das mais diversas áreas além da financeira, como comércios, governos, IoT, cidades digitais, etc. (ABIJAUDE et. al., 2018)

As transações são os seus componentes básicos e compõe uma unidade de informação, podendo ser representadas por qualquer coisa, tais como: ativos financeiros, músicas, documentos, contratos inteligentes e até mesmo propriedades intelectuais. (PROOF, 2019) Antes de serem adicionadas a um bloco, estas informações aguardam em um local chamado de *pool* enquanto os nós competem entre si para formar um bloco válido, resolvendo um enigma matemático dentro desta "sala de espera". Quando um computador resolve este enigma, ele emite um alerta com a solução, para que se realize um consenso de validação. Quando a rede aprova este bloco, seu *Hash* é criado adicionando-se um *Timestamp*, que funciona como Prova de Trabalho (*Proof of Work* - PoW). Os blocos criados são adicionados de modo sintagmático, com um bloco fazendo referência ao anterior de forma *criptograficamente* segura. (EVANS, 2014)

A segurança é empregada através do uso de criptografia, funções HASH, Assinaturas e Certificados Digitais, e ainda pelo *Timestamp.* Desta forma se atinge os pilares da segurança da informação:

Confidencialidade: A informação deve estar disponível somente as partes autorizadas. Isto é obtido por intermédio de criptografia. *Integridade:* garante que não houve alteração indevida através de funções Hash.

Autenticidade: Garantia de que as informações foram enviadas para a parte legitima, através da assinatura digital. *Disponibilidade:* Por conter dados distribuídos identicamente em todos os nós, a retirada de um ou vários membros não impede o acesso ás informações, desde que haja ao menos um participante.

Além da irrefutabilidade e de eventos temporais implementados por meio dos certificados digitais juntamente ao *Timestamp,* respectivamente.

As técnicas vistas acima são de extrema importância para garantir a segurança das transações, porém não fornecem a infraestrutura necessária para sua operação. A seguir serão descritas as tecnologias utilizadas na comunicação e armazenamento.

Rede Ponto-a-Ponto

As redes *Peer-to-Peer* (P2P) são sistemas distribuídos sem controle centralizado ou organização hierárquica onde cada elemento, chamado de nó, funciona de forma igual. Podem ter três classificações: M*odo centralizado:* Mantém um índice global dos objetos armazenados, disponibilizando-o para acesso direto dos clientes; *Modelo hierárquico:* Possui nós com características especiais, chamados de *super-nós,* para manutenção de índices. Pode ser visto também como um modelo intermediário; e por fim o *modelo descentralizado*, que não mantém nenhum tipo de índice global. (REZENDE, 2009)

Banco de Dados Distribuído

"Um *banco de dados distribuídos* é uma coleção de dados pertencentes logicamente a um sistema, mas distribuídos sobre vários sítios de uma rede de computadores". (HOPPER, 1995)

Do ponto de vista administrativo, permite que setores de uma organização, mesmo que espalhados geograficamente, mantenham controle de seus próprios dados e ainda os compartilhem de forma global. Do ponto de vista da escalabilidade, facilitam o crescimento modular, pois cada novo nó implantado compartilha seus recursos. Aumentam ainda a confiabilidade através da replicação das partes críticas do banco em mais de um nó e pode ainda, aumentar a eficiência, através de um criterioso particionamento e replicação que coloca os dados próximos do local em que são mais acessados, oferecendo maior qualidade ao se comparar ao acesso remoto em um banco de dados centralizado. (CASANOVA e MOURA, 1985).

3 MATERIAL E MÉTODOS

O Java 8 e o kit de desenvolvimento JDK (*Java Development Kit*) versão 1.8.0_111, foram selecionados como linguagem de programação. A interface de interação com o usuário foi construída com o *Swing*, construtor de interfaces gráficas do próprio Java. Como IDE de desenvolvimento, o *NetBeans* 8.2. Os testes foram realizados em um computador com Sistema Operacional (S.O) *MS Windows* 7 e outro com S.O *Debian 8*, ambos dentro da mesma rede.

Uma *Blockchain* deve realizar os seguintes requisitos: 1) Um nó que deseje se conectar deve se cadastrar. 2) O usuário pode enviar ou receber uma transação a outro membro. 3) Os membros devem receber qualquer transação e minerá-la. 4) Após o consenso deve-se anexar a rede.

As classes mínimas necessárias são: Membro/Participante: Deve possuir os dados de identificação do usuário, assim como certificado digital se disponível. Um *ArrayList* de *Sockets* conectados e métodos de gerenciamento dos mesmos, e um objeto *Blockchain*; Bloco: Deve conter um *Hash*, o *Hash* anterior e uma transação; Transação: O tipo de transação pode ser um documento em qualquer formato ou de outro tipo, a critério do desenvolvedor; *Blockchain*: Deve conter um objeto chamado de *Pool*, que conterá um *ArrayList* de Blocos aguardando para ser adicionados, um *ArrayList* de Blocos já adicionados representando a própria *Blockchain*.

A seguir estão descritas os principais métodos: ***hashFileMD5()****:* Para criação do *Hash* do arquivo, para transações que compostos por estes; ***hashBlockSHA256()****:* Cria um *Hash* com o conteúdo do bloco; ***mineBlock()****:* Para mineração do bloco; ***isChainValid()****:* validação da *Blockchain* construída. A conexão entre os nós se dá por intermédio de *Sockets*. Cada nó deve conter uma lista dos *Sockets* conectados e os disponibilizam no instante que outro nó se conecta a ele.

4 RESULTADOS E DISCUSSÃO

Este trabalho apresenta resultados parciais de um projeto de iniciação científica. Os testes foram realizados em um processo de programação sequencial (método estruturado). Testando-se passo-a-passo: a instanciação do bloco, a seleção de um arquivo, a leitura e construção do objeto Transação, a mineração, a criação do *Hash* e a adição do bloco. Foram criados cinco blocos, com modelos de arquivos diferentes. No primeiro teste, foram adicionados blocos com dados corretos que seguiram o fluxo sem intervenção. Ao ser validado pelo método "*isChainValid()"*, foi aprovado, como esperado. O segundo teste foi realizado com os mesmos dados, porém, antes de

se adicionar a *Blockchain*, os dados do bloco anterior foram intencionalmente adulterados e, ao ser submetido à validação finalizou retornando erro identificando sua adulteração. No terceiro, foram alterados os dados do último bloco e ao ser submetido à validação, também foi identificada a incoerência.

Também foram realizados testes de conferência visual, seguindo os passos anteriores, porém, ao invés de submeter à verificação pelo método *isChainValid()*, criava-se um arquivo "TXT" com o *Hash* resultante de cada bloco, e após a execução do software eram conferidos manualmente, apresentando os mesmos resultados obtidos anteriormente.

5 CONSIDERAÇÕES FINAIS

O estudo demonstrou como as técnicas utilizadas são capazes de garantir a integridade do dado no qual é aplicado; o certificado digital garante a identificação do membro envolvido na transação; e o *timestamp* registra o exato momento em que a transação ocorre. Estas técnicas, por si só, já são de grande incremento a segurança das informações. Soma-se a isto o enlace criado entre os blocos, que força a modificação de todos os blocos subsequentes ao alvo da adulteração, o que atualmente é tecnicamente custoso e inviável tecnologicamente, dependendo de seu tamanho. A disponibilidade dos dados, distribuídos em todos os nós participantes, garante que qualquer pessoa possa visualizá-los e conferi-los.

Desta forma, observa-se que a tecnologia pode auxiliar no desenvolvimento do Modulo de Auditoria dos resultados obtidos de uma Urna Eletrônica Educacional, provendo aumento da transparência, segurança e integridade dos dados ali incluídos.

Os autores gostariam de agradecer pelo apoio financeiro recebido através do Programa Institucional de Bolsas de Iniciação Científica e Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (PIBIFSP) – Edição 2019 (Edital: 49/2018) desenvolvido no Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP).

REFERÊNCIAS

ABIJAUDE, J. W. et.al. Blockchain e a revolução do consenso sob demanda. In: **Livro de minicursos do SBRC 2018**. 1º ed. Porto Alegre: Sociedade Brasileira de Computação, v. 1, p. 1-52, 2018.

BRAGA, A. M.; FILHO, J. R. F.; LEAL, R. L. V. **Tecnologia blockchain**: uma visão geral. CPqD. Soluções inovadoras e Tecnológicas, 2017. Disponível em: <https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf> Acesso em: 02 de Set. de 2019.

CASANOVA, M. A. e MOURA, A. V. **Princípios de sistemas de gerencia de banco de dados distribuídos**. Rio de Janeiro: Editora Campus, 1985.

EVANS, D. S. **Economic aspects of bitcoin and other decentralized public-ledger currency platforms** (April 15, 2014). University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 685. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424516>. Acesso em: 02 de Set. de 2019

ENTENDA Blockchain em menos de 15 minutos. **Proof - o principal trusted advisor de segurança da informação do mercado brasileiro**. Disponível em: < https://www.proof.com.br/blog/blockchain/>. Acesso em: 02 de Set. de 2019

FORECAST: Blockchain Business Value, Worldwide, 2017-2030. **GARTNER**, 2017. Disponível em: <https://www.gartner.com/en/documents/3627117>. Acesso em: 02 de Set. de 2019.

FEBRABAN - Federação Brasileira de Bancos. (2018). **Pesquisa FEBRABAN de tecnologia bancária 2018**. São Paulo: FEBRABAN, 2018. Disponível em: < https://portal.febraban.org.br/pagina/3106/48/pt-br/pesquisa>. Acesso em: 02 de Set. de 2019.

HOPPER, T. **Distributed relational database architecture**: connectivity guide. IBM Corporation, 4 ed. Prentice Hall PTR, 1995

LAMOUNIER, L. **Curso gratuito sobre blockchain**: tudo que você precisa saber. 101 Blockchains, 2019. Disponível em: <https://101blockchains.com/pt/curso-tecnologia-blockchain/>. Acesso em: 02 de Set. de 2019.

REZENDE, E. S. **Modelo estrutural para compartilhamento de arquivos peer-to-peer**. Dissertação (Mestrado) - Instituto de Biociências, Letras e Ciências Exatas Universidade Estadual Paulista, 2009. Disponível em: <http://hdl.handle.net/11449/98698>. Acesso em: 02 de Set. de 2019.

TAVARES, J. F. C.; TEIXEIRA, L. F. D. Blockchain: dos conceitos às possíveis aplicações. In: **II Seminário Governança das Redes e o Marco Civil da Internet**, 2016, Belo Horizonte. Anais do II Seminário Governança das Redes e o Marco Civil da Internet: Globalização, Tecnologias e Conectividade, 2016. Disponível em: <http://irisbh.com.br/wp-content/uploads/2017/09/Anais-II-Semin%C3%A1rio-Governan%C3%A7a-das-Redes-e-o-Marco-Civil-da-Internet.pdf>. Acesso em: 02 de Set. de 2019.