AECIO DE OLIVEIRA SOUZA
EDUARDO CORREIA DOS SANTOS JÚNIOR
ERNESTO SOUZA MENEZES NETO JUNIOR
JEFERSON SANTOS DE ALMEIDA
LUIZ CARLOS DOS SANTOS FERREIRA SACRAMENTO

Aquisição de tokens por demanda para sistemas de votação eletrônica baseados em Blockchain e criptomoedas

Salvador-BA

12 de novembro de 2021

AECIO DE OLIVEIRA SOUZA
EDUARDO CORREIA DOS SANTOS JÚNIOR
ERNESTO SOUZA MENEZES NETO JUNIOR
JEFERSON SANTOS DE ALMEIDA
LUIZ CARLOS DOS SANTOS FERREIRA SACRAMENTO

Aquisição de tokens por demanda para sistemas de votação eletrônica baseados em Blockchain e criptomoedas

Áreas da Computação: Banco de dados, Sistemas distribuídos
Área de Concentração: Blockchain

UNEB - Universidade do Estado da Bahia
Departamento de Ciências Exatas e da Terra

Salvador-BA

12 de novembro de 2021

Sumário

1 Introdução

Ao longo do tempo, inúmeras sociedades ao redor do globo implementaram, testaram e ruíram sob a gerência de vários tipos de regimes políticos, que, por definir as regras de interação entre as pessoas, e os critérios de elegibilidade dos governantes, tem papel crucial na qualidade de vida da população. Dentre esses vários tipos de regimes, destacamos a democracia, mundialmente reconhecida e que constitui a política de mais da metade dos países do mundo, como visto em (1). A democracia tem seu alicerce na vontade do povo, e por isso, os governantes devem garantir que essa vontade possa ser expressada, e como visto em (2, p. 1): "[...] 'vote' has emerged as a tool for representing the will of the people when a selection is to be made among the available choices.", dessa forma, assegurar a segurança e confiabilidade dos processos de votação numa democracia é, indubitavelmente, uma questão de necessidade.

Abordaremos de forma mais específica os sistemas de votação envolvidos nos processos eleitorais de uma democracia, que, como dito em (3), já foram implementados de diferentes formas ao longo do tempo, desde o voto falado e o levantar das mãos até o voto em papel e voto impresso. E além disso, com o avanço da tecnologia, os sistemas de votação por meio eletrônico, ou Electronic Voting System (EVS), começaram a ser introduzidos, e é nessa grande área que o nosso problema está inserido.

Como dito em (4), nos processos eleitorais convencionais, a estrutura e o método de votação são controlados de forma centralizada por uma organização, e todo esse poder centralizado pode levantar questionamentos sobre a confiabilidade do processo. Nesse cenário tecnologias modernas com potencial descentralizador apresentam grande potencial de aplicabilidade, como é o caso da blockchain. Conforme mostrado em (5) a blockchain consiste em uma tecnologia que armazena transações de forma eficiente, verificável e permanente, no que é conhecido como *distributed ledger*.

A estrutura de blockchain, e por consequência, os EVS baseados em blockchain, apresentam certa complexidade, pois são um agregado de conceitos e tecnologias, como o

conceito de blocos e a forma que compõem a blockchain, as estratégias de criptografia e segurança envolvidas, os recursos computacionais empregados, e a própria rede P2P de blockchain, tudo isso pode ser visto com mais detalhes em (6). A blockchain também se divide em tipos, baseados no permissionamento dado aos usuários daquela rede, sendo assim, a blockchain pode ser pública ou permissionda (7). A blockchain é apenas uma abstração - atualmente sendo implementada por várias iniciativas, como: Bitcoin, Ethereum, Hyperledger e etc - e tem seu potencial explorado de várias formas. Do ponto de vista de plataforma, a blockchain pode ser utilizada para sustentar as tecnologias modernas das aplicações descentralizadas, ou Decentralized Apps (dApps).

A blockchain tem a aptidão para solucionar os problemas dos EVS, e no estado da arte isto é feito majoritariamente com o auxílio de Smart Contracts (SC's) e/ou criptomoedas, o que formam dois grandes conjuntos de soluções de EVS baseados em blockchain, como é visto em (8).

No primeiro conjunto, destacamos o trabalho de Fernandes et al.(4), que traz uma grande preocupação com encriptação, comprovando com definições e teoremas a assertividade dos mecanismos de segurança. A solução traz a proposta do voto remoto, por uma dApps que interage com SC's da rede Ethereum, e o processo eleitoral corre através de várias etapas que contam com 6 (seis) entidades envolvidas, cada um com seu papel.

Já no segundo conjunto, o trabalho de Murtaza, Alizai e Iqbal(9) traz um solução baseada em criptomoeda, onde as carteiras digitais (*Digital Wallets*, ou simplesmente, *Wallets*) dos eleitores acomodam uma moeda, que representa o direito a um voto, e é transferida para a carteira do candidato escolhido no momento do voto. Este trabalho apresenta um EVS cujo processo de confirmação de identidade é baseado em zkSNARKs para a verificação do voto, e na apresentação de credenciais biométricas em conjunto com uma identificação emitida por um órgão nacional nas cabines de votação, para autenticação antes do voto.

Também existem trabalhos que unem os dois conjuntos, como em (1), que apresenta uma solução de EVS com foco em um design descentralizado, que, como dito no artigo, transfere algumas responsabilidades geralmente designadas a uma autoridade central para um Secret Contract, para que o sistema esteja mais sob o controle dos *peers* da rede, em vez de uma única organização. O sistema proposto conta com o apoio de uma autoridade central da eleição no processo de identificação dos eleitores elegíveis ao voto, um funcionamento cooperativo entre Secret Contracts da blockchain Enigma, e Smart Contracts da blockchain Ethereum, e um mecanismo baseado em token para garantir que cada eleitor

vote apenas uma vez.

E por último, trabalhos que não se enquadram em nenhum dos dois conjuntos, como em (7), ou que apresentam uma visão geral de várias soluções do estado da arte, como pode ser observado em (5), também trazem sua contribuição para o estado da arte.

Entretanto, duas lacunas são claras no estado da arte, e este projeto se propõe a resolver a segunda. Primeiro, não foi encontrado nenhum trabalho que apresente experimentos em grande escala sustentados por métricas reconhecidas pela área, e isso denota uma falta de padronização no método em que os EVS são avaliados, além de uma possível omissão de problemas de escala, em decorrência, por exemplo, do *gas limit* da blockchain pública do Ethereum, como previsto em Hjálmarsson et al.(10), ou a falta de observação empírica, que dificulta a determinação da capacidade de escala das plataformas baseadas em blockchain (11); Em segundo lugar, existe um problema nos EVS baseados em criptomoedas nas blockchains públicas, como apresentado em (10, p. 9):

> [...] for every eligible voter, a token must be purchased to enable every voter with a voting right. This can lead to cost inefficiency with low voter turnout, f.x. if a government purchases 3 million tokens for 3 million eligible voters, but the voter turnout is 50%, then 1.5 million tokens would have sufficed. There would be no possibility for the government to purchase only 1.5 million tokens, since that would lead to the individuals that would not vote to not having a right to vote, which is illegal and predicting voter turnout precisely is impossible.

E que pode se tornar uma barreira de entrada para nações democráticas que tenham interesse em implementar um EVS baseado em blockchain.

2 Objetivos

2.1 Objetivo Geral

Esse projeto tem a finalidade de otimizar os gastos públicos com tokens necessários para implementar um EVS baseado em criptomoeda numa plataforma de blockchain pública, e para isso, implementaremos uma solução de votação segura baseada em blockchain, focada em garantir a segurança dos processos eleitorais, e com o envolvimento de intermediários reduzido, uma vez que o processo é descentralizado, o que aumenta a confiabilidade do sistema.

Almejamos com esse trabalho propor um novo modelo de aquisição dos tokens: a aquisição por demanda. De um modo que, no momento do voto, a aquisição seja feita, e então mesmo considerando as taxas de abstenção, o custo total com tokens da rede de blockchain pública sejam justos e alinhados com a quantidade total de eleitores que exerceram seu direito de voto, evitando assim, desperdício de tokens e garantindo que todo eleitor elegível ao voto possa participar do processo eleitoral.

Entendemos que essa tecnologia solucionará de maneira significativa o problema citado, democratizando o acesso a esse tipo de sistema de votação, a partir do momento que, nações com orçamentos muito limitados, possam desfrutar dos benefícios da blockchain no processo eleitoral.

Essa solução se mostra exequível pelo fato de que a negociação de criptoativos realizadas por ferramentas de automação - como os bots - já é realidade para quem especula no mercado financeiro, como visto em (12). E esse tipo de solução pode ser aproveitada, e implementada com adaptações para solucionar o problema apresentado.

2.2 Objetivos Específicos e Secundários

Para alcançar nosso objetivo, além de construir o sistema em blockchain, planejamos construir uma rotina que negocie os criptoativos necessários para contemplar o processo eleitoral sob demanda, de modo que os tokens adquiridos sejam diretamente enviados para o endereço da *wallet* do eleitor elegível, para também otimizar os custos com eventuais taxas para realizar as transferências.

Além disso, será necessária uma etapa destinada a seleção da rede de blockchain a ser utilizada no projeto, haja vista que existem várias soluções diferentes no mercado, cada uma com suas vantagens e desvantagens, necessitando um trabalho de análise que fundamente uma escolha. Nesse sentido, também será necessário executar uma atividade de seleção de ferramentas de teste compatíveis com a rede escolhida.

3 Justificativas e Contribuições

É comum que os processos eleitorais sejam questionados, principalmente na iminência de uma eleição, e garantir a confiabilidade e segurança desse processo é uma questão de segurança nacional pois tem impacto direto na sociedade, e tendo em vista as características da blockchain e o seu já visto potencial de aplicabilidade, surge a motivação para a criação da solução proposta, que já se mostra de grande valor social neste ponto.

A entrega de valor desse trabalho tem grande força no aspecto econômico, pois a efetividade dos gastos no processo eleitoral proposto é otimizada, devido ao método de aquisição de tokens de blockchain por demanda.

Do ponto de vista acadêmico, a proposta é trazer para a área de pesquisa, estratégias de aquisição de criptoativos de forma automatizada, que já são utilizadas em outras áreas, dessa forma, a contribuição é feita à medida que a lacuna apontada é solucionada.

A contribuição clara nesses três pontos sustenta o racional por trás do desenvolvimento desse projeto, e indica o potencial da solução em difundir a tecnologia de blockchain aplicada a EVS com menor custo, mas garantindo um processo transparente e seguro.

4 Metodologia

O maior entregável, que será chamado de Atividade 1, é constituído pelo sistema de blockchain que manterá as regras de negócio associadas com o processo eleitoral, que será feito com o auxílio da tecnologia de SC's, e esta decisão é fundamentada na força que a tecnologia apresentou no estado da arte, como visto na revisão sistemática que precede este trabalho, onde foi possível observar que 79% dos trabalhos analisados apresentaram os SC's como solução tecnológica para EVS. Nesta etapa, construiremos os contratos necessários, em cima da plataforma escolhida, utilizando as ferramentas de teste selecionadas em outra etapa. Esta etapa é considerada concluída e pode ser validada quando uma versão estável da solução esteja implantada, mesmo que ambiente de testes, e possa ser testada publicamente. Além disso, eficiência nos gastos deve ser comprovada em um quadro comparativo, que contemple o modelo de aquisição de tokens proposto, e o modelo majoritariamente usado no estado da arte (a aquisição de token antes do processo eleitoral), e devem comparados sob o indicador de custo total por votos contabilizados.

Este grande entregável será apoiado por outras duas etapas, a primeira, chamada de Atividade 2, consiste na análise e definição da rede de blockchain, que será feita com base nos resultados de uma revisão sistemática de literatura realizada anteriormente, partindo de uma análise das redes/protocolos apresentadas nesta, e sustentada pelo quadro comparativo apresentado em (13), utilizando as características apresentadas na sessão *A. Characteristics*, como nossos critérios objetivos de análise. Esta etapa é considerada concluída e pode ser validada, quando uma plataforma de blockchain tenha sido selecionada, e as justificativas que embasem a escolha estejam disponíveis, assim como um quadro comparativo construído sob os critérios objetivos de análise, apresentando as soluções que foram consideradas.

A segunda etapa de apoio complementa a primeira, é chamada de Atividade 3, e trata da seleção das ferramentas de teste e desenvolvimento compatíveis com a rede de blockchain escolhida. Essa etapa será realizada partindo da documentação técnica oficial da rede escolhida, e das ferramentas que são publicamente reconhecidas e/ou recomendadas

por ela, buscando encontrar, em primeiro lugar, ferramentas open source avaliadas sob os critérios de *Maturity*, *Vulnerability*, *Reliability*, *License* e *Issues of license use*, *Popularity* e *Project activity* definidos em (14). Caso não existam ferramentas open source que atendam aos critérios, a seleção de ferramentas proprietárias vai ser realizada considerando a relação custo X *Popularity*(14). Esta etapa é considerada concluída e pode ser validada, quando pelo menos uma plataforma que permita a implantação simulada dos sistemas de blockchain e dos SC's seja selecionada.

Para estender a Atividade 1, e contemplar a entrega do maior diferencial deste projeto, será necessário o desenvolvimento de um módulo apartado (Atividade 4), mas que pode ser desenvolvido em paralelo, e que será utilizado pelo sistema principal de blockchain para realizar as tratativas de aquisição dos criptoativos sob demanda, para serem utilizados no processo eleitoral.

5 Cronograma

O cronograma deste projeto é apresentado nas tabelas 1 e 2.

	S01	S02	S03	S04
Atividade 1				
Atividade 2	•	•		
Atividade 3			•	•
Atividade 4				

Tabela 1: Cronograma das semanas de dezembro de 2021

	Jan	Fev	Mar	Abr
Atividade 1	•	•	•	•
Atividade 2				
Atividade 3				
Atividade 4	•	•		

Tabela 2: Cronograma de janeiro a abril de 2022

Referências

1 ZAGHLOUL, E.; LI, T.; REN, J. d-bame: Distributed blockchain-based anonymous mobile electronic voting. *IEEE Internet of Things Journal*, p. 1–1, 2021.

2 SHAHZAD, B.; CROWCROFT, J. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, v. 7, p. 24477–24488, 2019.

3 MATILE, R. et al. Caiv: Cast-as-intended verifiability in blockchain-based voting. In: *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. [S.l.: s.n.], 2019. p. 24–28.

4 FERNANDES, A. et al. Decentralized online voting using blockchain and secret contracts. In: *2021 International Conference on Information Networking (ICOIN)*. [S.l.: s.n.], 2021. p. 582–587.

5 KHANDELWAL, A. Blockchain implimentation on e-voting system. In: *2019 International Conference on Intelligent Sustainable Systems (ICISS)*. [S.l.: s.n.], 2019. p. 385–388.

6 AGBESI, S.; ASANTE, G. Electronic voting recording system based on blockchain technology. In: *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*. [S.l.: s.n.], 2019. p. 1–8.

7 B, S. et al. Secured electronic voting system using the concepts of blockchain. In: *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. [S.l.: s.n.], 2019. p. 0675–0681.

8 DOOST, M. et al. Analysis and improvement of an e-voting system based on blockchain. In: *2020 28th Iranian Conference on Electrical Engineering (ICEE)*. [S.l.: s.n.], 2020. p. 1–4.

9 MURTAZA, M. H.; ALIZAI, Z. A.; IQBAL, Z. Blockchain based anonymous voting system using zksnarks. In: *2019 International Conference on Applied and Engineering Mathematics (ICAEM)*. [S.l.: s.n.], 2019. p. 209–214.

10 HJáLMARSSON, F. et al. Blockchain-based e-voting system. In: *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. [S.l.: s.n.], 2018. p. 983–986.

11 KSHETRI, N.; VOAS, J. Blockchain-enabled e-voting. *IEEE Software*, v. 35, n. 4, p. 95–99, 2018.

12 POPESCU, O. *Crypto trading bots: The ultimate beginner's guide*. jun. 2021. Disponível em: ¡⟨https://www.trality.com/blog/crypto-trading-bots⟩¿.

13 ANILKUMAR, V. et al. Blockchain simulation and development platforms: Survey, issues and challenges. In: *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. [S.l.: s.n.], 2019. p. 935–939.

14 ZHAO, Y. et al. Evaluation indicators for open-source software: a review. *Cybersecurity*, v. 4, n. 1, p. 20, Jun 2021. ISSN 2523-3246. Disponível em: ¡⟨https://doi.org/10.1186/s42400-021-00084-8⟩¿.