TÍTULO (Definição de uma Arquitetura para Aplicativo de Emissão de Documento de Identificação Estudantil Digital utilizando Blockchains)

MATEUS K. FERREIRA[1], CARLOS E. BELUZO[2]

Graduando em Tecnologia de Análise e Desenvolvimento de Sistemas, Bolsista CNPQ, IFSP, Câmpus Campinas, mateus.krejci@live.com.

Área de conhecimento (Tabela CNPq): 1.03.03.04-9 Sistemas de Informação

Apresentado no
8° Congresso de Inovação, Ciência e Tecnologia do IFSP
06 a 09 de novembro de 2017 – Cubatão-SP, Brasil

RESUMO: Esta pesquisa se propõe a definir uma arquitetura que será utilizada no desenvolvimento de um aplicativo para emissão e validação de documentos de identificação estudantil digital, onde a identidade pode ser garantida pela *blockchain*. E não menos importante contribuir para a ampliação deste horizonte, pois além das funcionalidades do aplicativo, o trabalho é também uma "prova de conceito", e outras pesquisas podem ser realizadas na mesma linha, utilizando a mesma arquitetura.

PALAVRAS-CHAVE: Blockchain; Ethereum;

TÍTULO EM INGLÊS (Definition of an Architecture for Document Emission Application Of Digital Student Identification Using Blockchains)

ABSTRACT: This research proposes to define an architecture that will be used in the development of an application for issuing and validating digital student identification documents, where identity can be guaranteed by blockchain. And not least to contribute to the expansion of this horizon, because besides the functionalities of the application, the work is also a "proof of concept", and other research can be carried out in the same line, using the same architecture.

KEYWORDS: Blockchain; Ethereum;

INTRODUÇÃO

Com o advento da informatização, novas formas para garantir autenticidade tem sido estudas. Uma dessas formas seria a como garantir se um dado é autêntico por meio de uma maneira descentralizada, onde não é necessário a verificação de um terceiro, por exemplo, no caso de uma transação monetária entre uma pessoa física e outra o órgão garantidor seria o próprio banco (NAKAMOTO, 2008).

Visto isso, no ano 2008, surgiu a tecnologia *blockchain*, a qual foi utilizada primeiramente para criação da rede *BitCoin*, um sistema de informação para implementação de criptomoedas. Implementada em uma rede *P2P* (*peer-to-peer*), permite, entre outras coisas, verificar a autenticidade de dados através de política definida por meio de contratos inteligentes (ETHEREUM). Além disso

qualquer cadeia de blocos pode ser rastreada por meio de sua chave pública, isso constitui o mecanismo para verificar a autenticidade do bloco (Litchfield e Herbert, 2015).

Pensando nesta mesma via, a aplicação *blockchain* pode ser utilizada além de operações de permuta de transações pela internet. Com a finalidade de validar a viabilidade da utilização deste recurso para aplicações de diferentes nichos o objetivo deste trabalho será criar um protótipo utilizando a plataforma para dispositivos móveis Android, que implemente a funcionalidade de "Documento de Identificação Estudantil Digital", utilizando métodos e tecnologias similares às utilizadas em sistemas de *BitCoin*, para garantir autenticidade e unicidade dos documentos de identificação digital que serão emitidos pelo aplicativo.

Este trabalho contribuirá para a ampliação deste horizonte, pois ira prototipar uma "prova de conceito", e outras pesquisas podem ser realizadas na mesma linha, utilizando a mesma arquitetura.

MATERIAL E MÉTODOS

Blockchain, *Ethereum* e Contratos Inteligentes *Blockchain*, ou "encadeamento de blocos", é uma rede transparente, onde cada cliente possui um "livro verdade" de forma pública, compartilhada e descentralizada. Esta tecnologia é uma solução para garantir a segurança das transações de *BitCoin*, uma moeda digital criptográfica que permite a transferência monetária entre duas partes *P2P* (*peer-to-peer*) de uma maneira totalmente segura e descentralizada, sem necessidade da intervenção de um terceiro. (SWAN, 2015).

Por meio da segurança da criptografia e da arquitetura, as transações só poderão ser iniciadas por usuários que possuem a chave privada da criptografia implementada que permitirá a transação monetária que estará disponível em sua carteira. Que por sua vez, os registros gerados são armazenados em blocos sequenciais, interligados uns aos outros por meio de identificadores criptográficos únicos, *hashcode*.

Com relação a validação dos dados, além da criptografia, é necessário que os nós que compõem a rede *blockchain* implementada, retorne verdadeiro para a autenticidade do dado, que para isto, deve ser definido nas regras de validação universal.

Ethereum, por sua vez, é um projeto de rede *blockchain* que ultrapassa os limites das transações monetárias e pode ser aplicado para outros fins, tais como a criação de Documentos Digitais Estudantis. Ela possui uma linguagem de programação própria a *Solidity*, que serve para a construção de aplicações descentralizadas, onde será desenvolvido os contratos digitais que irão compor as regras da rede, entre outras aplicações (*COINBR*).

Web3J

O *Web3J* é uma biblioteca Java que implementará a interface que será chamada entre a linguagem de programação Java e os nós da rede *Ethereum*. Esta API é conhecida como *JSON-RPC*. Através dela, conseguiremos realizar as transações dos dados e contratos a partir da aplicação desenvolvida em Java. Na Figura 1 é possível observar a conexão entre as partes citadas.

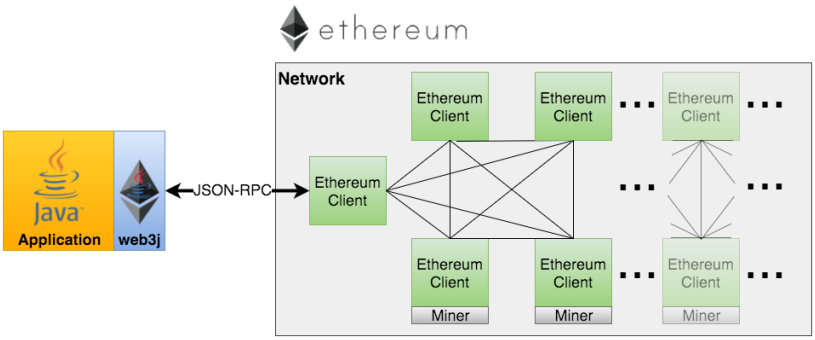

FIGURA 1. Comunicação da aplicação java com a rede *blockchain* – Fonte: Imagem extraída do GitHub *Web3J*

Geth

A rede *blockchain Ethereum* é formada por nós, que possuem aplicações com capacidade de descoberta de pares (*peer-to-peer*) e controle de carteiras. O recurso que utilizaremos neste trabalho é conhecido como *Geth*, que por sua vez é utilizado para implementar todas as especificações técnicas da rede.

Kryonet

Kryonet é uma biblioteca Java que será responsável por fazer a interface entre a comunicação do aplicativo cliente, e servidor, onde ficará implementada a rede *blockchain* através de redes *TCP*/*IP*. Além disso, facilita integração com plataforma *Android*, possibilitando implementações futuras (KRYONET, 2017).

RESULTADOS E DISCUSSÃO

Abaixo é demonstrado como a aplicação se conecta com a rede *blockchain* utilizando o *Web3j*. A aplicação se conecta a rede e cada nó da rede por sua vez é um *host*. Todos compartilham a mesma cadeia de informação.

CONCLUSÕES

Foi possível conectar a rede *blockchain* da *Ethereum* de teste. Também foi possível fazer as configurações da conta e baixar os blocos de dados trafegados pela rede.

AGRADECIMENTOS

Agradecemos ao CNPQ e ao Instituto Federal de São Paulo pela oportunidade de expansão do nosso conhecimento fazendo esta pesquisa. Agradeço em particular ao Professor Carlos Eduardo Beluzo pelo projeto e por poder confiar a mim a pesquisa.

REFERÊNCIAS

COINBR. (15 de Abril de 2016). Guia B´asico Ethereum. Acesso em 07 de 05 de 2017. Disponível em CoinBR.

ETHEREUM. White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. Disponível em. Acesso em 07 de Abril de 2017.

KRYONET. TCP/UDP client/server library for Java, based on Kryo. EsotericSoftware. Disponível em: Acesso em: 07 maio. 2017.

Litchfield, A., e Herbert, J. (2015). A Novel Method for Decentralised Peer-to-Peer Software License. Proceedings of the 38th Australasian Computer Science Conference (p. 9). Sydney: Australia. Disponível em: Acesso em 29 de Março de 2017.

NAKAMOTO, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Disponível em: Acesso em 28 de Março de 2017.

SWAN, Melanie. Blockchain: Blueprint for a new economy. Sebastopol, CA: O'Reilly Media, Inc., 2015.