PROPOSTA DE UM SISTEMA DESCENTRALIZADO E BASEADO EM BLOCKCHAIN PARA IDENTIFICAÇÃO DE USUÁRIOS

GUSTAVO SANTOS[1]; RENATA REISER[2]; MAURICIO PILLA[3]

[1]*Universidade Federal de Pelotas – gfdsantos@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – reiser@inf.ufpel.edu.br*
[3]*Universidade Federal de Pelotas – pilla@inf.ufpel.edu.br*

1. INTRODUÇÃO

A centralização da informação por entidades envolve que pessoas cujos dados são armazenados por esta entidade, confiem que estas informações nunca sejam maliciosamente alteradas por esta entidade ou por terceiros que exploram vulnerabilidades das entidades.

Uma estratégia diferente é a descentralização da informação, onde a identificação de pessoas não seja intermediada por uma terceira entidade. Sistemas baseados em blockchain promovem a confiabilidade necessária sem que exista uma entidade envolvida no processo.

Sistemas desenvolvidos com base em blockchain são confiáveis devido a natureza do mecanismo que dá suporte à blockchain. Blockchain é uma estrutura de dados distribuída composta por blocos interligados em forma de lista. Cada bloco possui um conjunto de transações, um carimbo de tempo que identifica quando o bloco foi gerado, uma assinatura digital única que resume os dados que o bloco contém e um número chamado de nonce - que é um número que, quando agregado ao bloco, produz uma sequência de zeros no início da sequência de caracteres que representa a assinatura digital do bloco (NAKAMOTO, 2008).

A Figura 1 mostra como os blocos são ligados em uma blockchain. Somente os nós mineradores possuem a capacidade de alterar a blockchain adicionando novos blocos e estes nós possuem uma cópia completa da blockchain. Cada novo bloco possui a assinatura digital do bloco anterior, dessa forma, se um bloco for modificado por algum nó na rede, a ramificação da blockchain que este participante possui torna-se inválida, sendo ignorada pelo restante do sistema.

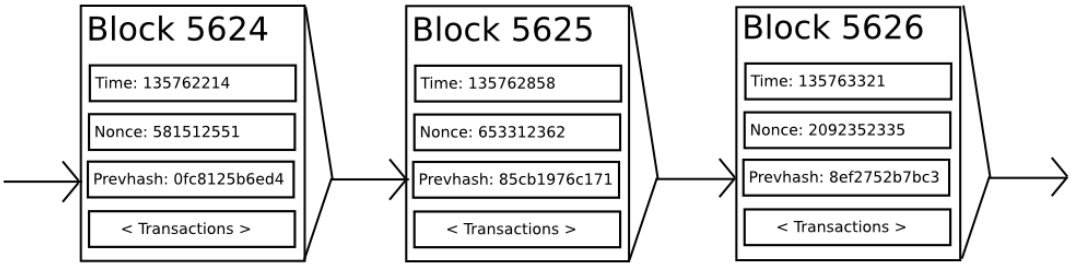

Figura 1: Estrutura de uma blockchain (BUTERIN, 2014).

Existem diversas plataformas baseadas em blockchain, como Bitcoin, Ethereum, Hyperledger, entre outros, onde, embora as plataformas possuem um padrão comum, que é o funcionamento com base em blockchain, cada uma tem suas próprias características. O escopo deste trabalho concentra-se no Ethereum,

portanto o restante do resumo trata exclusivamente das características do Ethereum.

O Ethereum é uma plataforma flexível baseado em blockchain com suporte a smart contracts (contratos digitais). Isto significa que contratos não podem ser censurados, não podem ter sua execução normal interrompida e são anti fraude. Um contrato digital é um programa Turing-completo, que representa cláusulas contratuais programáveis (BUTERIN, 2014).

O fato de sistemas baseados em blockchain serem de natureza distribuída, é necessário que os participantes da rede mantenham um consenso sobre a ramificação correta dos blocos. Este mecanismo é necessário pois blocos são adicionados à blockchain a todo momento e, muitos testes blocos podem ser modificados de modo a armazenar transações duplicadas e um sistema que garanta um consenso sobre quais blocos são válidos e quais são inválidos é necessário.

Sistemas baseados em blockchain realizam o processo de mineração. A mineração de blocos é diferente para cada sistema baseado em blockchain. Atualmente, o processo de mineração de blocos no Ethereum utiliza a estratégia cujo objetivo é encontrar o nonce do bloco - o algoritmo de mineração que o Ethereum utiliza é conhecido como Ethash (BUTERIN, 2014).

Durante o processo de mineração os contratos digitais são executados pela EVM - Ethereum Virtual Machine e, para evitar que um contrato seja executado eternamente, todos os contratos possuem sua execução limitada baseado no Gas. Gas vem do inglês Gasoline, que indica a quantidade de Wei (menor unidade do Ether - token válido no Ethereum) que um contrato pode consumir durante sua execução. A computação da quantidade de Gas que um contrato utiliza é medido com base nas instruções que o compõe.

Toda vez que um contrato digital é adicionado ao Ethereum, é necessário que o participante da rede anexe informações de Gas e Gas-Price, onde o Gas-Price significa o preço do consumo de Gas. Quanto maior o Gas-Price, maior será a recompensa ao nó que processar o contrato digital e mais cara será a execução do contrato. O Gas-Price é uma entidade fundamental no Ethereum pois é este parâmetro que regula quanto tempo um contrato ficará na fila para ser executado, uma vez que a preferência dos nós mineradores por contratos com alto valor de Gas-Price anexado, é maior.

Embora a alta volatilidade do preço do Ethereum, conforme um contrato digital consome recursos da EVM, o preço da sua execução aumenta, portanto é necessário formas de otimização de recursos. Segundo a precificação das instruções do Ethereum mostrado por WOOD (2014), o preço por gigabyte de informação armazenada no Ethereum pode chegar a milhares de dólares, então uma abordagem para armazenamento de dados off-chain - fora da blockchain, é necessária.

O Interplanetary File System (IPFS) surge como uma alternativa para o armazenamento de atributos e documentos. O IPFS é um conjunto de protocolos de rede Peer-to-Peer com a capacidade de indexar informação baseado no conteúdo. Uma porção de informação indexada pelo IPFS possui um Content Identifier (CID) único, que é uma assinatura criptográfica que representa a informação. No IPFS, os CIDs possuem duas propriedades importantes: qualquer diferença no conteúdo produz um novo CID e o mesmo conteúdo adicionado ao IPFS duas vezes em dois locais diferentes sob as mesmas configurações produzirão CIDs idênticos (BENET, 2014).

Este trabalho explora as capacidades do Ethereum em prover a confiança sobre a integridade da informação para o desenvolvimento de um sistema de identificação descentralizado e incensurável onde contratos digitais representam e armazenam atributos de cada pessoa. Pessoas podem se relacionar com sistemas através de seus contratos digitais, promovendo o gerenciamento digital de documentos, por exemplo, extratos de pagamentos, contratos de casamento, contratos de locação de casas e demais processos que envolvem identificação de pessoas.

2. METODOLOGIA

O mecanismo de identidade promovido neste trabalho é o uso de um sistema de criptografia assimétrica no esquema de chaves públicas e privadas. A chave pública deve ser conhecida e armazenada no contrato digital e todas as ações digitais necessárias de uma pessoa devem ser assinadas com sua chave privada. Este mecanismo clássico provê a capacidade de identificação digital de qualquer pessoa.

Todo e qualquer documento digital deve ser igualmente assinado com a chave privada, o que garante que a pessoa está ciente do que está assinando e que seja possível provar que um documento foi assinado por tal pessoa.

Este trabalho propõe que o consenso na rede deve ser alcançado através da estratégia de Prova de Autoridade com o algoritmo Aura, onde autoridades são pessoas ou entidades conhecidas e confiáveis. A estratégia de Prova de Autoridade é segura, exige menos energia elétrica dos participantes da rede e promove menor latência na comunicação entre os nós (ANGELIS, 2017).

Através das autoridades, pessoas são cadastradas no sistema, quando uma pessoa perde sua senha privada, é necessário que uma autoridade crie um novo contrato digital para a pessoa solicitante. Este novo contrato é ligado ao contrato anterior, garantindo que documentos assinados por uma pessoa utilizando contratos anteriores, sejam verificáveis quanto a sua origem.

Documentos e atributos pessoais são armazenados e indexados via IPFS e os CIDs referentes a porções de dados são armazenados nos contratos, o que diminui o custo de operação na blockchain.

Toda e qualquer ação executada por pessoas e autoridades são registradas na blockchain, onde qualquer alteração em informações é reconhecida e invalidada, tornando este mecanismo seguro quanto a consistência de informações.

As autoridades armazenam, cada uma, uma cópia inteira da blockchain e uma cópia dos documentos e atributos criptografados de cada pessoa, o que garante que a informação esteja continuamente disponível.

3. RESULTADOS E DISCUSSÃO

O estágio atual deste trabalho consiste em uma revisão bibliográfica extensa sobre o Ethereum e IPFS, bem como um esboço sobre os protocolos de interação entre contas adotados no sistema[1].

O sistema vem sendo implementado e testado com o fim de validar e colher dados de custos de operações, visando a otimização do sistema para utilizar

[1] https://github.com/gustavofsantos/Monografia

minimamente operações na *blockchain* sem que haja perdas de segurança quanto a consistência das informações.

Este trabalho traz um estudo sobre as capacidades de identificação de pessoas através de contratos digitais e também abre portas para aplicações que utilizam contratos digitais como base de operação.

Através de operações na blockchain do Ethereum e persistência de dados no IPFS, é possível construir aplicações seguras, consistentes, sem duplicação de informações e seguras quanto ao acesso à informação por terceiros - o que mantém a responsabilidade do usuário quanto a seus dados.

4. CONCLUSÕES

Foi concluído que é possível a recuperação, em partes, da informação do usuário caso ele perca sua chave privada. Através da estratégia de Prova de Autoridade, para alcançar o consenso entre os nós participantes da rede, é possível que uma autoridade conhecida e confiável realize operações contratuais para ligar um contrato digital cuja chave privada foi perdida a um novo contrato digital, no qual mantém a consistência das informações sobre um indivíduo.

O uso da persistência e versionamento da informação através do IPFS mostrou que é possível poupar custos de operação na *blockchain*, ao armazenar os CIDs nos contratos digitais.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ANGELIS, S., ANIELLO, L., BALDONI, R., LOMBARDI, F., MARGHERI, A.; SASSONE, V. **PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain**. 2017. Acessado em 7 de set. 2018. Online. Disponível em: https://eprints.soton.ac.uk/415083

BENET, J. IPFS-content addressed, versioned, P2P file system. **arXiv preprint** arXiv:1407.3561, 2014.

BUTERIN, V. **A next-generation smart contract and decentralized application platform**, 2014. Acessado em 7 de set. 2018. Online. Disponível em: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

WOOD, G. Ethereum: A secure decentralised generalised transaction ledger. **Ethereum project yellow paper**, v. 151, p. 1-32, 2014.