Aplicação Para Votação Utilizando a Tecnologia Blockchain

Johnny Brando Alagoano de Jesus, João Paulo de Brito Gonçalves

[1]Instituto Federal do Espírito Santo (IFES) – Cachoeiro de Itapemirim-ES – Brasil

johnny_brando@hotmail.com, jpaulobg@hotmail.com

Abstract. *With the advent of the Internet and the recent success of crypto-coins to Blockchain technology, it is very effective in decentralizing processes, as it allows to authenticate a transaction between two parties without the participation of a reliable third party. Therefore, this work aims to apply the operation of the Blockchain that had its origin with criptomoeda Bitcoin. The use of this technology will be through a decentralized application in the voting context.*

Resumo. *Com o advento da Internet e o recente sucesso das criptomoedas à tecnologia Blockchain se mostra muito eficaz na descentralização de processos, pois permite autenticar uma transação entre duas partes sem a participação de uma terceira parte confiável. Portanto, este trabalho visa aplicar o funcionamento da Blockchain que teve sua origem com criptomoeda Bitcoin. A utilização dessa tecnologia se dará através de uma aplicação descentralizada no contexto de votação.*

1. Introdução

A informação afeta direta e indiretamente uma organização tendo como base o valor que pode ser agregado a ela. Gestores dos mais variados tipos de negócios procuram utilizar bem de uma informação como um instrumento para lidar com problemas relacionados a sua organização [de Lacerda Moreira et al. 2013]. Por isso, sabendo da importância desse ativo na gestão de uma organização é necessário que o gestor se preocupe com a qualidade da mesma, sobretudo com sua integridade para que a decisão tomada seja também virtuosa. Um desafio relacionado a coleta de dados para a tomada de decisão é fazer com que essa coleta seja de forma democrática e transparente nas organizações, dando assim mais confiança ao tomador de decisão. Um outro problema análogo ao primeiro é quando a decisão deve ser tomada em conjunto com outros membros de uma organização por meio de uma votação. Como é possível garantir que o processo eleitoral não será fraudado para favorecer interesses de terceiros?

Pensando nisso, o trabalho apresenta uma proposta de aplicação para votações internas à uma organização, de forma transparente e confiável utilizando a tecnologia Blockchain. Esta tecnologia, responsável pelo sucesso das criptomoedas dentre elas, o Bitcoin [Ulrich 2014], pode ser usada em diversos tipos de aplicações descentralizadas que necessitem de transparência e confiabilidade.

Este artigo está organizado da seguinte forma: a seção 2 apresenta de forma resumida a tecnologia Blockchain. A seção 3 descreve os Contratos Inteligentes, componente fundamental do trabalho. Por fim, a seção 4 fala do estado atual do desenvolvimento do trabalho e as perspectivas futuras.

2. Blockchain

A Blockchain é uma tecnologia de armazenamento descentralizado desenvolvida por Satoshi Nakamoto, que é um pseudônimo para o criador ou criadores da criptomoeda Bitcoin, que em 2008 publicou um artigo descrevendo-a [Nakamoto 2008]. Inicialmente a Blockchain veio na missão de sanar uma falha chamada gasto-duplo que consiste em um mesmo valor ser utilizado mais de uma vez em transações financeiras diferentes. A Blockchain nesse caso funciona como um livro público onde todas as transações feitas estão escritas neste livro, quando uma nova transação ocorre ela é testada contra a Blockchain e assim verifica-se a mesma transação não foi realizada anteriormente [Ulrich 2014].

Na Blockchain, as transações são agrupadas em blocos, estando cada um conectado ao bloco anterior através de endereços *hash* formando uma cadeia, comumente utilizando o algoritmo de *hash* SHA-256 [Kelly and Frankel 2007] o que faz com que modificações ou tentativas de fraudes sejam praticamente nulas, já que uma vez que um bloco é gerado fica impossível sua alteração, tendo em vista que o mesmo está encadeado através de endereços *hash* a um bloco anterior e uma fraude no bloco pode ocasionar uma mudança de *hash*, fazendo assim com que a rede detecte uma tentativa de fraude.

Essa tecnologia funciona em consenso o que significa que cada transação realizada na rede é validada pelos seus próprios membros. E através dessa política, a Blockchain exime a necessidade de um agente centralizador, trazendo assim como uma das suas principais características o fato de ser uma tecnologia descentralizada. Como exemplos de agentes centralizadores temos bancos, cartórios, etc. Do modo tradicional esse agente centralizador funciona como um mediador de um processo, seja esse processo uma transação financeira ou a mudança do titular de um imóvel. No lugar deste agente centralizador, temos a validação por meio na mineração, que se dá através da realização de uma Prova de Trabalho onde o minerador testa valores submetidos a função SHA-256 para encontrar um *hash* que satisfaça uma condição da rede. Chamamos este valor a ser testado de *nonce* [Rodrigues 2018]. Uma vez que um *nonce* é descoberto por um nó, este nó envia em *broadcast* esse resultado e os demais nós o aceitam adicionando assim nas suas respectivas cópias da Blockchain. Para que os demais nós aceitem um novo bloco basta que o *nonce* encontrado seja submetido ao mesmo cálculo matemático realizado para o encontrar, portanto conclui-se que a Prova de Trabalho é muito difícil de ser resolvida, mas muito fácil de ser testada.

Com a popularidade das criptomoedas muitas plataformas utilizando a metodologia da Blockchain surgiram. Uma das mais famosas é a *Ethereum* [Ethereum 2018]. A *Ethereum* foi desenvolvida por Vitalik Buterin, um dentre muitos programadores envolvidos com o Bitcoin em 2010. Para ele uma linguagem de scripts mais robusta deveria ser criada e implementada ao sistema da criptomoeda. Então surgiu a ideia da *Ethereum*, uma plataforma comumente usada para a programação de aplicações descentralizadas utilizando Blockchain. A *Ethereum* faz o uso de ferramentas para dar mais dinamicidade para a programação como, por exemplo, Contratos Inteligentes que executam seus termos automaticamente.

3. Contratos Inteligentes

Um Contrato Inteligente (*Smart Contract*) pode ser definido como um protocolo de transação informatizado que executa os termos de um contrato. Se formos pensar em

uma fórmula sobre como funciona um *Smart Contract*, temos que: Se ocorrer o evento X, então o código de computador desencadeará a consequência Y [Stokes and Freire Ramos 2017]. Levando em consideração a fórmula citada acima, temos termos de um contrato que quando executados geram uma consequência automaticamente. Dentro do contexto da *Ethereum*, Contratos Inteligentes são scripts armazenados na Blockchain, de forma que transformam os termos dos contratos tradicionais em regras computacionais executadas automaticamente e de forma descentralizada a partir do momento em que o contrato é validado pela rede da *Ethereum* [Christidis and Devetsikiotis 2016].

Contratos Inteligentes são uma ferramenta importante no desenvolvimento de aplicações descentralizadas (*Decentralized Application* - DAPP). Uma DAPP basicamente consiste em um *front-end* geralmente desenvolvido em JavaScript e um Contrato Inteligente implementado na Blockchain como *back-end*. A comunicação do *front-end* com o *back-end* se dá através de uma ABI (*Application Binary Interface*) e da biblioteca Web3, sendo uma ABI uma interface do contrato que informa ao usuário quais os métodos estão implementados nesse determinado contrato. Já a Web3 é um conjunto de bibliotecas que nos permite interagir com um nó *Ethereum* local ou remoto, usando uma conexão HTTP ou IPC [Ethereum 2018].

4. Aplicação Para Votação

A Aplicação Descentralizada que está sendo desenvolvida se insere em um contexto do votações genéricas, podendo ser útil para organizações que desejam coletar de forma democrática informações íntegras e transparentes. O *front-end* da aplicação foi desenvolvido utilizando o Ionic Framework. O Ionic é comumente utilizado para o desenvolvimento de aplicações para dispositivos moveis, sendo essas aplicações multiplataformas [Tavares 2016]. O *back-end* está sendo desenvolvido utilizando a plataforma de Blockchain *Ethereum* e um Contrato Inteligente. Este Contrato Inteligente está sendo desenvolvido na linguagem Solidity, a mais popular para aplicações deste tipo. Podemos citar como funções principais da aplicação: **Abrir Votação**, **Encerrar Votação**, **Alertar Funcionário** e **Registrar Voto**.

A função **Abrir Votação**, consiste em permitir que gestor da organização abra para seus colegas e funcionários uma votação sobre determinado tema de interesse da organização afim de tomar uma melhor decisão. A função de **Encerrar Votação** ao contrário da função anterior, encerra uma votação quando já coletada uma quantidade satisfatória de opiniões para o tomador de decisões. **Alertar Funcionário**, pede para que um determinado usuário se apresse em emitir uma opinião para o gestor. Todas essas três primeiras funções da aplicação são realizadas pelo gestor da organização que se utilizará de um perfil privilegiado para executar essas funções. A quarta função, **Registrar Voto** é realizada pelos demais usuários e é onde está a parte mais importante da aplicação. Em **Registrar Voto** temos a conexão com a *Ethereum* utilizando a biblioteca Web3 para se conectar à um endereço de Contrato Inteligente que estará implementado na Blockchain. Os termos desse contrato estarão presentes na aplicação através da sua ABI e serão executados quando o usuário realizar o evento de clicar no botão **Registrar Voto** como vemos na imagem abaixo.

Figura 1. Registrar Voto

O trabalho se encontra então na fase de desenvolvimento do back-end, composto pelo Contrato Inteligente e sua posterior depuração na Blockchain. Terminada esta fase, será feita a conexão entre o front-end já desenvolvido e o back-end e serão realizados testes para demonstrar a eficácia da solução. Concluiremos a partir dos testes que a votação realizada é segura e pública.

Referências

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4:2292–2303.

de Lacerda Moreira, R., Vogel Encarnação, L., Neto de Almeida Bispo, O., Angotti, M., and Douglas Colauto, R. (2013). A importância da informação contábil no processo de tomada de decisão nas micro e pequenas empresas. Revista Contemporânea de Contabilidade, 10(19).

Ethereum (2018). Ethereum ethereum/web3.js. https://github.com/ethereum/web3.js.

Kelly, S. and Frankel, S. (2007). Using hmac-sha-256. Technical report, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. UNICAMP.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Rodrigues, C. K. d. S. (2018). Uma análise simples de eficiência e segurança da tecnologia Blockchain.

STOKES, M. and FREIRE RAMOS, G. (2017). Smart contracts. Actualidad Juridica (1578-956X), (46).

Tavares, H. L. (2016). Introdução a desenvolvimento de aplicações híbridas. Revista Eletrônica eF@ tec, 6(1):11–11.

Ulrich, F. (2014). Bitcoin. Instituto Ludiwg Von Mises Brasil, São Paulo, 1 edition.