UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
SISTEMAS DE INFORMAÇÃO

Vitor Patricio Chaves

Organização autônoma descentralizada para transparência e participação em serviços públicos

Florianópolis
2024

Vitor Patricio Chaves

Organização autônoma descentralizada para transparência e participação em serviços públicos

Trabalho de Conclusão de Curso submetido ao curso de Sistemas de Informação do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador(a): Prof. Jean Everson Martina, Dr.

Florianópolis

2024

Vitor Patricio Chaves

Organização autônoma descentralizada para transparência e participação em serviços públicos

Projeto apresentado na disciplina de Trabalho de Conclusão de Curso, como requisito para a aprovação na disciplina Projetos II, ministrada pelo Prof. Dr. Renato Cislaghi, no segundo semestre de 2024

Orientador:

_____

Prof. Dr. Jean Everson Martina

Banca Examinadora:

_____

Mauricio de Vasconcelos Barros

_____

Giovana Nunes Inocêncio

Florianópolis

2024

Dedico este trabalho, primeiramente, aos meus pais, que deram a vida para me colocar onde estou agora, permitindo-me realizar meus sonhos. Também dedico a todos que não só acreditam, mas trabalham por um futuro melhor.

AGRADECIMENTOS

Agradeço aos meus pais, pela fortaleza que me deram, aos meus professores, pelos conhecimentos compartilhados, e às amizades que fiz durante a graduação, que tornaram toda essa jornada uma verdadeira montanha-russa de emoções.

A UFSC me proporcionou momentos únicos e inesquecíveis, permitindo-me evoluir e, sem dúvida, por fim, me transformou em um ser humano muito melhor.

"A raiz do problema com a moeda convencional é toda a confiança necessária para fazê-la funcionar."

(NAKAMOTO, 2009)

RESUMO

Este projeto explora o potencial das Organizações Autônomas Descentralizadas (DAOs) para aprimorar a fiscalização de atividades públicas, promovendo transparência, responsabilização e participação cidadã na gestão dos recursos. Aproveitando a tecnologia blockchain e o emergente token digital brasileiro DREX, propomos a criação de uma DAO que permita aos cidadãos monitorar e verificar todas as etapas de projetos de interesse público em bairros, desde a proposta inicial até a execução final. Este trabalho apresenta o desenvolvimento da Bairro DAO, uma plataforma destinada a promover a transparência em serviços públicos em nível local. Entre os benefícios esperados, destacam-se o aumento da transparência, a redução da corrupção e a utilização mais eficiente dos recursos públicos. Baseada na tecnologia blockchain e em contratos inteligentes (smart contracts), a plataforma permite que cidadãos acompanhem e verifiquem todas as fases de trabalhos no setor cívico local, assegurando rastreabilidade e imutabilidade das transações. A DAO foi implementada na rede Ethereum, utilizando um token ERC-20 simulado (mock) para transações, garantindo compatibilidade com o emergente token digital brasileiro DREX. O projeto demonstra como a tecnologia blockchain pode transformar a relação entre governo e sociedade, promovendo uma governança mais transparente e participativa.

Palavras-chave: Blockchain; DAO; Contratos Inteligentes; Ethereum.

ABSTRACT

This project explores the potential of Decentralized Autonomous Organizations (DAOs) to improve the oversight of public activities, fostering transparency, accountability, and citizen participation in resource management. By leveraging blockchain technology and the emerging Brazilian digital token DREX, we propose the creation of a DAO that enables citizens to monitor and verify all stages of public-interest projects in their neighborhoods, from the initial proposal through to final execution. This work presents the development of the Bairro DAO, a platform designed to enhance transparency in local public services. Expected benefits include increased transparency, reduced corruption, and more efficient use of public resources. Based on blockchain technology and smart contracts, the platform allows citizens to track and verify every phase of civic projects at the local level, ensuring traceability and immutability of transactions. The DAO was implemented on the Ethereum network, using a mock ERC-20 token for transactions, ensuring compatibility with the emerging Brazilian digital token DREX. This project demonstrates how blockchain technology can transform the relationship between government and society, promoting more transparent and participatory governance.

Keywords: Blockchain; DAO; Government Transparency; BRZ; Smart Contracts; Ethereum.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
BRZ	Brazilian Real Token
CBDC	Central Bank Digital Currency
DAO	Decentralized Autonomous Organization
dApp	Decentralized Application
DREX	Digital Real Experience (token digital brasileiro)
EVM	Ethereum Virtual Machine
ETH	Ether (criptomoeda nativa da Ethereum)
ICO	Initial Coin Offering
NFT	Non-Fungible Token
PoS	Proof of Stake
PoW	Proof of Work

SUMÁRIO

1 INTRODUÇÃO

No final da década de 2000, o mundo testemunhou o surgimento de uma tecnologia revolucionária que transformaria o panorama das finanças digitais e da computação distribuída. A partir da publicação do white paper de Satoshi Nakamoto (2008), a tecnologia blockchain passou a ser entendida não apenas como a base para uma nova forma de moeda digital, mas também como um recurso capaz de viabilizar sistemas descentralizados, transparentes e resistentes à censura. Esse avanço lançou as bases para uma ampla gama de aplicações em diversos setores, redefinindo a forma como confiança, governança e transações são geridas na era digital.

Nas últimas décadas, a administração pública tem enfrentado o desafio de manter transparência, eficiência e participação cidadã em seus processos. A crescente demanda da sociedade por serviços mais ágeis, verificáveis e menos sujeitos a corrupção impulsiona a busca por soluções tecnológicas que tornem a gestão pública mais aberta e responsável. Nesse contexto, a tecnologia blockchain, com sua capacidade de registrar transações de maneira descentralizada, imutável e auditável, desponta como uma alternativa promissora (SWAN, 2015). Sua adoção pode contribuir para superar obstáculos ligados à opacidade, burocracia e dificuldade de monitoramento dos recursos públicos.

É neste cenário que as Organizações Autônomas Descentralizadas (DAOs) entram em cena, oferecendo um modelo organizacional baseado em contratos inteligentes (*smart contracts*) e regido pelo voto de seus membros, sem a necessidade de intermediários (BUTERIN, 2014). Uma DAO é um tipo de organização digital que funciona por meio de regras codificadas em blockchain, permitindo que decisões sejam tomadas coletivamente de forma transparente, auditável, imutável e democrática. Estando integrada com uma rede blockchain, a plataforma permite que seus usuários verifiquem todas as informações e todo histórico de transações, sem se preocupar com a falta de confiança que muitas vezes se faz presente em setores governamentais. Ao eliminar hierarquias rígidas e as burocracias contidas nelas, as DAOs proporcionam um ambiente em que as políticas, os gastos e as ações podem ser deliberados e executados conforme a vontade coletiva dos participantes, apresentando uma nova forma de se discutir a execução de trabalhos na área pública, distribuindo o poder de decisão e assegurando maior engajamento comunitário.

A proposta deste trabalho é o desenvolvimento de uma aplicação prática da tecnologia blockchain voltada para a integração coletiva na verificação e fiscalização de atividades do

setor público em âmbito local. A Bairro DAO visa oferecer uma plataforma transparente, descentralizada e segura para que cidadãos possam acompanhar, propor e participar da gestão de serviços públicos em sua comunidade. Ao utilizar a rede Ethereum, a plataforma integra transações financeiras rastreáveis por meio de contratos inteligentes auto executáveis, garantindo que todas as etapas do processo – desde a submissão de propostas até a execução de pagamentos a fornecedores – sejam verificáveis e imutáveis.

A natureza descentralizada reduz a dependência de intermediários, diminuindo oportunidades de corrupção e falhas administrativas. A DAO dá voz direta aos cidadãos, que passam a ter poder de influenciar o destino de recursos e a priorização de obras, aumentando a legitimidade das decisões. A imutabilidade do registro em blockchain assegura que decisões e transações não sejam adulteradas retroativamente, fortalecendo a confiança no processo decisório. Além disso, facilita o monitoramento contínuo dos projetos, permitindo que os cidadãos fiscalizem o andamento das obras e serviços de seu bairro, aumentando o senso de responsabilidade compartilhada e engajamento cívico.

Em síntese, ao propor a Bairro DAO, este trabalho se insere no debate sobre novas formas de governança pública, demonstrando como a combinação de blockchain, contratos inteligentes e DAOs pode trazer mais eficiência à gestão pública, atendendo a anseios sociais por processos mais abertos e colaborativos.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Viabilizar uma Organização Autônoma Descentralizada (DAO) que permita o monitoramento e gestão transparente de recursos públicos na execução de diferentes serviços, utilizando tecnologia blockchain, podendo através de uma aplicação auto soberana garantir transparência, responsabilidade e participação direta dos cidadãos na supervisão governamental. A proposta visa criar um sistema participativo, onde os cidadãos possam verificar e votar em todas as etapas de serviços públicos, desde a proposta inicial até o pagamento final, promovendo uma gestão financeira mais responsável.

1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

1. Desenvolver um sistema capaz de realizar transações financeiras de forma autônoma.
2. Permitir que usuários possam criar, votar e verificar propostas.

3. Realizar testes para garantir a integridade do sistema e a conexão com a rede blockchain

1.2 JUSTIFICATIVA

A proposta justifica-se pela crescente demanda por transparência na administração pública, onde a falta de ferramentas adequadas para participação pública tem resultado em ineficiências e perda de confiança por parte dos cidadãos. Além disso, o avanço da tecnologia blockchain demonstra ser uma alternativa viável para superar este desafio, permitindo maior envolvimento social.

1.3 ESTRUTURA DO DOCUMENTO

Este documento está organizado em onze capítulos, estruturados de forma a conduzir o leitor desde a contextualização teórica até os detalhes técnicos do desenvolvimento da Bairro DAO. A seguir, apresenta-se uma visão geral da estrutura do documento:

- ***Capítulo 1:Introdução***

  Apresenta o contexto do trabalho, destacando a importância da transparência em atividades públicas e a motivação para o desenvolvimento de uma DAO voltada para a fiscalização de obras públicas em bairros. São definidos os objetivos geral e específicos do projeto.
- ***Capítulo 2: Método de Pesquisa***

  Descreve a abordagem metodológica adotada, incluindo a pesquisa exploratória, o levantamento de requisitos, o design do sistema, o desenvolvimento do protótipo, os testes e validação, além desta seção que explica como o documento está organizado.
- ***Capítulo 3: Fundamentação Teórica***

  Fornece a base conceitual necessária para o entendimento do trabalho, abordando temas como blockchain, criptomoedas, Ethereum, contratos inteligentes e DAOs. Este capítulo contextualiza tecnicamente os elementos-chave utilizados no projeto.
- ***Capítulo 4: Trabalhos Correlatos***

  Analisa projetos e pesquisas semelhantes, destacando iniciativas que utilizam blockchain e DAOs para aprimorar processos governamentais. Esta comparação permite identificar desafios e oportunidades relevantes para o desenvolvimento.

- ***Capítulo 5: Desenvolvimento***

  Detalha a proposta do projeto, apresentando a visão geral do sistema, a integração com o BRZ e os contratos inteligentes desenvolvidos. Este capítulo define os objetivos de desenvolvimento da plataforma.

  Aborda a análise de requisitos funcionais e não funcionais, além da implementação dos contratos inteligentes. São descritas as funcionalidades dos contratos, suas responsabilidades e os mecanismos de segurança adotados.

  Apresenta o protótipo desenvolvido, incluindo a arquitetura do sistema, o desenvolvimento detalhado dos contratos inteligentes, a integração com o BRZ e os testes práticos realizados. Este capítulo é o mais técnico e detalhado do trabalho.

- ***Capítulo 6: Conclusão***

  Resume os resultados alcançados, avaliando a viabilidade técnica e os benefícios da implementação da DAO. São destacadas as contribuições do trabalho para a promoção da transparência e da participação cidadã na gestão pública.

  Apresenta sugestões para o desenvolvimento contínuo do projeto, incluindo o aprimoramento da interface gráfica, a expansão do sistema para outros tipos de projetos públicos, a realização de testes em comunidades reais e a análise de conformidade legal e regulatória.

Esta estrutura foi concebida para proporcionar uma leitura fluida e coerente, permitindo que o leitor compreenda o desenvolvimento do projeto em profundidade. Cada capítulo constroi sobre o anterior, garantindo que os conceitos e implementações sejam apresentados de forma lógica e progressiva. Assim, o documento oferece uma visão completa do processo de concepção, desenvolvimento e avaliação da plataforma, bem como de suas implicações práticas e teóricas.

2 MÉTODO DE PESQUISA

A metodologia foi constituída a partir de etapas que incluem pesquisa exploratória focada nas tecnologias em questão, etapa essencial para obter uma sólida fundamentação teórica e entendimento do estado da arte de sistemas blockchain. Esta investigação inclui a análise de artigos acadêmicos, *white papers*, estudos de caso e relatórios técnicos. A pesquisa exploratória tem como objetivo identificar as melhores práticas, os principais desafios e as oportunidades de aplicação no campo das organizações autônomas descentralizadas.

Com base nos insights obtidos na pesquisa exploratória, a etapa seguinte consiste em fazer um levantamento de requisitos detalhados. Esta etapa envolverá a identificação e documentação das respectivas necessidades para o desenvolvimento do sistema. Os requisitos são classificados em duas categorias principais: requisitos funcionais, que descrevem as operações que o sistema deve realizar, e requisitos não funcionais, que especificam atributos de qualidade como segurança, desempenho e usabilidade.

2.1 PESQUISA EXPLORATÓRIA

Inicialmente, foi realizada uma pesquisa exploratória para compreender os conceitos fundamentais relacionados à blockchain, criptomoedas, contratos inteligentes e DAOs. Foram analisados artigos científicos, livros, *white papers* e estudos de caso que abordam a aplicação destas tecnologias na administração pública e em outros setores.

Além disso, foram investigados os desafios atuais enfrentados pela administração pública em termos de transparência, participação cidadã e eficiência na gestão de recursos. Estudos sobre corrupção, ineficiências burocráticas e falta de confiança serviram como base para justificar a necessidade de soluções inovadoras.

2.2 LEVANTAMENTO DE REQUISITOS

Com base nos insights obtidos durante a pesquisa exploratória, foram definidos os requisitos funcionais e não funcionais do sistema. Os requisitos funcionais incluem funcionalidades essenciais, como a submissão e gestão de propostas de serviços, permitindo que usuários cadastrem propostas detalhadas com informações como orçamento, prazo e benefícios esperados. Além disso, o sistema incorpora mecanismos de votação e aprovação de propostas por meio de um sistema de votação baseado em tokens de governança,

estabelecendo um quórum mínimo para aprovação. A liberação de pagamentos automatizados conforme o progresso das obras também é uma funcionalidade-chave, integrando uma *stablecoin* para transações financeiras e automatizando a liberação de pagamentos conforme marcos definidos.

Os requisitos não funcionais também abordam aspectos cruciais do sistema, seguindo melhores práticas de desenvolvimento seguro. A escalabilidade é outro fator importante, garantindo que o sistema possa processar múltiplas propostas e votações simultaneamente, suportando o crescimento no número de usuários e transações através de uma arquitetura que facilita futuras expansões.

A ênfase na transparência e na auditoria, através do registro imutável de todas as transações e decisões na blockchain, disponibiliza ferramentas para consulta e auditoria pública, fortalecendo a confiança dos usuários no sistema.

2.3 DESENVOLVIMENTO E TESTE

Foi elaborado o design arquitetônico do sistema, definindo os componentes principais, suas interações e as tecnologias a serem utilizadas. Foi optado pelo uso da rede Ethereum devido à sua robustez e capacidade de execução de contratos inteligentes complexos (DRESCHER, 2017).

A implementação do protótipo foi realizada utilizando a linguagem Solidity para o desenvolvimento dos contratos inteligentes. As ferramentas Truffle e Ganache foram utilizadas para facilitar o processo de desenvolvimento e testes (ETHEREUM FOUNDATION, 2021). Os contratos inteligentes desenvolvidos abrangem funcionalidades como criação e gestão de propostas, mecanismos de votação, liberação de pagamentos e gerenciamento de tokens de governança.

Foram realizados testes unitários e de integração para verificar o correto funcionamento dos contratos inteligentes.

3 FUNDAMENTAÇÃO TEÓRICA

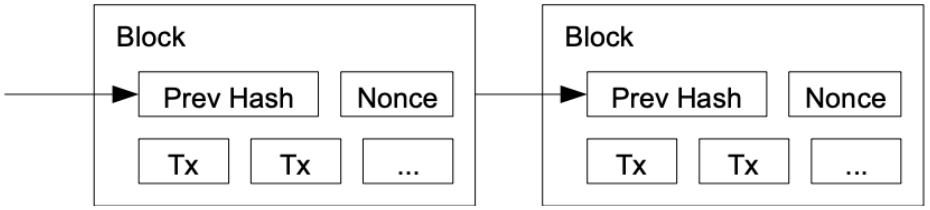
3.1 BLOCKCHAIN

3.1.1 Origem da Blockchain

A tecnologia blockchain emergiu em 2008 como a base para o Bitcoin, a primeira criptomoeda descentralizada, introduzida por um indivíduo ou grupo sob o pseudônimo de Satoshi Nakamoto. A blockchain foi concebida como uma solução para o problema do gasto duplo em transações digitais, eliminando a necessidade de uma autoridade central para verificar e validar transações (NAKAMOTO, 2008).

Blockchain é essencialmente um livro-razão distribuído e imutável que registra transações em uma rede descentralizada de computadores. Cada bloco na cadeia contém um conjunto de transações e um hash criptográfico que o vincula ao bloco anterior, garantindo segurança e integridade dos dados (NARAYANAN et al., 2016). Tendo os blocos encadeados entre si, o trabalho para alterar um deles resultaria numa alteração no resultado do hash de todos os blocos seguintes.

Figura 1 - Lista encadeada de blocos



Fonte: (NAKAMOTO, 2008)

3.1.2 Características Fundamentais

As principais características que definem uma blockchain são a descentralização, a imutabilidade, a transparência e a segurança. Na descentralização, não há uma autoridade central; a rede é mantida por nós (computadores) que validam e registram transações coletivamente. A imutabilidade garante que, uma vez que uma transação é registrada na blockchain, ela não pode ser alterada ou excluída, assegurando a integridade dos dados. A

transparência significa que todas as transações são públicas e podem ser visualizadas por qualquer participante da rede, aumentando a confiança no sistema. Por fim, a segurança é proporcionada pelo uso de criptografia avançada, que protege as transações e os dados armazenados, tornando o blockchain resistente a ataques e fraudes.

3.1.3 Evolução e aplicação

Após o sucesso inicial do Bitcoin, a tecnologia blockchain passou a ser explorada além das transações financeiras. Com o lançamento do Ethereum em 2015, que introduziu a funcionalidade de contratos inteligentes, a blockchain expandiu suas aplicações para múltiplos setores (BUTERIN, 2014). As suas aplicações incluem finanças descentralizadas (DeFi), oferecendo serviços financeiros sem intermediários, como empréstimos e investimentos (SCHÄR, 2021); gestão da cadeia de suprimentos, permitindo o rastreamento de produtos desde a origem até o consumidor final, garantindo autenticidade e ética (KOSHY et al., 2018); registros de propriedade, proporcionando um registro seguro e transparente de propriedades imobiliárias e outros ativos (ZHENG et al., 2017); votação eletrônica, com sistemas de votação seguros que previnem fraudes e aumentam a confiança nos resultados eleitorais (HARDY; MAURO, 2017); e na área da saúde, facilitando a gestão de registros médicos eletrônicos, garantindo privacidade e interoperabilidade entre sistemas (AZARIA et al., 2016).

Apesar de seu potencial, a tecnologia blockchain enfrenta desafios como a escalabilidade, já que a capacidade de processar um grande número de transações por segundo é limitada, afetando a adoção em larga escala (ZHENG et al., 2017). O consumo de energia é outro problema, pois o mecanismo de consenso de prova de trabalho (*PoW*) utilizado por algumas blockchains consome grandes quantidades de energia (VRIGNAUD et al., 2019). Além disso, a falta de regulamentação clara em muitos países cria incertezas jurídicas para empresas e usuários (FINCK, 2018).

3.1.4 Custo de verificação

A eficiência de setores depende da capacidade dos participantes de verificar atributos das transações, garantindo que ambas as partes cumpram suas obrigações. Em transações tradicionais, especialmente aquelas realizadas pessoalmente, compradores podem avaliar diretamente a qualidade dos bens ou serviços, enquanto vendedores verificam a autenticidade do pagamento. No entanto, à medida que os mercados se expandem geograficamente e as

transações tornam-se digitais, a necessidade de intermediários para assegurar a confiança entre as partes aumenta significativamente (CATALINI; GANS, 2016).

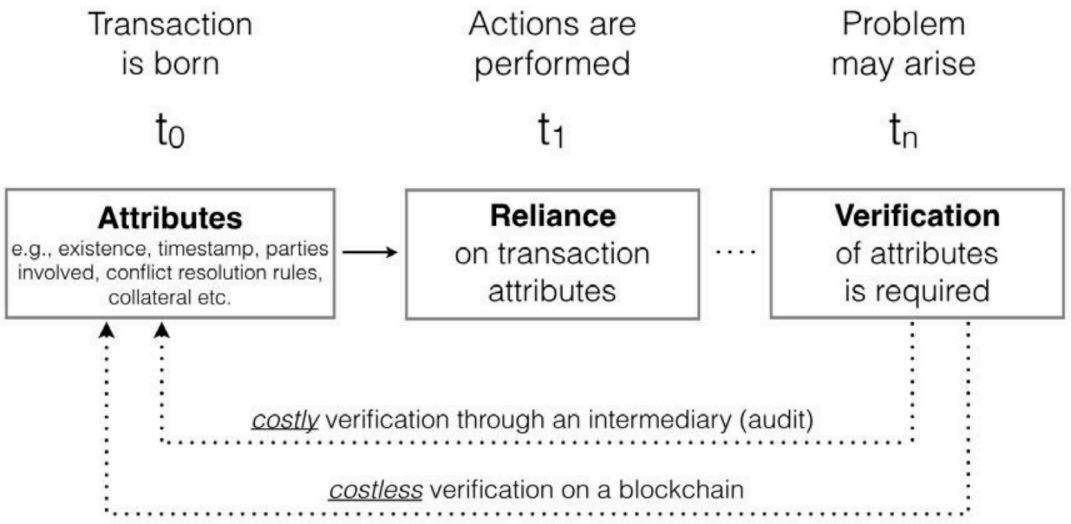
Em uma organização como a Bairro DAO, o uso da tecnologia blockchain reduz substancialmente o custo de verificação. A blockchain permite que transações sejam registradas de forma transparente e imutável, eliminando a necessidade de intermediários tradicionais, como instituições financeiras ou órgãos governamentais, que normalmente cobram taxas por seus serviços de verificação e introduzem riscos de privacidade e censura.

Ao utilizar contratos inteligentes, a DAO possibilita que os participantes verifiquem autonomamente atributos das transações e executem acordos automaticamente quando condições predefinidas são atendidas. Isso aumenta a eficiência ao reduzir os custos associados à necessidade de confiança em terceiros. Por exemplo, na contratação de uma obra pública, os cidadãos podem verificar o andamento do projeto e a utilização dos recursos em tempo real, sem depender de relatórios fornecidos por intermediários ou autoridades centralizadas.

Entretanto, é importante reconhecer que, embora a blockchain reduza os custos de verificação para informações digitais, ainda existem desafios significativos na interface entre registros digitais ("on-chain") e eventos do mundo real ("off-chain"). A precisão dos dados inseridos na blockchain é crucial; se informações incorretas ou fraudulentas forem registradas, a confiabilidade do sistema pode ser comprometida. No caso, isso significa que a confiança dos participantes no que está sendo descrito pelo participante *proposer* condiz com a realidade, garantindo que o progresso físico das obras públicas seja registrado corretamente na blockchain.

Além disso, a ausência de intermediários tradicionais também implica na necessidade de soluções alternativas para problemas como disputas entre partes ou falhas na execução de contratos. Enquanto os contratos inteligentes podem automatizar a execução com base em parâmetros pré-estabelecidos, eles não podem, por si só, lidar com todas as nuances e imprevistos que podem surgir em projetos do mundo real.

Figura 2 - Custo de verificação



Fonte: (CATALINI; GANS, 2016)

No modelo baseado em blockchain, a verificação é inerente ao funcionamento da rede descentralizada. As transações são registradas em um livro-razão distribuído, onde todos os participantes da rede podem verificar a autenticidade e integridade dos dados. No entanto, é importante notar que esse processo não é totalmente isento de custos, uma vez que as taxas de transação (*gas fees*) são necessárias para remunerar os validadores da rede (CATALINI; GANS, 2016). Apesar disso, os custos podem ser menores em comparação com os modelos tradicionais, especialmente quando considerados os benefícios adicionais de transparência e segurança.

3.1.5 Algoritmos de consenso

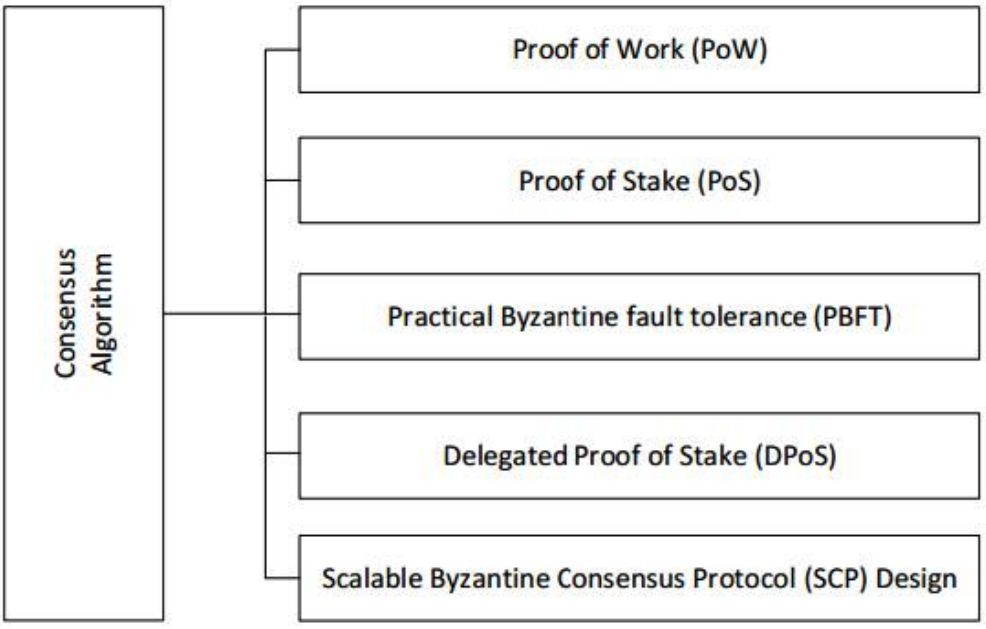
É importante considerar que, embora a blockchain reduza significativamente os custos de verificação ao eliminar intermediários e permitir acesso direto aos dados, o uso da rede implica em custos associados às taxas de transação, conhecidas como *gas fees*. Essas taxas são pagas aos mineradores ou validadores que processam e confirmam as transações na rede, garantindo sua segurança e integridade.

Os algoritmos de consenso são mecanismos fundamentais que permitem que os nós em uma rede blockchain distribuída concordem sobre o estado atual do livro-razão (ledger) e validem novas transações de forma segura. Eles garantem que todas as transações registradas na blockchain sejam legítimas e que não haja inconsistências ou gastos duplos. Dois dos

algoritmos de consenso mais proeminentes são a Prova de Trabalho (*Proof of Work* - PoW) e a Prova de Participação (*Proof of Stake* - PoS). A compreensão desses algoritmos é essencial para analisar questões como taxas de transação (*gas fees*), eficiência energética e segurança da rede, especialmente no caso da rede Ethereum, utilizada na Bairro DAO.

Além dos algoritmos de consenso PoW e PoS, existem outros mecanismos relevantes, como o PBFT (Practical Byzantine Fault Tolerance), o DPoS (Delegated Proof of Stake) e o SCP (Stellar Consensus Protocol). O PBFT é um algoritmo que permite alcançar consenso em sistemas distribuídos mesmo na presença de até um terço de nós maliciosos ou falhos, sendo eficiente em redes permissionadas com número limitado de participantes, como em algumas implementações do *Hyperledger Fabric*. O DPoS é uma variação do PoS em que os detentores de tokens elegem delegados responsáveis por validar os blocos e manter a rede, aumentando a eficiência e a escalabilidade; esse modelo é utilizado em plataformas como a EOS e a Tron. Já o SCP é o protocolo de consenso da rede Stellar, que utiliza um sistema de acordos bizantinos federados para alcançar consenso rapidamente, permitindo transações de alta velocidade e baixo custo, ideal para aplicações que exigem alto desempenho e confirmação quase instantânea (ARCHANA PRASHANTH JOSHI MENG HAN, 2018).

Figura 3 – Algoritmos de consenso



Fonte: (ARCHANA PRASHANTH JOSHI MENG HAN, 2018)

Com a transição do Ethereum para o PoS, conhecida como "The Merge", espera-se que muitos dos desafios enfrentados com o PoW sejam mitigados. Para o sistema em questão, isso significa potencialmente taxas de transação mais baixas, maior eficiência e um ambiente mais robusto para operar. Compreender os algoritmos de consenso é essencial para planejar a implementação e o futuro desenvolvimento da plataforma, garantindo a melhor experiência possível para o cidadão.

3.1.5.1 Proof of Work (PoW)

A Prova de Trabalho (PoW) foi introduzida pela primeira vez como um conceito para combater spam e ataques de negação de serviço (DoS) por Cynthia Dwork e Moni Naor em 1993 (DWORK; NAOR, 1993). No contexto das criptomoedas, o PoW foi popularizado pelo Bitcoin, criado por Satoshi Nakamoto em 2008 (NAKAMOTO, 2008). O PoW é um mecanismo que exige que os participantes da rede resolvam problemas matemáticos complexos para validar novas transações e adicionar blocos à blockchain.

Os mineradores competem para resolver um desafio criptográfico que exige poder computacional significativo. Esse desafio geralmente envolve encontrar um valor chamado *nonce* que, quando combinado com os dados do bloco e passado por uma função hash, produz um hash que atende a certos critérios (por exemplo, um número de zeros iniciais).

O processo pode ser descrito da seguinte forma:

1. **Criação do Bloco:** Transações pendentes são agrupadas em um bloco candidato.
2. **Resolução do Problema:** Mineradores tentam adivinhar o *nonce* correto que satisfaz a condição do hash.
3. **Validação e Propagação:** O primeiro minerador a encontrar a solução transmite o bloco para a rede.
4. **Verificação pelos Nós:** Os outros nós verificam se o bloco e a solução são válidos.
5. **Adição à Blockchain:** Se válido, o bloco é adicionado à blockchain, e o minerador recebe uma recompensa.

O PoW é conhecido por seu alto consumo de energia, pois requer hardware especializado e grande poder computacional (VRIGNAUD et al., 2019). Este consumo energético se traduz em custos operacionais elevados para os mineradores, que muitas vezes são repassados aos usuários na forma de taxas de transação mais altas. No Ethereum, que

utilizava PoW até recentemente, essas taxas são pagas em forma de *gas fees*, que remuneram os mineradores pelo processamento das transações.

A segurança do PoW deriva da dificuldade em comprometer a rede, pois um atacante precisaria controlar mais de 50% do poder computacional total para subverter o consenso (NARAYANAN et al., 2016). No entanto, a concentração de poder de mineração em grandes pools pode levar à centralização, o que é contrário aos princípios fundamentais da tecnologia blockchain.

3.1.5.2 Proof of Stake (PoS)

A Prova de Participação (PoS) foi proposta como uma alternativa ao PoW para abordar questões de escalabilidade, eficiência energética e descentralização. O conceito foi introduzido em 2011 por Sunny King e Scott Nadal no projeto Peercoin (KING; NADAL, 2012). No PoS, a probabilidade de um nó validar o próximo bloco é proporcional à quantidade de criptomoedas que ele possui e está disposto a "apostar" ou "congelar" como garantia.

No PoS, os validadores são selecionados com base em sua participação na rede:

1. **Seleção do Validador:** Os validadores são escolhidos de acordo com a quantidade de criptomoedas que possuem e comprometeram como garantia.
2. **Validação do Bloco:** O validador selecionado cria o próximo bloco, validando as transações e adicionando-o à blockchain.
3. **Recompensas e Penalidades:** O validador recebe recompensas por validar corretamente o bloco. Se agir de forma maliciosa, pode perder sua participação (garantia).
4. **Redução de Consumo Energético:** Como não há necessidade de resolver problemas matemáticos complexos, o consumo de energia é significativamente menor.

O PoS reduz drasticamente o consumo de energia, tornando a rede mais sustentável e potencialmente reduzindo as taxas de transação. No Ethereum 2.0, que está migrando para PoS, espera-se que o mecanismo de consenso melhore a escalabilidade e diminua as *gas fees*, beneficiando usuários e desenvolvedores de contratos inteligentes (BUTERIN, 2020).

A segurança no PoS depende de incentivos econômicos. Validadores têm interesse em agir corretamente para não perder suas participações. No entanto, o PoS enfrenta desafios como o "Nada em Jogo", onde validadores podem tentar validar múltiplas versões da blockchain sem custo adicional (KRAVCHENKO, 2016). Protocolos avançados e mecanismos de punição foram desenvolvidos para mitigar esses riscos.

3.2 CRIPTOMOEDAS

3.2.1 Surgimento e Funcionamentos das Criptomoedas

As criptomoedas surgiram como uma aplicação direta da tecnologia blockchain, sendo o Bitcoin a primeira e mais conhecida delas. Concebido por Satoshi Nakamoto em 2008, o Bitcoin foi projetado como uma forma de dinheiro eletrônico peer-to-peer, permitindo transações financeiras sem a necessidade de intermediários tradicionais, como bancos ou instituições financeiras (NAKAMOTO, 2008).

São ativos digitais que utilizam criptografia para garantir a segurança das transações e controlar a criação de novas unidades. Elas operam em redes descentralizadas baseadas em blockchain, onde as transações são registradas em um livro-razão público, imutável e transparente (ANTONOPOULOS, 2017).

- **Descentralização:** Não são emitidas por instituições governamentais.
- **Segurança:** Criptografia avançada protege as transações e previne fraudes.
- **Transparência:** As transações são públicas.
- **Imutabilidade:** Uma vez confirmadas, as transações não podem ser alteradas.

As principais características das criptomoedas incluem a descentralização, pois não são emitidas ou controladas por governos ou instituições financeiras; a segurança, garantida pela criptografia avançada que protege as transações e previne fraudes; a transparência e o pseudoanonimato, já que as transações são públicas, mas os usuários podem manter-se anônimos; e a imutabilidade, uma vez que as transações, após confirmadas, não podem ser alteradas ou excluídas.

Após o surgimento do Bitcoin, uma infinidade de outras criptomoedas, conhecidas como altcoins, foram desenvolvidas, cada uma buscando aprimorar ou adaptar os conceitos originais para diferentes propósitos e aplicações. Essa diversificação tem impulsionado a inovação no ecossistema de criptomoedas, levando ao surgimento de plataformas com funcionalidades e características únicas.

- Criptomoedas notáveis:
    - **Ethereum (ETH):** Introduziu contratos inteligentes e aplicativos descentralizados (dApps), permitindo que desenvolvedores criem e implantem programas autônomos na blockchain (BUTERIN, 2014).
    - **Ripple (XRP):** Focado em soluções para pagamentos internacionais entre instituições financeiras, visando transações rápidas e de baixo custo (SCHWARTZ et al., 2014).
    - **Litecoin (LTC):** Criado como uma "prata para o ouro do Bitcoin", oferece confirmações de transações mais rápidas e um algoritmo de mineração diferente (SCRYPT) (LEE, 2011).
    - **Solana (SOL):** Uma plataforma blockchain de alta performance que utiliza o mecanismo de consenso Proof of History (PoH) combinado com Proof of Stake (PoS), permitindo uma alta taxa de transações por segundo (TPS) com baixas taxas de transação (YAKOVENKO, 2018). A Solana ganhou destaque por sua escalabilidade e tem sido utilizada para aplicações financeiras descentralizadas (DeFi) e tokens não fungíveis (NFTs).

Essa evolução e diversificação são impulsionadas por diferentes objetivos. Projetos como Solana e Polkadot buscam aumentar o número de transações que podem ser processadas por segundo, abordando uma das limitações do Bitcoin e Ethereum em suas versões originais. Monero (XMR) e Zcash (ZEC) focam em fornecer transações verdadeiramente anônimas, protegendo a privacidade dos usuários.

3.2.2 Stablecoins

Stablecoins são criptomoedas projetadas para minimizar a volatilidade de preço típica das criptomoedas convencionais, sendo geralmente atreladas a ativos estáveis como moedas fiduciárias (por exemplo, dólar ou euro), commodities (como ouro) ou cestas de ativos (MUSLIMIN; NAZIEF, 2020). O objetivo das stablecoins é combinar os benefícios da tecnologia blockchain, como a rapidez nas transações e a segurança, com a estabilidade de valor proporcionada pelos ativos tradicionais.

Entender estas criptomoedas é parte fundamental no desenvolvimento do projeto porque os fundos da nossa Organização Autônoma Descentralizada (DAO) são controlados por contratos inteligentes que movimentam *stablecoins*. Ao utilizá-las, garantimos que os valores transacionados mantenham uma paridade com ativos estáveis, reduzindo a exposição à volatilidade comum em criptomoedas como Bitcoin ou Ether. Isso é especialmente importante em um contexto de gerenciamento de fundos públicos ou comunitários, onde a preservação do valor é crucial para o planejamento e execução de projetos.

Existem diferentes tipos de *stablecoins*, categorizadas de acordo com o mecanismo utilizado para manter a estabilidade de preço:

- *Stablecoins* lastreadas em moeda fiduciária: São suportadas por reservas de moeda fiduciária mantidas por uma entidade centralizada. Cada unidade da stablecoin corresponde a uma unidade da moeda fiduciária. Exemplos incluem Tether (USDT) e USD Coin (USDC).
- *Stablecoins* lastreadas em criptomoedas: Utilizam outras criptomoedas como colateral para manter sua estabilidade. Como as criptomoedas são voláteis, essas stablecoins geralmente são supercolateralizadas para absorver flutuações de preço. Um exemplo é a DAI, que é colateralizada em Ether (ETH) e outras criptomoedas.
- *Stablecoins* algorítmicas: Não possuem colateral, mas utilizam algoritmos e contratos inteligentes para controlar a oferta e a demanda, mantendo o preço estável.

As *stablecoins* desempenham um papel fundamental no ecossistema de criptomoedas, facilitando transações, servindo como reserva de valor estável e permitindo a participação em aplicações de finanças descentralizadas (DeFi). O uso de *stablecoins* contribui para a transparência e auditabilidade das transações financeiras dentro da plataforma. Todas as movimentações são registradas na blockchain, permitindo que membros da comunidade e auditores externos acompanhem o fluxo de recursos em tempo real. Isso é fundamental para promover a responsabilidade fiscal e combater a corrupção na gestão de fundos públicos.

Estas criptomoedas também desempenham um papel importante na mitigação de riscos cambiais em transações internacionais ou em contextos onde a moeda local é volátil. Ao utilizar uma *stablecoin* atrelada a uma moeda forte ou ao próprio real, é possível proteger os fundos contra depreciações abruptas, garantindo que os recursos disponíveis para os projetos mantenham seu poder de compra ao longo do tempo.

Em suma, as stablecoins proporcionam uma combinação de estabilidade financeira com os benefícios tecnológicos das criptomoedas, como segurança, transparência e eficiência. Sua integração no projeto da Bairro DAO é essencial para assegurar que as operações financeiras sejam conduzidas de maneira confiável, segura e alinhada às necessidades da comunidade local.

3.2.2.1 DREX

O token digital brasileiro representa a versão digital do Real, mantendo o mesmo valor e reconhecimento legal da moeda física. Projetado para operar em uma infraestrutura baseada em blockchain, o DREX é compatível com a Ethereum Virtual Machine (EVM), permitindo a execução de contratos inteligentes e integração com aplicativos descentralizados (BANCO CENTRAL DO BRASIL, 2023). Essa compatibilidade facilita a interoperabilidade e a integração com soluções já estabelecidas, reduzindo custos de desenvolvimento e promovendo a adoção.

A iniciativa busca facilitar transações mais rápidas e eficientes, potencializando o desenvolvimento de novos modelos de negócio e serviços financeiros. Além disso, por ser emitido e controlado pelo Banco Central, o DREX garante segurança jurídica e estabilidade monetária, fatores essenciais para a confiança dos usuários e para a estabilidade econômica.

A compatibilidade do DREX com a EVM é altamente relevante para a organização, pois permite que a plataforma seja desenvolvida utilizando contratos inteligentes e uma infraestrutura já familiar aos desenvolvedores e usuários do Ethereum. Integrar o DREX como meio de transação na organização significa ser pioneira no desenvolvimento do setor governamental, inovando em direção a uma maior transparência, participação e confiança pública nas atividades de serviço público.

Primeiramente, o DREX proporciona estabilidade monetária, uma vez que é lastreado no Real e emitido pelo Banco Central, reduzindo riscos associados à volatilidade de criptomoedas tradicionais. Isso facilita a compreensão e adoção por parte da população local, que pode transacionar em uma moeda digital que representa o Real, sem a necessidade de lidar com conversões ou flutuações cambiais significativas.

Além disso, o uso do DREX garante conformidade com as regulamentações financeiras brasileiras, aspecto crucial para um projeto voltado à gestão de recursos públicos. A adoção de uma moeda digital oficial promove transparência nas transações e pode facilitar a integração com sistemas governamentais e instituições financeiras.

3.2.2.2 BRZ

O BRZ é uma *stablecoin* brasileira lastreada no real (BRL), o que significa que cada BRZ emitido corresponde a um real em reserva (TRANSFERO SWISS, 2021). Isso proporciona estabilidade e confiabilidade, tornando o BRZ adequado para transações financeiras dentro da DAO enquanto o token digital brasileiro oficial não for lançado.

A utilização do BRZ traz consigo estabilidade de valor, conformidade regulatória e facilidade de conversão. Minimizando a volatilidade comum em outras criptomoedas, alinhando às regulamentações brasileiras, facilitando a adoção e futuramente poderá ser facilmente convertido para DREX, graças a compatibilidade com *Ethereum Virtual Machine* (EVM), permitindo a interação com o sistema financeiro governamental brasileiro.

3.3 ETHEREUM

3.3.1 Origem e Desenvolvimento do Ethereum

O Ethereum foi proposto em 2013 por Vitalik Buterin como uma plataforma descentralizada capaz de executar contratos inteligentes, expandindo as funcionalidades da tecnologia blockchain para além das transações financeiras simples (BUTERIN, 2014). Lançado oficialmente em 2015, o Ethereum tornou-se a segunda maior blockchain em termos de capitalização de mercado e uso (WOOD, 2014).

A arquitetura do Ethereum permite a criação e execução de contratos inteligentes e aplicativos descentralizados (dApps). Um componente fundamental é a Ethereum Virtual Machine (EVM), um ambiente de execução que processa contratos inteligentes escritos em linguagens como Solidity (ETHEREUM FOUNDATION, 2021). O Ether (ETH) é a criptomoeda nativa do Ethereum, usada para pagar taxas de transação e recompensar os mineradores ou validadores que mantêm a rede. O conceito de "*gas*" é utilizado para medir o esforço computacional necessário para executar operações na rede, prevenindo abusos e ataques, pois cada operação consome uma quantidade específica de gás que deve ser paga em Ether.

O Ethereum tem sido a plataforma preferida para o desenvolvimento de contratos inteligentes, dApps e para a emissão de tokens seguindo padrões como ERC-20 (tokens fungíveis) e ERC-721 (tokens não fungíveis, ou NFTs). Sua flexibilidade e robustez têm impulsionado a inovação em áreas como finanças descentralizadas (DeFi), NFTs e organizações autônomas descentralizadas (DAOs).

A rede possui uma arquitetura que permite a criação e execução de contratos inteligentes e aplicativos descentralizados (dApps):

- Ethereum Virtual Machine (EVM): Ambiente de execução que processa contratos inteligentes escritos com a linguagem de programação Solidity (ETHEREUM FOUNDATION, 2021).
- Ether (ETH): A criptomoeda nativa do Ethereum, usada para pagar taxas de transação e recompensar mineradores.
- *Gas Fee*: Unidade que mede o esforço computacional necessário para executar operações na rede, prevenindo abusos e ataques.

3.3.2 *Smart Contracts*

Contratos inteligentes são programas auto executáveis que residem na blockchain. Concebidos inicialmente por Nick Szabo em 1994, eles automatizam acordos e transações, operando com base em condições predefinidas (SZABO, 1997). No Ethereum, os contratos inteligentes são escritos em linguagens específicas, como Solidity, e são executados na EVM.

Os contratos inteligentes surgiram para automatizar processos, reduzindo a intervenção humana e minimizando erros ou manipulações. Eles garantem o cumprimento de acordos, pois as ações programadas são executadas automaticamente quando as condições especificadas são atendidas. Por exemplo, um contrato inteligente pode ser programado para liberar um pagamento somente quando um serviço é concluído ou um produto é entregue.

Uma das principais vantagens dos contratos inteligentes é a transparência e a auditabilidade. Todas as ações e eventos associados são registrados na blockchain, permitindo auditorias independentes e garantindo a confiança entre as partes, mesmo sem a necessidade de intermediários. Em caso de disputas ou suspeitas de irregularidades, é possível rastrear exatamente quando e como uma determinada ação ocorreu.

Além disso, mecanismos podem ser implementados para lidar com exceções, como congelamento temporário de fundos ou suspensão de pagamentos até que uma situação seja resolvida. Isso adiciona uma camada de segurança e flexibilidade aos contratos inteligentes, tornando-os uma ferramenta poderosa para uma ampla gama de aplicações, desde finanças até governança.

Estes algoritmos automatizam a execução de acordos pré-estabelecidos, mas também registram todas as ações e eventos associados. Isso significa que, em caso de disputas ou suspeitas de irregularidades, é possível rastrear exatamente quando e como uma determinada ação ocorreu.

Além do Ethereum, plataformas como Cardano (ADA) e Tezos (XTZ) oferecem funcionalidades de contratos inteligentes com diferentes abordagens para governança e escalabilidade. Essa diversidade no ecossistema de criptomoedas permite que diferentes necessidades e casos de uso sejam atendidos, promovendo a inovação contínua. No entanto, também apresenta desafios em termos de interoperabilidade, segurança e regulamentação.

3.3.2.1 Decentralized Applications (dApps)

As Aplicações Descentralizadas, ou dApps (do inglês *decentralized applications*), são aplicações que operam em redes blockchain descentralizadas, como o Ethereum. Diferentemente das aplicações tradicionais, que dependem de servidores centralizados, as dApps funcionam em uma rede peer-to-peer, onde o código de backend é executado em contratos inteligentes na blockchain (JÄRVINEN et al., 2019).

Os dApps possuem características fundamentais que as distinguem das aplicações convencionais. Elas operam de forma descentralizada, armazenando código-fonte e dados em uma rede blockchain pública, o que evita pontos únicos de falha e aumenta a resistência a censuras. Muitas dApps são de código aberto, permitindo que a comunidade inspecione, verifique e contribua para seu desenvolvimento, promovendo transparência e colaboração.

Também utilizam tokens criptográficos para recompensar os participantes da rede e incentivar a manutenção do sistema. Estes tokens podem ser usados para acessar funcionalidades da aplicação ou como meio de troca dentro do ecossistema. As operações das dApps são regidas por protocolos e algoritmos criptográficos padronizados, garantindo consistência, segurança e confiança nos processos executados (ZHENG et al., 2017).

Alguns exemplos de dApps são:

- **Uniswap**: Plataforma de troca descentralizada que permite a negociação de tokens ERC-20 sem intermediários.
- **MakerDAO**: Plataforma que permite a criação de stablecoins descentralizadas, como a DAI, e incorpora mecanismos de governança comunitária.

3.3.2.2 Decentralized Autonomous Organization (DAO)

Uma Organização Autônoma Descentralizada (DAO) é uma forma inovadora de organização que opera por meio de regras codificadas como contratos inteligentes, sem gestão centralizada, e cujas decisões são tomadas coletivamente pelos seus membros (JENTZSCH, 2016). As DAOs utilizam a tecnologia blockchain para garantir a transparência, a imutabilidade e a execução automática das decisões tomadas.

As principais características das DAOs incluem a descentralização, onde não há uma hierarquia tradicional e as decisões são tomadas de forma coletiva; a autonomia, pois operam independentemente de intervenções humanas diretas após a implantação; e a transparência, já que as regras e transações são públicas e auditáveis na blockchain.

Implementadas em plataformas como o Ethereum, as DAOs executam protocolos definidos por contratos inteligentes, garantindo que as decisões acordadas pelos membros sejam executadas automaticamente. As decisões dentro de uma DAO são geralmente tomadas através de mecanismos de votação, onde a influência de cada membro é proporcional aos seus tokens de governança. Isso promove um ambiente democrático onde as políticas e orientações da organização são moldadas coletivamente pelos interesses e consenso dos seus membros, sem a necessidade de uma autoridade centralizada interferir no processo de tomada de decisão. Algumas aplicações e vantagens das DAOs são:

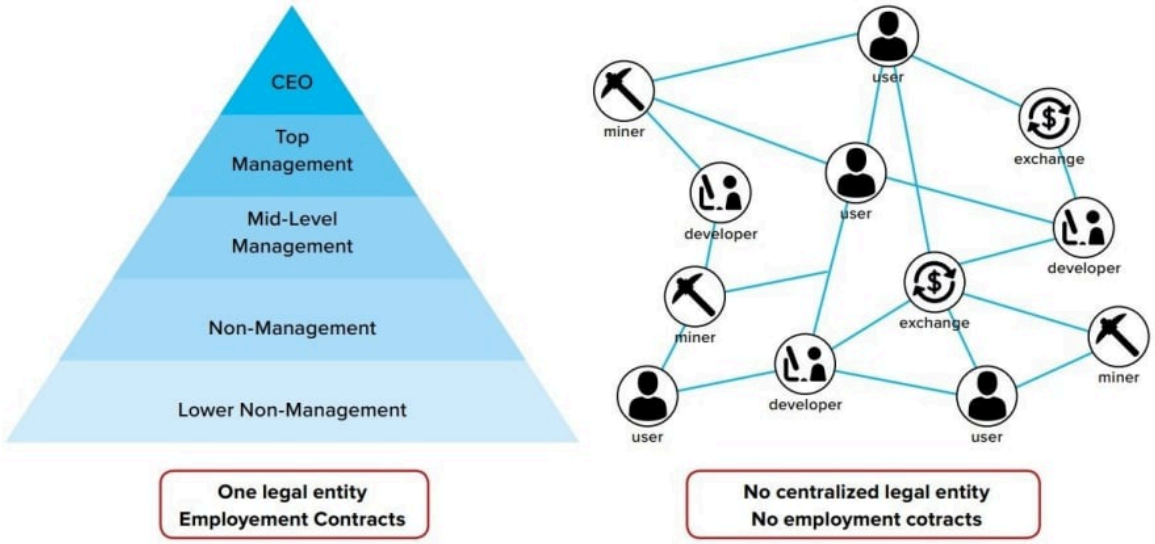
- Gestão de Projetos Open Source: Coordenação de esforços e recursos para desenvolvimento de software de forma colaborativa.
- Investimentos Coletivos: Fundos descentralizados onde membros decidem onde investir recursos, compartilhando riscos e retornos.
- Governança de Protocolos: Tomada de decisões sobre parâmetros e atualizações em protocolos financeiros descentralizados, garantindo que o desenvolvimento seja alinhado com os interesses dos usuários.

As vantagens das DAOs incluem a transparência e a confiança, com operações abertas que podem ser verificadas por qualquer membro; a participação democrática, onde membros têm voz proporcional nas decisões, promovendo engajamento; e a eficiência operacional, através da eliminação de intermediários e burocracias desnecessárias.

No contexto governamental, as DAOs podem promover a transparência nas decisões públicas, com registro aberto de decisões e gastos públicos. Elas também incentivam o engajamento cidadão, permitindo participação direta dos cidadãos na formulação de políticas e projetos, e contribuem para a redução da corrupção, através de processos automatizados que minimizam a intervenção humana e, consequentemente, a oportunidades de fraude.

Na Figura X, a organização tradicional é representada por uma estrutura hierárquica em formato de pirâmide, onde o poder e a tomada de decisões estão concentrados nos níveis superiores da hierarquia. Este modelo centralizado evidencia como as informações fluem de cima para baixo, limitando a participação dos níveis inferiores no processo decisório.

Figura 4 - *Comparing traditional organization and DAO*



Fonte: (MORALIS ACADEMY, 2021)

Em contraste, a DAO é ilustrada como uma rede descentralizada, onde todos os membros estão interconectados sem uma autoridade central dominante. Essa representação destaca a natureza distribuída das DAOs, na qual a governança é coletiva e as decisões são tomadas de forma colaborativa pelos participantes. A imagem enfatiza as diferenças fundamentais entre os modelos organizacionais, mostrando como as DAOs promovem maior participação, transparência e descentralização em comparação com as estruturas organizacionais tradicionais. Essa visualização reforça a compreensão de como a Bairro DAO busca inovar na gestão pública, adotando um modelo que incentiva o engajamento cidadão e a eficiência nos processos de tomada de decisão.

4 TRABALHOS CORRELATOS

Este capítulo apresenta uma análise detalhada de trabalhos e iniciativas que exploram o uso de blockchain, contratos inteligentes e DAOs em contextos similares ao do projeto. O objetivo é compreender os desafios, as soluções implementadas e os resultados obtidos por esses projetos, identificando práticas que podem ser incorporadas ou adaptadas para o desenvolvimento da Bairro DAO. São analisados trabalhos correlatos que se destacam pela relevância e pelas contribuições significativas nas áreas de governança descentralizada, participação cidadã e transparência pública.

4.1 *The DAO: A Primeira Organização Autônoma Descentralizada*

"The DAO" foi lançada em 2016 na plataforma Ethereum e é considerada a primeira Organização Autônoma Descentralizada notável. Seu principal objetivo era criar um fundo de investimento descentralizado que permitiria aos membros investir coletivamente em projetos de interesse, sem a necessidade de intermediários tradicionais como bancos ou instituições financeiras (SIEGEL et al., 2016). A DAO funcionaria através de contratos inteligentes, nos quais os investidores poderiam propor projetos, votar e decidir onde os fundos seriam alocados.

Para viabilizar "The DAO", foi realizada uma Oferta Inicial de Moedas (ICO) que arrecadou cerca de 150 milhões de dólares em Ether (ETH), tornando-se uma das maiores campanhas de *crowdfunding* da época. A estrutura da DAO baseava-se em contratos inteligentes complexos escritos em Solidity, a linguagem de programação do Ethereum. Esses contratos deveriam automatizar todo o processo de governança e investimento, desde a proposição de projetos até a distribuição de retornos financeiros.

Apesar do sucesso inicial na captação de recursos, "The DAO" enfrentou um grave problema de segurança. Em junho de 2016, um invasor explorou uma vulnerabilidade no código do contrato inteligente, conhecida como "recursive call vulnerability", e conseguiu desviar aproximadamente 50 milhões de dólares em ETH (ATZEI et al., 2017). Este incidente gerou uma crise na comunidade Ethereum e levantou questões sobre a segurança de contratos inteligentes e a viabilidade de DAOs.

Para mitigar os danos, a comunidade Ethereum optou por realizar um hard fork na blockchain, revertendo as transações fraudulentas. Isso resultou na divisão da rede em duas: Ethereum (ETH), que seguiu com o fork, e Ethereum Classic (ETC), que manteve a cadeia original sem alterações.

A experiência de "The DAO" ressalta a importância crucial da segurança no desenvolvimento de contratos inteligentes. Para a *Bairro DAO*, que envolve recursos públicos e participação cidadã, é indispensável adotar práticas rigorosas de desenvolvimento seguro.
Desde o incidente com "The DAO", a comunidade Ethereum e os desenvolvedores de contratos inteligentes têm trabalhado intensamente para prevenir vulnerabilidades semelhantes. Houve o desenvolvimento de ferramentas de análise e verificação, como o Mythril e o Oyente, que permitem a análise estática de contratos inteligentes e a detecção de possíveis vulnerabilidades antes da implantação. Essas ferramentas auxiliam os desenvolvedores na identificação de pontos fracos no código, permitindo correções antecipadas.

Além disso, foram adotados padrões de projeto seguros, como o padrão "Checks-Effects-Interactions", que orienta a ordem das operações em contratos inteligentes para minimizar riscos. O uso de bibliotecas confiáveis, como a OpenZeppelin, tornou-se prática comum. Essas bibliotecas fornecem implementações seguras de componentes comuns, reduzindo a probabilidade de erros de codificação. A linguagem Solidity passou por atualizações significativas para evitar armadilhas comuns e facilitar a escrita de código seguro, melhorando a documentação e oferecendo recursos que promovem a elaboração de contratos mais robustos.

O crescimento de empresas especializadas em auditorias de contratos inteligentes também contribuiu para a segurança. Essas auditorias independentes adicionam uma camada extra de verificação, identificando vulnerabilidades que podem passar despercebidas pelos desenvolvedores originais. Apesar de todas essas melhorias, a segurança dos contratos inteligentes continua sendo um desafio constante. Novas vulnerabilidades podem surgir, e erros humanos na codificação são sempre possíveis. Portanto, a segurança não pode ser garantida apenas por ferramentas e padrões; requer uma cultura de segurança e processos rigorosos de desenvolvimento que incluam testes extensivos, revisões de código e atualizações contínuas.

A segurança dos contratos inteligentes é melhor hoje do que em 2016, graças aos avanços em ferramentas, padrões e práticas de desenvolvimento. No entanto, riscos persistem, e a implementação de tal sistema deve ser realizada com planejamento cuidadoso, foco na segurança e atenção às implicações legais e sociais. É essencial seguir processos rigorosos de desenvolvimento, aderindo às melhores práticas de codificação, realizando auditorias independentes e implementando medidas de segurança robustas. Trabalhar em conjunto com órgãos reguladores é fundamental para assegurar que uma organização robusta opere dentro do marco legal, incluindo questões fiscais e de proteção ao consumidor. Combinar mecanismos descentralizados com estruturas tradicionais de governança pode ajudar a lidar com a responsabilidade e a prestação de contas, estabelecendo uma governança híbrida que aproveita o melhor dos dois mundos. Além disso, promover a educação digital e garantir que a plataforma seja acessível a todos os cidadãos é crucial para o sucesso da iniciativa.

4.2 GovChain: Blockchain na Administração Pública

O estudo conduzido por Ølnes et al. (2017), intitulado "Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Public Services", investiga o potencial da tecnologia blockchain na administração pública. O objetivo principal é analisar como os governos podem utilizar a blockchain para aprimorar a eficiência, a transparência e a confiança nos serviços públicos, enfrentando problemas como burocracia excessiva, corrupção e falta de credibilidade nas instituições governamentais.

A pesquisa envolveu uma revisão abrangente da literatura existente e a análise de casos de uso em diferentes países. Os autores identificaram áreas-chave onde a tecnologia blockchain poderia ser aplicada na esfera governamental. Uma dessas áreas é a de registros públicos, onde a implementação de registros imutáveis para propriedades, documentos oficiais e outros ativos pode garantir a integridade dos dados e facilitar o acesso por parte dos cidadãos e autoridades.

Outra aplicação relevante é a identidade digital. A criação de sistemas de identidade baseados em blockchain permitiria a autenticação segura dos indivíduos, dando ao cidadão controle sobre seus próprios dados pessoais e reduzindo o risco de fraude e roubo de identidade. No contexto da votação eletrônica, a blockchain pode ser utilizada para desenvolver sistemas que assegurem transparência, anonimato e resistência a fraudes, aumentando a confiança do público no processo eleitoral.

Além disso, o estudo destaca a importância da transparência fiscal. O rastreamento de despesas governamentais e contratos públicos por meio da blockchain pode facilitar auditorias independentes, combater a corrupção e promover uma gestão mais responsável dos recursos públicos.

O estudo concluiu que a tecnologia blockchain tem o potencial de revolucionar a administração pública, mas também identificou desafios significativos que precisam ser superados. Um dos principais desafios é a interoperabilidade, ou seja, a necessidade de integração com sistemas existentes e entre diferentes organizações governamentais. A escalabilidade também é uma preocupação, uma vez que as limitações técnicas atuais podem dificultar o suporte a grandes volumes de dados e transações necessários em nível governamental.

Questões regulamentares representam outro obstáculo. Há incertezas legais e a necessidade de regulamentações específicas que abranjam o uso da blockchain no setor público. Além disso, existe resistência cultural e organizacional à adoção de novas tecnologias, o que pode dificultar a implementação de soluções baseadas em blockchain.

Para a Bairro DAO, os insights de GovChain são valiosos na identificação de oportunidades e obstáculos na aplicação da blockchain em serviços públicos. O projeto pode:

- Adaptar casos de uso, implementando registros transparentes de propostas, votações e execução de obras.
- Planejar a escalabilidade, desenvolvendo uma arquitetura que suporte crescimento no número de usuários e transações.
- Envolver stakeholders, promovendo o envolvimento de autoridades locais e cidadãos para facilitar a adoção.

4.3 Decidim: Plataforma de Participação Cidadã

Decidim é uma plataforma digital de código aberto criada pela Prefeitura de Barcelona em 2016, com o objetivo de promover a participação cidadã na tomada de decisões municipais (FUSTER MORELL et al., 2017). A iniciativa busca fortalecer a democracia participativa, permitindo que cidadãos influenciem diretamente políticas públicas, projetos e investimentos que afetam suas comunidades.

A plataforma foi desenvolvida utilizando tecnologias web modernas e princípios de design centrado no usuário. Decidim oferece funcionalidades que permitem aos cidadãos

propor iniciativas, participar de debates públicos, votar em propostas e acompanhar a implementação de projetos. Todas as propostas e discussões são públicas e auditáveis, promovendo transparência e confiança no processo democrático. A plataforma é modular e extensível, possibilitando a integração com outras tecnologias, incluindo blockchain, para aprimorar a segurança e a imutabilidade dos registros.

Decidim teve ampla adoção em Barcelona, envolvendo milhares de cidadãos e resultando em diversas políticas e projetos implementados com base nas propostas e votações realizadas. A plataforma também foi adotada por outras cidades e organizações ao redor do mundo, demonstrando sua eficácia em promover participação cidadã. O sucesso de Decidim destaca a importância de facilitar o envolvimento de diferentes segmentos da população e de fornecer ferramentas acessíveis para que os cidadãos participem ativamente da governança local.

4.4 Smart Dubai: Blockchain em Serviços Governamentais

A iniciativa Smart Dubai, lançada em 2016 pelo governo dos Emirados Árabes Unidos, tem como meta transformar Dubai na primeira cidade do mundo totalmente alimentada por blockchain (SMART DUBAI, 2016). O objetivo é melhorar a eficiência dos serviços governamentais, reduzir custos operacionais e promover a inovação tecnológica, posicionando Dubai como líder global em tecnologias emergentes.

O projeto envolve a implementação de blockchain em diversas áreas, incluindo pagamentos governamentais, registros de propriedade, licenças, documentos oficiais e serviços comerciais. Ao digitalizar e automatizar processos administrativos por meio da blockchain, o governo busca reduzir a burocracia, agilizar transações e eliminar a necessidade de documentos físicos. Isso inclui a gestão de escrituras e transações imobiliárias, a emissão e verificação de documentos oficiais de forma segura e eficiente, e a facilitação de processos empresariais, como registro de empresas e contratos.

A iniciativa resultou em significativas reduções de custos e ganhos de eficiência. Estima-se que a economia em horas de trabalho e recursos financeiros seja substancial, permitindo que o governo redirecione esforços para áreas mais estratégicas. A confiança pública nos serviços governamentais aumentou devido ao uso de registros imutáveis, promovendo transparência e responsabilidade. Além disso, Dubai consolidou sua posição como referência em adoção de tecnologias emergentes, atraindo investimentos e talentos globais.

A experiência de Dubai demonstra como a blockchain pode ser integrada em serviços governamentais em grande escala. A Bairro DAO pode aprender com a abordagem estratégica de Smart Dubai, alinhando o projeto com políticas públicas e objetivos governamentais. Estabelecer parcerias estratégicas com empresas e organizações pode fortalecer a implementação e fornecer recursos adicionais. Desenvolver soluções que sejam acessíveis e úteis para os cidadãos aumenta a adoção e o impacto positivo da plataforma. Além disso, considerar o contexto local e adaptar as soluções às necessidades específicas da comunidade garantirá maior relevância e eficácia.

4.5 Open Government Partnership: Transparência e Participação Cidadã

A Open Government Partnership (OGP) é uma iniciativa internacional lançada em 2011, que visa promover governos mais transparentes, participativos e responsáveis (OGP, 2021). Governos participantes comprometem-se a implementar planos de ação com reformas concretas em áreas como transparência fiscal, acesso à informação e participação cidadã. O Brasil é um dos países fundadores da OGP e tem desenvolvido iniciativas para aprimorar a governança pública.

A OGP funciona por meio da elaboração de planos de ação nacionais, nos quais cada país estabelece compromissos específicos com metas claras e mensuráveis. A iniciativa promove a colaboração multissetorial, envolvendo governos, sociedade civil e setor privado. O monitoramento e a avaliação são componentes-chave, com acompanhamento dos progressos e avaliação independente dos resultados, garantindo que os compromissos sejam cumpridos e que os impactos sejam mensurados.

- Transparência: Abertura de dados e informações governamentais.
- Participação Cidadã: Envolvimento dos cidadãos na tomada de decisões.
- *Accountability*: Prestação de contas e responsabilidade governamental.

A OGP tem contribuído para maior transparência, com a abertura de dados governamentais e melhoria no acesso à informação. A iniciativa tem fortalecido o engajamento cidadão, criando canais para a participação ativa da população em processos decisórios. Isso tem resultado em políticas públicas mais alinhadas com as necessidades dos cidadãos e em maior confiança nas instituições. A implementação de mecanismos de prestação de contas e fiscalização também tem sido um instrumento eficaz no combate à corrupção. Os princípios e práticas da OGP podem orientar o projeto na promoção de uma

governança local mais aberta e participativa. Definir compromissos claros e estabelecer metas específicas para transparência e participação pode direcionar os esforços do projeto. A inclusão da comunidade é essencial; envolver os cidadãos desde a concepção até a implementação do projeto garante que as soluções atendam às necessidades reais e promovam o senso de propriedade. A transparência nos processos, com a publicação de dados e informações de forma acessível e compreensível, aumenta a confiança e o engajamento da população.

4.6 Civic: Identidade Digital Segura para DAOs

Civic é uma solução pioneira para identidade digital descentralizada, projetada para resolver desafios relacionados à autenticação segura e verificação de identidade em plataformas baseadas em blockchain (CIVIC, 2024). Sua aplicação em Organizações Autônomas Descentralizadas (DAOs) é particularmente relevante para garantir que apenas usuários autênticos participem de decisões e transações, aumentando a confiabilidade do sistema.

1. **Autenticação Descentralizada:**
    - O Civic utiliza verificadores descentralizados para autenticar usuários sem a necessidade de armazenar dados sensíveis em um servidor centralizado. Isso elimina riscos de violação de dados e fortalece a segurança das informações pessoais.
    - Na Bairro DAO, essa solução pode assegurar que apenas moradores cadastrados e autorizados possam propor, votar e fiscalizar projetos comunitários.
2. **Mitigação de Riscos de Fraude:**
    - A tecnologia Civic impede a criação de identidades falsas ou múltiplas, garantindo integridade no processo de governança.
    - Isso é essencial para impedir manipulação de votos ou participação de indivíduos não autorizados.
3. **Educação e Acessibilidade:**
    - Além de oferecer um sistema seguro, o Civic também promove educação digital para que os usuários compreendam como utilizar sua identidade digital. Isso é útil para garantir inclusão digital no contexto da Bairro DAO.

Civic tem sido utilizado em diversos cenários, incluindo aplicações como verificação de identidades em bolsas de criptomoedas, serviços financeiros descentralizados e processos eleitorais. Esses exemplos reforçam a viabilidade de seu uso em DAOs que exigem participação cidadã autêntica e segura.

Com a integração do Civic, a Bairro DAO poderia criar um sistema onde moradores cadastrados têm suas identidades verificadas sem comprometer a privacidade. Isso fortalece o processo de tomada de decisão e garante maior confiança entre os participantes, consolidando o princípio de transparência e responsabilidade.

4.7 MakerDAO: Um Caso de Sucesso em Governança Descentralizada

A MakerDAO é amplamente reconhecida como uma das DAOs mais bem-sucedidas no ecossistema blockchain (MAKERDAO, 2020). Ela gerencia a *stablecoin* DAI, um ativo digital totalmente descentralizado e lastreado por garantias on-chain. Este caso é um exemplo de como fundos podem ser gerenciados de forma segura e transparente sem depender de uma entidade centralizada.

- **Gestão Descentralizada:**
  - Todos os fundos e colaterais usados para emitir a *stablecoin* DAI são bloqueados em contratos inteligentes que operam sob regras definidas pela comunidade de governança.
  - A comunidade, por meio do token de governança MKR, vota nas mudanças de parâmetros, como taxas de juros e novos colaterais aceitos. Essas decisões são automaticamente implementadas pelos contratos inteligentes após as votações.
- **Transparência e Auditabilidade:**
  - Toda a gestão financeira é registrada na blockchain, permitindo que qualquer pessoa acompanhe as transações em tempo real.
  - Os contratos inteligentes imutáveis garantem que nenhuma decisão seja alterada ou revertida sem o consenso da comunidade.
- **Segurança Automática:**
  - Em caso de crises (como flutuações no valor dos colaterais), o sistema executa liquidações automáticas para proteger os fundos restantes e manter a estabilidade do DAI.

Assim como a MakerDAO gerencia colaterais para manter a estabilidade do token DAI, a Bairro DAO pode gerenciar recursos públicos de forma transparente e segura, garantindo que cada real investido em projetos seja rastreável e utilizado de acordo com as regras aprovadas pela comunidade. A experiência desta plataforma demonstra que é possível implementar um modelo de governança descentralizado, eficiente e resiliente, mesmo em sistemas complexos e com grandes volumes de fundos.

Um dos testes mais conhecidos do sistema ocorreu durante a "Quinta-Feira Negra" em março de 2020, quando o mercado de criptoativos enfrentou uma crise. Apesar das perdas iniciais, as ferramentas de governança e os contratos inteligentes da DAO garantiram a continuidade e estabilidade do sistema, mostrando a robustez do modelo descentralizado.

A experiência da MakerDAO é um exemplo poderoso de como fundos podem ser gerenciados exclusivamente por contratos inteligentes, eliminando o risco de controle centralizado. Ao adotar princípios semelhantes, a Bairro DAO pode assegurar que recursos públicos sejam usados de maneira responsável e transparente, aumentando a confiança dos cidadãos no sistema.

5 DESENVOLVIMENTO

5.1 VISÃO GERAL

Este capítulo descreve as etapas de desenvolvimento do sistema da Organização Autônoma Descentralizada, detalhando as funcionalidades dos contratos inteligentes, scripts de apoio, e prototipagem para validação do modelo. O desenvolvimento deste projeto DAO tem como objetivo implementar uma solução descentralizada para governança e gestão financeira de uma comunidade. A escolha de cada tecnologia foi estratégica para atender às necessidades do projeto. Integrando tecnologias robustas como blockchain Ethereum, contratos inteligentes em Solidity, e ferramentas como Truffle e Ganache. O objetivo principal foi criar uma solução funcional para a governança descentralizada, permitindo a criação e votação de propostas, além de gerenciar a distribuição de fundos. Cada componente foi projetado para atender às necessidades específicas da organização, alinhado aos princípios apresentados no capítulo de fundamentação teórica.

5.2 ANÁLISE DE REQUISITOS

Requisitos são uma descrição das necessidades para um determinado produto, onde o objetivo básico é identificar e documentar o que é realmente necessário, de forma a comunicar claramente essa informação tanto ao cliente quanto aos membros da equipe de desenvolvimento. A definição de requisitos de maneira não ambígua é de suma importância para que os riscos sejam identificados e não ocorram surpresas durante o desenvolvimento do produto (LARMAN, 2000). Os requisitos de um software podem ser classificados em Requisitos Funcionais (RF) e Requisitos Não Funcionais (RNF). Os Requisitos Funcionais são responsáveis por definir as funções e comportamentos do software, enquanto os Requisitos Não Funcionais dizem respeito às restrições de desenvolvimento, aspectos de desempenho, interfaces com o usuário, confiabilidade, segurança, manutenibilidade, portabilidade e padrões a serem seguidos. Esta seção detalha os requisitos identificados para a DAO.

5.2.1 Requisitos Funcionais

Para o levantamento dos Requisitos Funcionais do projeto, foram considerados os recursos mínimos necessários para o funcionamento adequado da aplicação e as principais funcionalidades esperadas em uma plataforma descentralizada. Os requisitos foram definidos com base nas necessidades identificadas durante a pesquisa exploratória e refletem as funcionalidades essenciais para promover a participação cidadã e a transparência na gestão de serviços públicos.

Tabela 1 - Requisitos Funcionais

ID	Descrição
RF-01	O sistema deve permitir que os membros da DAO submetam propostas para novos serviços.
RF-02	As propostas devem incluir um atributo de descrição contendo claras informações com justificativa, orçamento e cronograma.
RF-03	O sistema deve permitir que os membros da DAO votem nas propostas submetidas
RF-04	Cada membro deve ter um único token de voto para participar das decisões.
RF-05	O sistema deve calcular o quórum necessário para aprovação de uma proposta com base em regras predefinidas.
RF-06	Após aprovação, o sistema deve permitir a execução automatizada das ações associadas à proposta.
RF-07	O sistema deve liberar pagamentos de forma condicionada ao cumprimento de etapas das obras.

Fonte: Elaborado pelo autor

5.2.2 Requisitos Não Funcionais

Os Requisitos Não Funcionais estabelecem critérios de qualidade e restrições que o sistema deve atender para assegurar seu desempenho, segurança, usabilidade e conformidade com padrões. Para o projeto em questão, os RNFs foram definidos visando garantir a eficácia e a confiabilidade da plataforma, bem como a satisfação dos usuários.

Tabela 2 - Requisitos Não-Funcionais

ID	Descrição
RNF-01	O sistema deve garantir alta segurança contra fraudes e ataques cibernéticos, utilizando criptografia avançada.
RNF-02	O sistema deve ser capaz de processar múltiplas propostas e votações simultaneamente, garantindo escalabilidade.
RNF-03	O consumo de gas deve ser otimizado, minimizando os custos para os usuários ao interagir com os contratos.
RNF-04	O sistema deve garantir a imutabilidade de registros, impossibilitando alterações retroativas nas transações.
RNF-05	A implementação dos contratos inteligentes deve seguir os padrões ERC-20, garantindo compatibilidade com DREX.
RNF-06	A plataforma deve suportar atualizações nos contratos inteligentes sem comprometer os dados existentes ou a integridade do sistema.

Fonte: Elaborado pelo autor

5.3 TECNOLOGIAS

5.3.1 Ethereum

A escolha do algoritmo de consenso impacta diretamente o funcionamento e a eficiência da organização. Utilizando o Ethereum como plataforma base, é importante compreender as implicações dos mecanismos de consenso em termos de segurança, custos operacionais e sustentabilidade. No PoW, as *gas fees* podem ser altas devido à competição entre mineradores e ao consumo de energia. Isso pode desincentivar a participação de cidadãos na Bairro DAO devido aos custos associados a cada transação. O PoS promete melhorar a escalabilidade da rede Ethereum, permitindo que mais transações sejam processadas por segundo. Isso é crucial para o funcionamento fluido da DAO, especialmente se o número de usuários crescer. A redução no consumo de energia torna o PoS uma opção mais sustentável, podendo alinhar-se melhor com políticas públicas. Ambos os mecanismos têm vantagens e desafios em termos de segurança. É fundamental que a plataforma opere em uma rede confiável para garantir a integridade das transações.

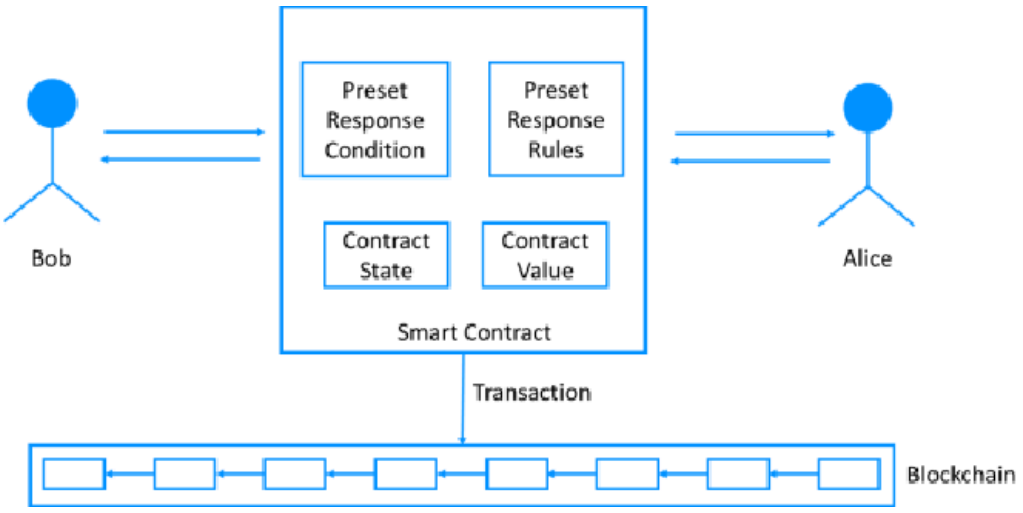
O Ethereum é uma rede blockchain amplamente utilizada para a execução de contratos inteligentes. No contexto do projeto, foi escolhida por sua capacidade de descentralização,

transparência, segurança e pelo amplo suporte intelectual disponível. Com uma estrutura baseada em proof-of-stake (PoS), o Ethereum possibilita que transações e contratos sejam executados de forma confiável. Isso o torna ideal para o caso de uso em questão, onde a confiança entre as partes é transferida para o código.

Com o objetivo de desenvolver um sistema com suporte ao DREX, a plataforma poderá automatizar pagamentos utilizando contratos inteligentes que liberam fundos em DREX conforme metas e condições previamente estabelecidas são atingidas. Todas as transações financeiras serão registradas na blockchain, permitindo auditorias e aumentando a confiança pública no gerenciamento dos recursos.

Na Figura 5, é ilustrado o funcionamento de uma transação por meio de contratos inteligentes utilizando os personagens Alice e Bob. A figura demonstra como Alice, desejando compartilhar dados com Bob, estabelece um contrato inteligente que define as condições de acesso e os termos da transação. O contrato inteligente atua como um intermediário autônomo e confiável, garantindo que as regras acordadas sejam executadas exatamente como programadas, sem a necessidade de intervenção de terceiros ou autoridades centrais. Este exemplo visual simplifica a compreensão de como contratos inteligentes podem automatizar processos e assegurar a integridade e transparência nas transações entre partes. A ilustração destaca a eliminação de intermediários tradicionais, reforçando a eficiência e a confiança proporcionadas pela tecnologia dos *smart contracts* nas interações descentralizadas.

Figura 5 - *Smart Contract Interaction*



Fonte: (WANG, 2018)

- Execução de contratos inteligentes, como os que gerenciam a governança e o tesouro.

- Registro imutável de dados e ações, como votos e transações financeiras.

5.3.1.1 Solidity

A linguagem Solidity foi utilizada para implementar os contratos inteligentes. Ela é especialmente projetada para a Ethereum Virtual Machine (EVM), oferecendo recursos específicos para manipulação de dados on-chain e segurança no controle de fundos no projeto, contratos como o ***BairroGovernance***, que define as regras de governança, ***Treasury***, responsável pela gestão financeira, e ***VoteToken***, responsável pelo token de governança.

5.3.1.2 OpenZeppelin

Os contratos do OpenZeppelin são amplamente reconhecidos como padrão de segurança e eficiência no desenvolvimento em Ethereum. A utilização deste padrão garante que os contratos estejam alinhados com as melhores práticas de segurança.

5.3.1.3 Truffle

Truffle é um framework que facilita o desenvolvimento, teste e implantação de contratos inteligentes. Ele oferece ferramentas para compilar contratos, migrá-los para redes locais ou públicas, e executar scripts. No projeto, o Truffle foi fundamental para organizar o desenvolvimento e garantir que os contratos fossem implementados corretamente em ambientes de teste.

5.3.1.4 Ganache

Ganache foi utilizado para simular uma blockchain local, proporcionando um ambiente controlado para testes. A ferramenta permite que os desenvolvedores interajam com os contratos em tempo real, podendo avançar blocos manualmente e verificar estados, como o resultado de propostas. A utilização de Ganache eliminou custos com *gas* e acelera o processo de validação do sistema.

5.3.1.5 JavaScript

Além de ser a base dos scripts utilizados no projeto, o JavaScript integrou perfeitamente com o Truffle e outras bibliotecas Ethereum, como `web3.js`. A linguagem goi utilizada para automatizar tarefas como criação de propostas, votação e execução.

5.3.1.6 Node.js

Node.js é a base para executar scripts e ferramentas de desenvolvimento como Truffle e Ganache. Este projeto requer a instalação de uma versão do Node.js (abaixo de 16.5.0), garantindo compatibilidade com as dependências do Truffle.

5.3.1.7 Web3.js

A biblioteca Web3.js é a ponte entre os contratos inteligentes e a interface do usuário ou scripts. Ela permite interagir com a blockchain Ethereum através de chamadas de função, transferências de tokens entre outras operações. Oferece uma API abrangente para interação com redes Ethereum, sendo uma escolha lógica para este tipo de aplicação.

5.3.1.8 Prettier

A formatação do código é garantida pelo Prettier, com suporte ao Solidity através do `prettier-plugin-solidity`. Essa ferramenta assegura que o código do contrato seja limpo, legível e consistente, promovendo boas práticas de desenvolvimento. A configuração personalizada no `package.json` evidencia o foco em padrões específicos para contratos inteligentes.

5.3.2 Integração com token fiduciário

A possível integração com os tokens DREX e BRZ no projeto possibilita adoção de usuários, permitindo que utilizem a moeda digital por meio de dispositivos móveis ou outros meios tecnológicos acessíveis como em uma transação bancária padrão. Isso promove a inclusão financeira e amplia o alcance da DAO, permitindo que mais membros da comunidade participem ativamente das decisões e do desenvolvimento local.

No contexto do Bairro DAO, a utilização do BRZ permite que as transações sejam realizadas na blockchain com segurança e transparência, mantendo a familiaridade e a

estabilidade da moeda local. Isso facilita a adoção pelos usuários, que podem participar sem se preocupar com flutuações cambiais significativas. A escolha do BRZ como moeda principal baseia-se na sua disponibilidade e compatibilidade com a EVM, tendo em vista que a DREX ainda não está disponível. Por fim, a utilização de uma destas *stablecoins* em contratos inteligentes possibilita a automação de pagamentos e liberações de fundos lastreados no real brasileiro.

5.3.3 Escalabilidade

A escalabilidade é um fator crucial no desenvolvimento da plataforma, principalmente devido às limitações inerentes às blockchains públicas como o Ethereum. Por mais robusta que seja a rede, sua capacidade de processar transações simultâneas ainda apresenta desafios significativos, especialmente em sistemas com grande número de usuários.

A rede Ethereum, apesar das melhorias com o mecanismo de consenso Proof-of-Stake (PoS), enfrenta limitações na quantidade de transações por segundo (TPS) que podem ser processadas. Um aumento exponencial no número de usuários pode resultar em:

- **Atrasos na Rede:**
    - A alta demanda pode congestionar a rede, causando atrasos na validação de transações.
- **Altos Custos de Gás:**
    - Em momentos de congestionamento, as taxas de gas aumentam significativamente, tornando o uso inviável para muitos participantes.

A escolha de implementar a aplicação em um contexto local é proposital e estrategicamente alinhada às limitações de escalabilidade. Um público limitado facilita a administração do sistema e diminui a sobrecarga na rede Ethereum. Com um volume menor de transações simultâneas, os custos de gás são minimizados, mantendo a plataforma acessível para todos os membros da comunidade. O modelo reduz a complexidade das votações e aprovações, permitindo uma governança mais ágil e organizada.

Ao priorizar bairros como unidade de governança, a DAO maximiza a eficiência, participação comunitária e transparência, sem comprometer o desempenho da plataforma.

5.4 PROTOTIPAGEM

O protótipo desenvolvido representa uma versão funcional dos contratos que compõem a DAO, incorporando e executando estes *smart contracts*.

5.4.1 Organização do Sistema

A base deste sistema está nos contratos inteligentes escritos em Solidity. Estes contratos são implantados em uma blockchain, fornecendo uma plataforma imutável e auditável para a tomada de decisões. O coração do projeto é o contrato ***BairroGovernance***, que gerencia a governança, enquanto outros contratos, como ***VoteToken*** e ***Treasury***, fornecem suporte essencial. O ***VoteToken*** é usado para representar o poder de voto, e o ***Treasury*** é responsável por gerenciar fundos associados a propostas aprovadas. O contrato ***BairroGovernance*** foi projetado para possibilitar o ciclo completo de governança, desde a criação de propostas até a execução de ações correspondentes. Ele segue um fluxo lógico rigoroso, começando com a criação de uma proposta por um membro da DAO. A proposta inclui endereços de destino, valores financeiros, chamadas de função específicas e uma descrição. Após a criação, a proposta passa por um período de votação, onde os participantes utilizam seus tokens de voto para decidir seu destino. Esse processo é fundamentalmente democrático, garantindo que todas as decisões sejam tomadas de forma coletiva e transparente.

5.4.2 Estrutura do Repositório

O código do projeto está estruturado de forma lógica para facilitar o desenvolvimento, a manutenção e escalabilidade. Abaixo, detalhamos a organização das pastas e arquivos do repositório:

- **`contracts/`**: Contém os contratos inteligentes desenvolvidos em Solidity. Cada contrato implementa uma funcionalidade específica da DAO.
    - **`BairroGovernance.sol`**: Gerencia a governança descentralizada.
    - **`Treasury.sol`**: Administra os fundos da DAO e os pagamentos.
    - **`MockERC20.sol`**: Simula uma *stablecoin* para testes.
    - **`Migrations.sol`**: Automatiza a implantação dos contratos.

- **`scripts/`**: Scripts em JavaScript que automatizam tarefas como criação de propostas, votação e execução.
    - **`3_create_proposal.js`**: Gerencia o ciclo completo de uma proposta, desde a criação até a execução.
- **`migrations/`**: Scripts que definem a ordem de implantação dos contratos na blockchain, garantindo que dependências sejam respeitadas.
- **`test/`**: (Atualmente vazio, mas reservado para testes automatizados).
    - **`truffle-config.js`**: Define as redes e o compilador Solidity utilizado.
    - **`package.json`**: Gerencia as dependências do projeto, como Web3.js e Truffle.

Essa organização reflete boas práticas de desenvolvimento, separando a lógica de contratos, automação e configuração em diretórios distintos.

5.4.3 Desenvolvimento dos *Smart Contracts*

Os contratos foram desenvolvidos utilizando a linguagem Solidity, seguindo padrões de design e melhores práticas recomendadas pela comunidade Ethereum.

Tabela 3 - Contratos Inteligentes

Contrato	Funções Principais	Responsabilidades
Governance	`propose(), vote(), executeProposal()`	Gerenciar propostas de votação
Treasury	`releaseInitialPayment(), releaseFinalPayment(), confirmCompletion()`	Gerenciar fundos e pagamentos
Token	`assignToken(), revokeToken()`	Gerenciar tokens de governança

Fonte: Elaborado pelo autor

5.4.3.1 Contrato de Governança

O contrato ***BairroGovernance*** gerencia a governança descentralizada. Ele permite que os membros criem propostas, votem e executem decisões. Para garantir a transparência e a justiça, o contrato define estados para as propostas, como Pending, Active e Executed. Cada proposta deve atender a um quórum mínimo de 50% de participação, além de obter maioria de

votos favoráveis. Esse contrato foi projetado para ser resiliente e flexível, permitindo que regras sejam atualizadas se necessário. Exemplos de código de implementação das propostas no contrato de governança abaixo:

Figura 6 - Estrutura da proposta

```
struct Proposal
{
        uint256 id;
        address proposer;
        address[] targets;
        uint256[] values;
        bytes[] calldatas;
        string description;
        ProposalState state;
        uint256 votesFor;
        uint256 votesAgainst;
        uint256 startBlock;
        uint256 endBlock;
}
```

Fonte: (Elaborado pelo autor)

O atributo `description` desempenha um papel fundamental na comunicação do conteúdo de cada proposta. É por meio dele que o criador da proposta pode detalhar, de forma clara e completa, as informações essenciais que embasam a iniciativa. Isso inclui, por exemplo, a especificação dos valores monetários associados, prazos, expectativas de resultados, justificativas e quaisquer outros elementos que contribuam para o entendimento pleno da proposta por parte dos demais participantes. Dessa forma, o campo `description` se torna um canal central de transparência e clareza, garantindo que todos tenham acesso às informações necessárias para tomar decisões bem embasadas.

Dentro do contrato, a função `propose()` é fundamental porque inicia todo o fluxo de governança, oferecendo uma plataforma para os membros exercerem seu direito de decisão. Ela também incorpora princípios essenciais, como a transparência (através de eventos emitidos) e a segurança (através de verificações e inicializações controladas). Sem esta função, a DAO perderia sua capacidade de funcionar como uma organização autônoma e descentralizada. Portanto, a `propose()` representa não apenas uma funcionalidade central, mas também o espírito democrático que define a essência de uma DAO.

Figura 7 - Código do Contrato de Governança

```
function propose(
    address[] memory targets,
    uint256[] memory values,
    bytes[] memory calldatas,
    string memory description
) public returns (uint256) {
    uint256 proposalId = proposalCount++;
    uint256 startBlock = block.number + 1;
    uint256 endBlock = startBlock + 20; // exemplo simplificado para testes

    proposals[proposalId] = Proposal({
        id: proposalId,
        proposer: msg.sender,
        targets: targets,
        values: values,
        calldatas: calldatas,
        description: description,
        state: ProposalState.Pending,
        votesFor: 0,
        votesAgainst: 0,
        startBlock: startBlock,
        endBlock: endBlock
    });

    emit ProposalCreated(proposalId, msg.sender, targets, values, calldatas,
description, startBlock, endBlock);
    return proposalId;
}
```

Fonte: (Elaborado pelo autor)

No contexto da DAO, essa função representa o ponto de partida do processo decisório. Ao chamá-la, um membro submete uma proposta para ser avaliada pelos demais participantes. Emite um evento `ProposalCreated` que notifica a rede (e qualquer observador externo) de que uma nova proposta foi criada. Eventos são importantes para indexar informações fora da blockchain e possibilitam que interfaces gráficas ou outros sistemas acompanhem as atividades do contrato.

Uma vez criada, a proposta aguarda o início do período de votação. A contabilização de votos e a eventual execução da proposta ocorrem posteriormente, por meio de funções como `vote()` e `executeProposal()`.

A função `vote()` verifica se o participante possui tokens de governança e se ainda não votou naquela proposta, garantindo que cada membro exerça seu direito de voto de forma única. Caso as condições sejam atendidas, o voto é contabilizado de acordo com o saldo de tokens do votante, assegurando o poder de votação do usuário. Ao final do período de votação, se o quórum mínimo for alcançado e a maioria favorável obtida, a função `executeProposal()` aciona as transações especificadas, efetivando a decisão da

comunidade.

Dessa forma, o contrato de governança não apenas organiza a lógica decisória, mas também zela pela integridade do processo, assegurando que o fluxo democrático seja respeitado e auditável por qualquer participante.

Figura 8 - Código de execução de proposta

```
function executeProposal(uint256 proposalId) external {
    Proposal storage proposal = proposals[proposalId];
    ProposalState state = getProposalState(proposalId);
    require(
        state == ProposalState.Succeeded,
        "Proposal is not in a succeeded state"
    );

    // Execute proposal actions
    proposal.state = ProposalState.Executed;

    for (uint256 i = 0; i < proposal.targets.length; i++) {
        (bool success, ) = proposal.targets[i].call{
            value: proposal.values[i]
        }(proposal.calldatas[i]);
        require(success, "Transaction execution failed");
    }

    emit ProposalExecuted(proposalId);
}
```

Fonte: (Elaborado pelo autor)

A função `executeProposal` desempenha o papel crucial de efetivar as decisões aprovadas no processo de governança. Uma vez que a proposta atinge o estado `Succeeded` (ou seja, recebeu votos suficientes para sua aprovação), essa função atualiza o estado da proposta para `Executed` e executa cada uma das ações planejadas – enviando transações para os endereços-alvo com os valores e dados fornecidos. Caso todas as operações sejam concluídas com êxito, um evento (`ProposalExecuted`) é emitido, registrando de forma pública e imutável que a proposta foi efetivamente implementada. Isso garante que as deliberações coletivas do sistema de governança sejam colocadas em prática, fortalecendo a transparência e a autonomia do processo decisório.

5.4.3.2 Contrato de Tesouraria

O contrato **Treasury.sol** é responsável por gerenciar os fundos da DAO e garantir que os pagamentos sejam liberados de maneira segura e condicional. Ele protege os ativos do

sistema enquanto implementa a lógica necessária para pagamentos baseados no progresso de serviços prestados.

O contrato, através da função `releaseInitialPayment()` libera um pagamento inicial para o prestador de serviços. Este é o primeiro passo do fluxo financeiro, garantindo que os fundos sejam liberados apenas se as condições forem atendidas.

Através da função `releaseFinalPayment()`, o contrato libera o pagamento final ao prestador de serviços após a conclusão do serviço e confirmação pelo mesmo. Assegura que o pagamento final só seja feito quando o prestador de serviços confirmar que o trabalho foi concluído. Essa abordagem protege os interesses da DAO e reduz o risco de desvios.

Figura 9 - Eventos do Contrato de Tesouraria

```
event InitialPaymentReleased(address serviceProvider, uint256 amount);
event FinalPaymentReleased(address serviceProvider, uint256 amount);
event ServiceCompleted(address serviceProvider);
```

Fonte: (Elaborado pelo autor)

Os eventos `InitialPaymentReleased`, `FinalPaymentReleased` e `ServiceCompleted` representam ocorrências importantes no fluxo do contrato e, uma vez emitidos, tornam-se registros públicos e imutáveis na blockchain. Isso significa que todos os participantes da rede podem acessar, consultar e auditar esses eventos, garantindo maior transparência, rastreabilidade e confiança no processo. Cada evento, ao ser disparado, adiciona um carimbo permanente do momento em que ocorreu, do provedor de serviço envolvido e dos valores liberados, permitindo que qualquer interessado confirme o cumprimento dos acordos estabelecidos, bem como o ciclo de pagamentos e a conclusão dos serviços.

Figura 10 - Contrato de realização de pagamento

```
function releaseInitialPayment(
       uint256 amount
   ) public onlyOwner nonReentrant {
       // Checks
       require(!isInitialPaymentReleased, "Initial payment already released");
       require(
           fundToken.balanceOf(address(this)) >= amount,
           "Insufficient funds"
       );

       // Effects
       isInitialPaymentReleased = true;
       emit InitialPaymentReleased(serviceProvider, amount); // Emit event after
state change

       // Interactions
       fundToken.transfer(serviceProvider, amount);
   }
```

Fonte: (Elaborado pelo autor)

A função `releaseInitialPayment` no contrato de tesouraria é responsável por liberar o pagamento inicial ao prestador de serviços, garantindo que a operação seja executada de forma segura e transparente. Antes da transferência, o código verifica se o pagamento inicial ainda não foi realizado e se há fundos suficientes no contrato. Caso as condições sejam atendidas, o estado do pagamento é atualizado para indicar que a parcela inicial foi liberada, e um evento (`InitialPaymentReleased`) é emitido, tornando o registro público e imutável na blockchain. Por fim, os fundos são efetivamente transferidos para o prestador de serviços, cumprindo o acordo de forma auditável e confiável.

5.4.3.3 Contrato de Token de Governança

O contrato desempenha um papel central no sistema DAO, servindo como o token de governança que define o poder de voto dos participantes. Implementado no padrão ERC20, ele garante compatibilidade com a infraestrutura Ethereum e facilita a integração com ferramentas e contratos baseados no mesmo padrão.

O token VOTE é utilizado como unidade de poder de decisão na DAO. Cada participante detém um número de tokens que corresponde à sua influência nas decisões

tomadas por meio de propostas e votações. Essa abordagem não apenas garante transparência, mas também atribui responsabilidade proporcional ao peso de cada voto, incentivando a participação ativa dos membros.

No contexto do sistema, o contrato **VoteToken** é essencial para:

- **Distribuição de Poder de Voto**: Cada participante recebe um token representando seu poder de voto.
- **Segurança e Compatibilidade**: Como um token ERC20, o **VoteToken** herda a robustez do padrão, assegurando a integridade de transferências e consultas de saldo.
- **Interação com Outros Contratos**: O contrato **BairroGovernance** utiliza o saldo de **VoteToken** dos participantes para calcular votos a favor ou contra uma proposta.

O contrato foi implementado utilizando o padrão ERC20, com funcionalidades básicas de criação e transferência de tokens. Ele também oferece suporte a funções adicionais, como emissão de novos tokens, para o caso de novos moradores no bairro. Sua implementação assegura que cada morador receba um único VOTE token.

1. **Proposta e Votação**:
    - Os proponentes devem possuir um saldo mínimo de **VoteToken** para criar propostas, garantindo compromisso financeiro ou reputacional com a comunidade.
    - Durante a votação, cada token representa um voto, e o saldo de tokens define a força da decisão de cada participante.
2. **Quórum e Resultados**:
    - O saldo total de **VoteToken** em circulação é utilizado para calcular o quórum mínimo necessário para validar uma votação.
    - Após o término do período de votação, os resultados são determinados com base na quantidade de votos favoráveis e contrários, proporcional aos saldos dos votantes.

O **VoteToken** introduz uma governança proporcional e escalável, permitindo que a influência de cada participante esteja diretamente vinculada ao número de tokens que ele possui. Isso incentiva a aquisição e retenção de tokens, além de criar um mercado interno de poder de decisão. Além disso, sua implementação no padrão ERC20 assegura interoperabilidade com soluções financeiras existentes, reforçando a eficiência do sistema.

No futuro, o **VoteToken** pode ser integrado com modelos de staking ou recompensas para engajar ainda mais os membros da DAO. Por exemplo, tokens poderiam ser ganhos por participação em atividades comunitárias ou retenção prolongada, reforçando a fidelidade ao sistema.

5.4.3.4 Contrato de Mock

O **MockERC20** é um contrato simulado que representa uma *stablecoin*. Sua inclusão no projeto permitiu a realização de testes no sistema sem depender de tokens reais. Ele foi implementado com base no padrão ERC20, garantindo compatibilidade com outras ferramentas Ethereum. Esse contrato prepara o sistema para a integração futura com uma stablecoin, como BRZ ou DREX, para gerenciar fundos reais.

5.4.3.5 Contrato de Migrações

O contrato **Migrations** é um componente essencial para a implantação de contratos no Ethereum. Ele rastreia quais contratos já foram migrados, prevenindo duplicações. Embora seja trivial para desenvolvedores experientes, sua inclusão no projeto foi vital para garantir que a sequência de implantação fosse mantida.

5.4.4 Comandos de Configuração do Ambiente de Desenvolvimento

1. Compilar os contratos:
    a. truffle compile
2. Rodar a blockchain local:
    a. ganache-cli
3. Executar:
    a. truffle migrate – reset: Faz a migração para a blockchain local
    b. truffle exec ./scripts/3_create_proposal.js: Executa os contratos

5.5 EXECUÇÃO

Esta etapa busca garantir que o sistema funcione conforme o esperado e esteja preparado para resistir a possíveis vulnerabilidades. Através de um ambiente de teste controlado, simulamos cenários reais de uso, verificando a corretude funcional, a segurança e a eficiência dos contratos. A validação foi conduzida em um ambiente de desenvolvimento local, utilizando ferramentas como o Truffle e Ganache.

5.5.1 Comandos de Execução e Verificação de Logs

- **Comando Truffle Compile:**
  - `truffle compile`
- **Comando Truffle Migrate:**
  - `truffle migrate --reset`
- **Comando Truffle Exec:**
  - `truffle exec ./scripts/3_create_proposal.js`

5.5.2 Testes

Os testes foram divididos em etapas que cobriram desde funções individuais até fluxos completos do sistema. Destaca-se a importância do script `3_create_proposal.js`, que simula o ciclo de vida completo de uma proposta, permitindo testar as interações entre os contratos e os usuários.

5.5.2.1 Script de Criação de Proposta

O script `3_create_proposal.js` automatizou o ciclo de vida completo de uma proposta. Abaixo, descrevemos os passos executados pelo script:

Figura 11 - Script de execução I

```
vitorpchavess@MacBook-Pro-de-Vitor DAO % truffle exec ./scripts/3_create_proposal.js

Using network 'development'.

Step 1: Checking proposer's VoteToken balance...

Proposer's VoteToken balance: 1
Checking voters' VoteToken balances...

Voter 0xA9ed8C6AF06a4adF2B91fC0578514301499d5783 has 1 VoteToken(s).
Voter 0x4166A6E1059D514FB2A1bA8d00530ff589340691 has 1 VoteToken(s).
Voter 0x5660e52Ac28c391D970C5fce0D40C8bEB06F5fD6 has 1 VoteToken(s).
Voter 0x29ae42Ef3e181b01225540bfea401f5b532e3540 has 1 VoteToken(s).
Voter 0xDAa6FF6C001993508423AA06a626C36304604a02 has 1 VoteToken(s).
Step 2: Creating initial payment proposal...

Initial payment proposal created successfully! Proposal ID: 0

Step 3: Simulating voting on initial proposal...

Voter 0xA9ed8C6AF06a4adF2B91fC0578514301499d5783 voted in favor.
Voter 0x4166A6E1059D514FB2A1bA8d00530ff589340691 voted in favor.
Voter 0x5660e52Ac28c391D970C5fce0D40C8bEB06F5fD6 voted in favor.
Voter 0x29ae42Ef3e181b01225540bfea401f5b532e3540 voted in favor.
Voter 0xDAa6FF6C001993508423AA06a626C36304604a02 voted in favor.
All votes cast successfully.

Step 4: Advancing blocks to end voting period...

Advanced 17 blocks.

Advanced 17 blocks.

Proposal state after advancing blocks: 3
Step 5: Executing initial payment proposal...

Initial payment executed successfully.
```

Fonte: (Elaborado pelo autor)

Figura 11 - Script de execução II

```
Service provider confirming completion of service...

Step 6: Creating final payment proposal...

Final payment proposal created successfully. Proposal ID: 1

Step 7: Simulating voting on final proposal...

Voter 0xA9ed8C6AF06a4adF2B91fC0578514301499d5783 voted in favor.
Voter 0x4166A6E1059D514FB2A1bA8d00530ff589340691 voted in favor.
Voter 0x5660e52Ac28c391D970C5fce0D40C8bEB06F5fD6 voted in favor.
Voter 0x29ae42Ef3e181b01225540bfea401f5b532e3540 voted in favor.
Voter 0xDAa6FF6C001993508423AA06a626C36304604a02 voted in favor.
All votes cast successfully.

Step 8: Advancing blocks to end voting period...

Advanced 17 blocks.

Step 9: Executing final payment proposal...

Final payment executed successfully. Process complete.

vitorpchavess@MacBook-Pro-de-Vitor DAO % truffle compile
```

Fonte: (Elaborado pelo autor)

1. **Validação de Saldos**: O script inicia verificando se o proponente e os votantes possuem saldo de tokens VOTE. Caso algum participante não possua o token, o script interrompe a execução e retorna um erro, simulando a impossibilidade de criar uma proposta sem o compromisso financeiro necessário.
2. **Criação de Proposta**: Uma proposta é criada utilizando a função `propose()` do contrato de governança. Os parâmetros incluem:
    - **Valores financeiros**: Define os montantes envolvidos nas transações.
    - **Chamadas de função**: Codifica, em formato ABI, as funções que serão executadas, como `releaseInitialPayment()`.
3. **Simulação de Votação**: Os membros da DAO, representados por contas simuladas, participam da votação. Cada participante utiliza seus tokens para votar a favor ou contra a proposta. O script registra cada voto e verifica a consistência dos dados, garantindo que as regras de votação sejam respeitadas.
4. **Avanço de Blocos**: Para simular o decorrer do tempo na blockchain, o script utiliza o método `evm_mine` do Ganache CLI, avançando o número de blocos necessários para

atingir o fim do período de votação. Isso permite testar a transição de estados da proposta, de ativa para sucedida ou derrotada.

5. **Atualização e Execução da Proposta Inicial**: Após o término do período de votação, o estado da proposta é atualizado com base nos votos recebidos e no quórum atingido. Se a proposta for aprovada, o script chama a função `executeProposal()`, que aciona as transações especificadas. No caso, ocorre a liberação do pagamento inicial para o prestador de serviços através do contrato de tesouraria.

O prestador de serviços confirma a conclusão da etapa inicial, o que permite a criação de uma nova proposta para o pagamento final. Essa confirmação pode ser realizada através de um evento ou interação externa com o sistema.

6. **Criação da Proposta Final:** Similar ao passo 2, uma nova proposta é criada utilizando a função `propose()` do contrato ***BairroGovernance***, desta vez para liberar o pagamento final.
7. **Simulação de Votação na Proposta Final:** Os membros da DAO novamente votam na proposta final utilizando seus tokens de governança. O script utiliza novamente a função **vote()** para registrar os votos favoráveis. Todos os votos são contabilizados corretamente.
8. **Avanço dos Blocos:** Assim como no passo 4, o script avança os blocos necessários para finalizar o período de votação da proposta final. A simulação garante a transição do estado da proposta para *Succeeded*, permitindo sua execução. 17 blocos foram avançados com sucesso.
9. **Confirmação e Pagamento Final**: O fluxo é repetido para uma segunda proposta, que visa liberar o pagamento final. Esta etapa só é executada após a confirmação do prestador de serviços de que o trabalho foi concluído, assegurando que os fundos são liberados de acordo com o progresso real do projeto.

Este script foi essencial para validar não apenas as funções isoladas, mas também a interação entre elas em um cenário completo de uso, desde a criação da proposta até a execução dos pagamentos.

5.6 CONSIDERAÇÕES FINAIS

5.6.1 Desafios

Um desafio técnico e operacional significativo é garantir que os registros digitais na blockchain reflitam com precisão as atividades realizadas no mundo real, ou seja, as operações *off-chain*. Há uma necessidade de mecanismos confiáveis que validem e verifiquem os dados inseridos na blockchain, evitando fraudes ou discrepâncias. A utilização de oráculos, sensores IoT e outras tecnologias de validação externa pode ser explorada para conectar eventos do mundo físico aos contratos inteligentes. Por exemplo, no caso de uma obra pública, é necessário confirmar que determinada etapa foi concluída conforme especificado antes de liberar o pagamento correspondente. Estabelecer processos de verificação independentes, possivelmente envolvendo auditorias externas ou participação comunitária na fiscalização, pode reforçar a confiabilidade do sistema.

Promover a compreensão sobre o DREX e sua utilização dentro da plataforma é outro desafio significativo. Muitos cidadãos podem não estar familiarizados com moedas digitais ou podem ter desconfiança em relação a elas. Oferecer educação e suporte aos usuários é essencial para incentivar a participação cidadã e a adoção da tecnologia. Estratégias como oficinas educativas, tutoriais online, suporte técnico e canais de atendimento podem ajudar a superar barreiras tecnológicas e culturais. Além disso, é importante abordar questões de inclusão digital. Nem todos os membros da comunidade têm acesso fácil a dispositivos tecnológicos ou à internet. Desenvolver soluções que sejam acessíveis mesmo em ambientes com limitações tecnológicas, ou promover iniciativas que melhorem a infraestrutura digital local, pode ser necessário para garantir que a plataforma seja inclusiva.

5.6.2 Trabalhos Futuros

5.6.2.1 Ampliação do Sistema

- Desenvolvimento de Interface Gráfica
- Fazer o *deploy* dos *smart contracts* em uma *testnet* da rede *blockchain*
- Criar uma aplicação web ou móvel que permita aos cidadãos.
    - Autenticação segura de usuários.
    - Integração com carteiras digitais para gerenciamento de tokens.
    - Visualização gráfica de dados e estatísticas.

Reconhecemos que o projeto está em uma fase inicial e que há desafios a serem superados para alcançar todo o seu potencial. É fundamental avançar no desenvolvimento de

soluções que conectem de forma confiável os registros digitais às atividades realizadas fora da cadeia (*off-chain*), assegurando a integridade e a confiabilidade das informações inseridas na blockchain. A integração de tecnologias como oráculos pode ser essencial para validar dados externos e garantir que os contratos inteligentes reflitam com precisão o progresso e a execução dos projetos no mundo real.

5.6.2.2 Alternativas de Blockchain

Devido às altas taxas de gas fee da rede Ethereum, que foi um dos desafios encontrados durante o desenvolvimento deste trabalho, podendo se tornar inviáveis em cenários de grande volume de transações, torna-se necessário explorar alternativas de blockchain que ofereçam custos mais baixos. Uma das soluções mais promissoras está no uso de redes de segunda camada, como Arbitrum e Optimism, que são projetadas para operar sobre a blockchain principal do Ethereum.

Arbitrum e Optimism utilizam a tecnologia de *rollups*, que agrupa diversas transações fora da cadeia principal e, em seguida, envia um único lote de dados para validação na blockchain principal. Isso reduz significativamente os custos de *gas* ao mesmo tempo em que mantém a segurança e descentralização oferecidas pela Ethereum. Ao processar transações fora da cadeia (off-chain) e consolidar apenas os resultados finais na rede principal, essas soluções conseguem lidar com um volume muito maior de transações por segundo.

Ao considerar essas alternativas, a Bairro DAO poderá evoluir para um sistema mais econômico e eficiente, mantendo os princípios de transparência e governança descentralizada, enquanto supera os desafios associados às limitações atuais da rede Ethereum.

6 CONCLUSÃO

Este trabalho explorou e demonstrou a viabilidade técnica e prática da utilização de Organizações Autônomas Descentralizadas (DAOs) como uma solução inovadora para promover transparência e engajamento cívico em atividades públicas de nível local. O estudo apresentou o desenvolvimento da plataforma Bairro DAO, uma aplicação prática da tecnologia blockchain voltada para a gestão descentralizada de serviços públicos, permitindo que os cidadãos participem ativamente em processos como a submissão de propostas, monitoramento financeiro e operacional, além do gerenciamento transparente dos recursos alocados.

Ao longo do trabalho, foram abordados fundamentos teóricos e práticos necessários para a implementação da DAO, destacando o potencial da blockchain em reduzir custos de verificação e assegurar que todas as transações e decisões sejam registradas de forma imutável e auditável. Essa característica não apenas aumenta a confiança nos processos, mas também proporciona um modelo de governança que distribui o poder de decisão entre os membros da comunidade, eliminando intermediários e minimizando oportunidades de corrupção.

A implementação da plataforma representa uma ruptura significativa com os modelos tradicionais de organização e gestão pública, ao integrar contratos inteligentes e um sistema de governança transparente e participativo. Contudo, o sucesso dessa iniciativa depende de uma mudança de mentalidade tanto por parte dos gestores públicos quanto dos cidadãos. Resistências à mudança, desconfiança em sistemas descentralizados e falta de familiaridade com tecnologias digitais são desafios a serem superados. Para enfrentar essas barreiras, é essencial promover uma cultura de inovação e aprendizado contínuo. Envolver líderes comunitários, educadores e influenciadores locais pode ser uma estratégia eficaz para difundir os valores e as vantagens das dos sistemas descentralizados, construindo confiança e adesão ao modelo.

Além disso, a consolidação de uma DAO eficiente e sustentável exige abordagens multidisciplinares que integrem aspectos técnicos, legais, sociais e educacionais. Colaborações entre desenvolvedores, gestores públicos, juristas, especialistas em segurança digital, educadores e a própria comunidade são cruciais para criar uma plataforma robusta e alinhada às reais necessidades dos cidadãos. Essa sinergia pode não apenas garantir o sucesso do sistema, mas também estabelecer um modelo replicável que inspire novas iniciativas em diferentes contextos governamentais.

Por fim, este trabalho contribui para o avanço do conhecimento e das práticas relacionadas às organizações autônomas descentralizadas, demonstrando como a tecnologia blockchain pode ser uma ferramenta transformadora para fortalecer a governança pública, aumentar a transparência e fomentar a participação cidadã. O futuro da Bairro DAO é promissor, mas depende do comprometimento coletivo em superar os desafios apresentados e aproveitar as oportunidades de inovação para criar uma sociedade mais justa, participativa e eficiente.

REFERÊNCIAS

ANTONOPOULOS, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, 2017.

ARCHANA PRASHANTH JOSHI MENG HAN, Yan Wang. survey on security and privacy issues of blockchain technology. v. 1, p. 121–147, 2018.

ATZEI, Nicola; BARTOLETTI, Massimo; CIMOLI, Tiziana. A Survey of Attacks on Ethereum Smart Contracts (SoK). In: *Proceedings of the 6th International Conference on Principles of Security and Trust (POST)*, Springer, 2017. p. 164-186.

AZARIA, Asaph et al. MedRec: Using Blockchain for Medical Data Access and Permission Management. In: *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016. p. 25-30.

BANCO CENTRAL DO BRASIL. Real Digital - DREX. 2023. Disponível em: https://www.bcb.gov.br/drex. Acesso em: 1 nov. 2024.

BUTERIN, Vitalik. A Next-Generation Smart Contract and Decentralized Application Platform. *Ethereum White Paper*, 2014. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 1 nov. 2024.

CIVIC. Civic: Secure Identity for Web3. Disponível em: https://www.civic.com/. Acesso em: 17 dez. 2024.

ETHEREUM FOUNDATION. Solidity Documentation. 2021. Disponível em: https://docs.soliditylang.org/. Acesso em: 1 nov. 2024.

FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2018.

FUSTER MORELL, Mayo et al. Citizen Participation in the City of the Future: The Case of Decidim Barcelona. In: *2017 Smart Cities Symposium Prague (SCSP)*. IEEE, 2017.

HARDY, Stephen; MAURO, John. Blockchain Voting: Election Integrity in the Digital Age. *Journal of Cyber Policy*, v. 2, n. 3, p. 306-328, 2017.

JÄRVINEN, Joni et al. Blockchain in Practice: Lessons from a Groundbreaking Supply Chain Implementation. *IEEE Software*, v. 36, n. 4, p. 55-61, 2019.

JENTZSCH, Christoph. Decentralized Autonomous Organization to Automate Governance. *White Paper*, 2016. Disponível em: https://download.slock.it/public/DAO/WhitePaper.pdf. Acesso em: 1 nov. 2024.

KOSHY, George et al. Blockchain-Based Supply Chain Management: A Systematic Mapping Study. In: *2018 International Conference on Emerging Technologies (ICET)*. IEEE, 2018. p. 1-6.

LEE, Charlie. Litecoin - Open Source P2P Digital Currency. 2011. Disponível em: https://litecoin.org. Acesso em: 1 nov. 2024.

MAKERDAO. MakerDAO: The Maker Protocol. Disponível em: https://makerdao.com/en/. Acesso em: 17 dez. 2024.

MORALIS ACADEMY. DAO vs Traditional Organization. *Moralis Academy Blog*, 2021. Disponível em: https://academy.moralis.io/blog/dao-vs-traditional-organization. Acesso em: 1 nov. 2024.

MUSLIMIN, Muslimin; NAZIEF, Budi Rahardjo. Stable Cryptocurrency: Review of the Existing Stablecoins. In: *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*. IEEE, 2020. p. 235-240.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 1 nov. 2024.

NARAYANAN, Arvind et al. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

OGP - Open Government Partnership. What is Open Government? 2021. Disponível em: https://www.opengovpartnership.org/. Acesso em: 1 nov. 2024.

ØLNES, Svein; UBACHS, Jelmer; JANSEN, Arild. Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Public Services. *Government Information Quarterly*, v. 34, n. 3, p. 355-364, 2017.

REGNER, Ferdinand; NAGEL, Jan; REPPEL, Alexander. Blockchain-Based Tokens and Their Impact on Financing Decisions. *Business Transformation through Blockchain*, p. 183-204, 2019.

SCHÄR, Fabian. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, v. 103, n. 2, p. 153-174, 2021.

SCHWARTZ, David; YOUNGS, Noah; BRITO, Arthur. The Ripple Protocol Consensus Algorithm. *Ripple Labs Inc.*, 2014.

SIEGEL, David et al. Understanding the DAO Attack. 2016. Disponível em: https://www.coindesk.com/understanding-dao-hack-journalists. Acesso em: 1 nov. 2024.

SMART DUBAI. Dubai Blockchain Strategy. 2016. Disponível em: https://www.smartdubai.ae/initiatives/blockchain. Acesso em: 1 nov. 2024.

SZABO, Nick. The Idea of Smart Contracts. 1997. Disponível em: https://nakamotoinstitute.org/the-idea-of-smart-contracts/. Acesso em: 1 nov. 2024.

TRANSFERO SWISS. BRZ Token. 2021. Disponível em: https://brztoken.io/. Acesso em: 1 nov. 2024.

VRIGNAUD, P.; SALKELD, P.; CAMPBELL, T. Bitcoin Energy Consumption: An Improved Methodology. *International Journal of Energy Economics and Policy*, v. 9, n. 6, p. 432-439, 2019.

WOOD, Gavin. Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, 2014.

YAKOVENKO, Anatoly. Solana: A New Architecture for a High Performance Blockchain. *White Paper*, 2018. Disponível em: https://solana.com/solana-whitepaper.pdf. Acesso em: 1 nov. 2024.

ZHENG, Zibin et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017. p. 557-564.

Apêndices

ANEXO A – Artigo da monografia

Organização autônoma descentralizada para transparência e participação em serviços públicos

Vitor Patricio Chaves [1]

[1] Sistemas de Informação
Universidade Federal de Santa Catarina (UFSC)

Abstract. *This project explores the potential of Decentralized Autonomous Organizations (DAOs) to improve the oversight of public activities, fostering transparency, accountability, and citizen participation in resource management. By leveraging blockchain technology and the emerging Brazilian digital token DREX, we propose the creation of a DAO that enables citizens to monitor and verify all stages of public-interest projects in their neighborhoods, from the initial proposal through to final execution. This work presents the development of the Bairro DAO, a platform designed to enhance transparency in local public services. Based on blockchain technology and smart contracts, the platform allows citizens to track and verify every phase of civic projects at the local level, ensuring traceability and immutability of transactions. The DAO was implemented on the Ethereum network, using a mock ERC-20 token for transactions, ensuring compatibility with the emerging Brazilian digital token DREX. This project demonstrates how blockchain technology can transform the relationship between government and society, promoting more transparent and participatory governance.*

Resumo. *Este projeto explora o potencial das Organizações Autônomas Descentralizadas (DAOs) para aprimorar a fiscalização de atividades públicas, promovendo transparência, responsabilização e participação cidadã na gestão dos recursos. Aproveitando a tecnologia blockchain e o emergente token digital brasileiro DREX, propomos a criação de uma DAO que permita aos cidadãos monitorar e verificar todas as etapas de projetos de interesse público em bairros, desde a proposta inicial até a execução final. Este trabalho apresenta o desenvolvimento da Bairro DAO, uma plataforma destinada a promover a transparência em serviços públicos em nível local. Baseada na tecnologia blockchain e em contratos inteligentes (smart contracts), a plataforma permite que cidadãos acompanhem e verifiquem todas as fases de trabalhos no setor cívico local, assegurando rastreabilidade e imutabilidade das transações. A DAO foi implementada na rede Ethereum, utilizando um token ERC-20 simulado (mock) para transações, garantindo compatibilidade com o emergente token digital brasileiro DREX. O projeto demonstra como a tecnologia blockchain pode transformar a relação entre governo e sociedade, promovendo uma governança mais transparente e participativa.*

1. Introdução

No final da década de 2000, o mundo testemunhou o surgimento de uma tecnologia revolucionária que transformaria o panorama das finanças digitais e da computação distribuída. A partir da publicação do white paper de Satoshi Nakamoto (2008), a tecnologia blockchain passou a ser entendida não apenas como a base para uma nova forma de moeda digital, mas também como um recurso capaz de viabilizar sistemas descentralizados, transparentes e resistentes à censura. Esse avanço lançou as bases para uma ampla gama de aplicações em diversos setores, redefinindo a forma como confiança, governança e transações são geridas na era digital.

Nas últimas décadas, a administração pública tem enfrentado o desafio de manter transparência, eficiência e participação cidadã em seus processos. A crescente demanda da sociedade por serviços mais ágeis, verificáveis e menos sujeitos a corrupção impulsiona a busca por soluções tecnológicas que tornem a gestão pública mais aberta e responsável. Nesse contexto, a tecnologia blockchain, com sua capacidade de registrar transações de maneira descentralizada, imutável e auditável, desponta como uma alternativa promissora (SWAN, 2015). Sua adoção pode contribuir para superar obstáculos ligados à opacidade, burocracia e dificuldade de monitoramento dos recursos públicos.

É neste cenário que as Organizações Autônomas Descentralizadas (DAOs) entram em cena, oferecendo um modelo organizacional baseado em contratos inteligentes (*smart contracts*) e regido pelo voto de seus membros, sem a necessidade de intermediários (BUTERIN, 2014). Uma DAO é um tipo de organização digital que funciona por meio de regras codificadas em blockchain, permitindo que decisões sejam tomadas coletivamente de forma transparente, auditável, imutável e democrática. Estando integrada com uma rede blockchain, a plataforma permite que seus usuários verifiquem todas as informações e todo histórico de transações, sem se preocupar com a falta de confiança que muitas vezes se faz presente em setores governamentais. Ao eliminar hierarquias rígidas e as burocracias contidas nelas, as DAOs proporcionam um ambiente em que as políticas, os gastos e as ações podem ser deliberados e executados conforme a vontade coletiva dos participantes, apresentando uma nova forma de se discutir a execução de trabalhos na área pública, distribuindo o poder de decisão e assegurando maior engajamento comunitário.

A proposta deste trabalho é o desenvolvimento de uma aplicação prática da tecnologia blockchain voltada para a integração coletiva na verificação e fiscalização de atividades do setor público em âmbito local. A Bairro DAO visa oferecer uma plataforma transparente, descentralizada e segura para que cidadãos possam acompanhar, propor e participar da gestão de serviços públicos em sua comunidade. Ao utilizar a rede Ethereum, a plataforma integra transações financeiras rastreáveis por meio de contratos inteligentes auto executáveis, garantindo que todas as etapas do processo – desde a submissão de propostas até a execução de pagamentos a fornecedores – sejam verificáveis e imutáveis.

A natureza descentralizada reduz a dependência de intermediários, diminuindo oportunidades de corrupção e falhas administrativas. A DAO dá voz direta aos cidadãos, que passam a ter poder de influenciar o destino de recursos e a priorização de obras, aumentando a legitimidade das decisões. A imutabilidade do registro em blockchain assegura que decisões e transações não sejam adulteradas retroativamente, fortalecendo a confiança no processo decisório. Além disso, facilita o monitoramento contínuo dos projetos, permitindo que os

cidadãos fiscalizem o andamento das obras e serviços de seu bairro, aumentando o senso de responsabilidade compartilhada e engajamento cívico.

Em síntese, ao propor a Bairro DAO, este trabalho se insere no debate sobre novas formas de governança pública, demonstrando como a combinação de blockchain, contratos inteligentes e DAOs pode trazer mais eficiência à gestão pública, atendendo a anseios sociais por processos mais abertos e colaborativos.

2. Fundamentação teórica

Este capítulo introduz ao leitor os conceitos necessários para entender o funcionamento das tecnologias relacionadas a este trabalho e os motivos de serem utilizadas.

2.1. Blockchain

A tecnologia blockchain emergiu em 2008 como a base para o Bitcoin, a primeira criptomoeda descentralizada, introduzida por um indivíduo ou grupo sob o pseudônimo de Satoshi Nakamoto. A blockchain foi concebida como uma solução para o problema do gasto duplo em transações digitais, eliminando a necessidade de uma autoridade central para verificar e validar transações (NAKAMOTO, 2008).

Blockchain é essencialmente um livro-razão distribuído e imutável que registra transações em uma rede descentralizada de computadores. Cada bloco na cadeia contém um conjunto de transações e um hash criptográfico que o vincula ao bloco anterior, garantindo segurança e integridade dos dados (NARAYANAN et al., 2016). Tendo os blocos encadeados entre si, o trabalho para alterar um deles resultaria numa alteração no resultado do hash de todos os blocos seguintes.

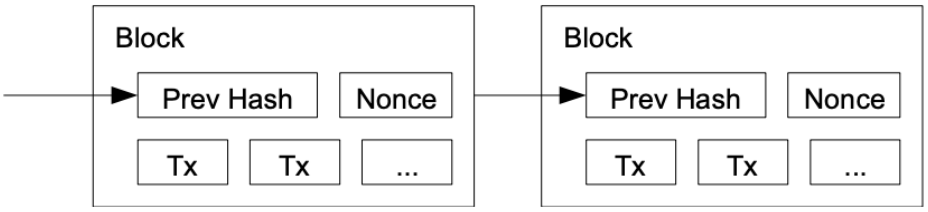


Figure 1. Lista encadeada de blocos

2.2. Custo de verificação

A eficiência de setores depende da capacidade dos participantes de verificar atributos das transações, garantindo que ambas as partes cumpram suas obrigações. Em transações tradicionais, especialmente aquelas realizadas pessoalmente, compradores podem avaliar diretamente a qualidade dos bens ou serviços, enquanto vendedores verificam a autenticidade do pagamento. No entanto, à medida que os mercados se expandem geograficamente e as transações tornam-se digitais, a necessidade de intermediários para assegurar a confiança entre as partes aumenta significativamente (CATALINI; GANS, 2016).

Em uma organização como a Bairro DAO, o uso da tecnologia blockchain reduz substancialmente o custo de verificação. A blockchain permite que transações sejam registradas de forma transparente e imutável, eliminando a necessidade de intermediários

tradicionais, como instituições financeiras ou órgãos governamentais, que normalmente cobram taxas por seus serviços de verificação e introduzem riscos de privacidade e censura.

Ao utilizar contratos inteligentes, a DAO possibilita que os participantes verifiquem autonomamente atributos das transações e executem acordos automaticamente quando condições predefinidas são atendidas. Isso aumenta a eficiência ao reduzir os custos associados à necessidade de confiança em terceiros. Por exemplo, na contratação de uma obra pública, os cidadãos podem verificar o andamento do projeto e a utilização dos recursos em tempo real, sem depender de relatórios fornecidos por intermediários ou autoridades centralizadas.

Entretanto, é importante reconhecer que, embora a blockchain reduza os custos de verificação para informações digitais, ainda existem desafios significativos na interface entre registros digitais ("on-chain") e eventos do mundo real ("off-chain"). A precisão dos dados inseridos na blockchain é crucial; se informações incorretas ou fraudulentas forem registradas, a confiabilidade do sistema pode ser comprometida. No caso, isso significa que a confiança dos participantes no que está sendo descrito pelo participante proposer condiz com a realidade, garantindo que o progresso físico das obras públicas seja registrado corretamente na blockchain.

Além disso, a ausência de intermediários tradicionais também implica na necessidade de soluções alternativas para problemas como disputas entre partes ou falhas na execução de contratos. Enquanto os contratos inteligentes podem automatizar a execução com base em parâmetros pré-estabelecidos, eles não podem, por si só, lidar com todas as nuances e imprevistos que podem surgir em projetos do mundo real.

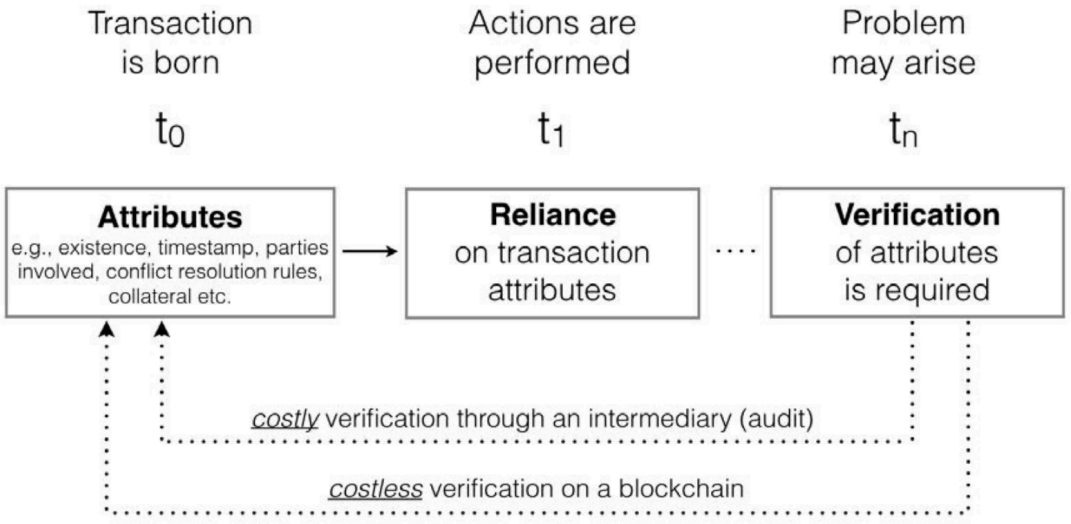


Figure 2. Custo de verificação

2.3. Ethereum e Smart Contracts

O Ethereum foi proposto em 2013 por Vitalik Buterin como uma plataforma descentralizada capaz de executar contratos inteligentes, expandindo as funcionalidades da tecnologia blockchain para além das transações financeiras simples (BUTERIN, 2014). Lançado oficialmente em 2015, o Ethereum tornou-se a segunda maior blockchain em termos de capitalização de mercado e uso (WOOD, 2014).

A arquitetura do Ethereum permite a criação e execução de contratos inteligentes e aplicativos descentralizados (dApps). Um componente fundamental é a Ethereum Virtual Machine (EVM), um ambiente de execução que processa contratos inteligentes escritos em linguagens como Solidity (ETHEREUM FOUNDATION, 2021). O Ether (ETH) é a criptomoeda nativa do Ethereum, usada para pagar taxas de transação e recompensar os mineradores ou validadores que mantêm a rede. O conceito de "gas" é utilizado para medir o esforço computacional necessário para executar operações na rede, prevenindo abusos e ataques, pois cada operação consome uma quantidade específica de gás que deve ser paga em Ether.

O Ethereum tem sido a plataforma preferida para o desenvolvimento de contratos inteligentes, dApps e para a emissão de tokens seguindo padrões como ERC-20 (tokens fungíveis) e ERC-721 (tokens não fungíveis, ou NFTs). Sua flexibilidade e robustez têm impulsionado a inovação em áreas como finanças descentralizadas (DeFi), NFTs e organizações autônomas descentralizadas (DAOs).

Contratos inteligentes são programas auto executáveis que residem na blockchain. Concebidos inicialmente por Nick Szabo em 1994, eles automatizam acordos e transações, operando com base em condições predefinidas (SZABO, 1997). No Ethereum, os contratos inteligentes são escritos em linguagens específicas, como Solidity, e são executados na EVM.

A rede possui uma arquitetura que permite a criação e execução de contratos inteligentes e aplicativos descentralizados (dApps):

- Ethereum Virtual Machine (EVM): Ambiente de execução que processa contratos inteligentes escritos com a linguagem de programação Solidity (ETHEREUM FOUNDATION, 2021).
- Ether (ETH): A criptomoeda nativa do Ethereum, usada para pagar taxas de transação e recompensar mineradores.
- *Gas Fee*: Unidade que mede o esforço computacional necessário para executar operações na rede, prevenindo abusos e ataques.

Os contratos inteligentes surgiram para automatizar processos, reduzindo a intervenção humana e minimizando erros ou manipulações. Eles garantem o cumprimento de acordos, pois as ações programadas são executadas automaticamente quando as condições especificadas são atendidas. Por exemplo, um contrato inteligente pode ser programado para liberar um pagamento somente quando um serviço é concluído ou um produto é entregue.

Uma das principais vantagens dos contratos inteligentes é a transparência e a auditabilidade. Todas as ações e eventos associados são registrados na blockchain, permitindo auditorias independentes e garantindo a confiança entre as partes, mesmo sem a necessidade de intermediários. Em caso de disputas ou suspeitas de irregularidades, é possível rastrear exatamente quando e como uma determinada ação ocorreu.

Além disso, mecanismos podem ser implementados para lidar com exceções, como congelamento temporário de fundos ou suspensão de pagamentos até que uma situação seja resolvida. Isso adiciona uma camada de segurança e flexibilidade aos contratos inteligentes, tornando-os uma ferramenta poderosa para uma ampla gama de aplicações, desde finanças até governança.

Estes algoritmos automatizam a execução de acordos pré-estabelecidos, mas também registram todas as ações e eventos associados. Isso significa que, em caso de disputas ou suspeitas de irregularidades, é possível rastrear exatamente quando e como uma determinada ação ocorreu.

Além do Ethereum, plataformas como Cardano (ADA) e Tezos (XTZ) oferecem funcionalidades de contratos inteligentes com diferentes abordagens para governança e escalabilidade. Essa diversidade no ecossistema de criptomoedas permite que diferentes necessidades e casos de uso sejam atendidos, promovendo a inovação contínua. No entanto, também apresenta desafios em termos de interoperabilidade, segurança e regulamentação.

2.4. DREX

O token digital brasileiro representa a versão digital do Real, mantendo o mesmo valor e reconhecimento legal da moeda física. Projetado para operar em uma infraestrutura baseada em blockchain, o DREX é compatível com a Ethereum Virtual Machine (EVM), permitindo a execução de contratos inteligentes e integração com aplicativos descentralizados (BANCO CENTRAL DO BRASIL, 2023). Essa compatibilidade facilita a interoperabilidade e a integração com soluções já estabelecidas, reduzindo custos de desenvolvimento e promovendo a adoção.

A iniciativa busca facilitar transações mais rápidas e eficientes, potencializando o desenvolvimento de novos modelos de negócio e serviços financeiros. Além disso, por ser emitido e controlado pelo Banco Central, o DREX garante segurança jurídica e estabilidade monetária, fatores essenciais para a confiança dos usuários e para a estabilidade econômica. A compatibilidade do DREX com a EVM é altamente relevante para a organização, pois permite que a plataforma seja desenvolvida utilizando contratos inteligentes e uma infraestrutura já familiar aos desenvolvedores e usuários do Ethereum. Integrar o DREX como meio de transação na organização significa ser pioneira no desenvolvimento do setor governamental, inovando em direção a uma maior transparência, participação e confiança pública nas atividades de serviço público.

Primeiramente, o DREX proporciona estabilidade monetária, uma vez que é lastreado no Real e emitido pelo Banco Central, reduzindo riscos associados à volatilidade de criptomoedas tradicionais. Isso facilita a compreensão e adoção por parte da população local, que pode transacionar em uma moeda digital que representa o Real, sem a necessidade de lidar com conversões ou flutuações cambiais significativas. Além disso, o uso do DREX garante conformidade com as regulamentações financeiras brasileiras, aspecto crucial para um projeto voltado à gestão de recursos públicos. A adoção de uma moeda digital oficial promove transparência nas transações e pode facilitar a integração com sistemas governamentais e instituições financeiras.

2.5. Decentralized Autonomous Organization (DAO)

Uma Organização Autônoma Descentralizada (DAO) é uma forma inovadora de organização que opera por meio de regras codificadas como contratos inteligentes, sem gestão centralizada, e cujas decisões são tomadas coletivamente pelos seus membros (JENTZSCH, 2016). As DAOs utilizam a tecnologia blockchain para garantir a transparência, a imutabilidade e a execução automática das decisões tomadas.

As principais características das DAOs incluem a descentralização, onde não há uma hierarquia tradicional e as decisões são tomadas de forma coletiva; a autonomia, pois operam independentemente de intervenções humanas diretas após a implantação; e a transparência, já que as regras e transações são públicas e auditáveis na blockchain.

Implementadas em plataformas como o Ethereum, as DAOs executam protocolos definidos por contratos inteligentes, garantindo que as decisões acordadas pelos membros sejam executadas automaticamente. As decisões dentro de uma DAO são geralmente tomadas através de mecanismos de votação, onde a influência de cada membro é proporcional aos seus tokens de governança. Isso promove um ambiente democrático onde as políticas e orientações da organização são moldadas coletivamente pelos interesses e consenso dos seus membros, sem a necessidade de uma autoridade centralizada interferir no processo de tomada de decisão. Algumas aplicações e vantagens das DAOs são:

- Gestão de Projetos Open Source: Coordenação de esforços e recursos para desenvolvimento de software de forma colaborativa.
- Investimentos Coletivos: Fundos descentralizados onde membros decidem onde investir recursos, compartilhando riscos e retornos.
- Governança de Protocolos: Tomada de decisões sobre parâmetros e atualizações em protocolos financeiros descentralizados, garantindo que o desenvolvimento seja alinhado com os interesses dos usuários.

As vantagens das DAOs incluem a transparência e a confiança, com operações abertas que podem ser verificadas por qualquer membro; a participação democrática, onde membros têm voz proporcional nas decisões, promovendo engajamento; e a eficiência operacional, através da eliminação de intermediários e burocracias desnecessárias.

No contexto governamental, as DAOs podem promover a transparência nas decisões públicas, com registro aberto de decisões e gastos públicos. Elas também incentivam o engajamento cidadão, permitindo participação direta dos cidadãos na formulação de políticas e projetos, e contribuem para a redução da corrupção, através de processos automatizados que minimizam a intervenção humana e, consequentemente, a oportunidades de fraude.

Na Figura X, a organização tradicional é representada por uma estrutura hierárquica em formato de pirâmide, onde o poder e a tomada de decisões estão concentrados nos níveis superiores da hierarquia. Este modelo centralizado evidencia como as informações fluem de cima para baixo, limitando a participação dos níveis inferiores no processo decisório.

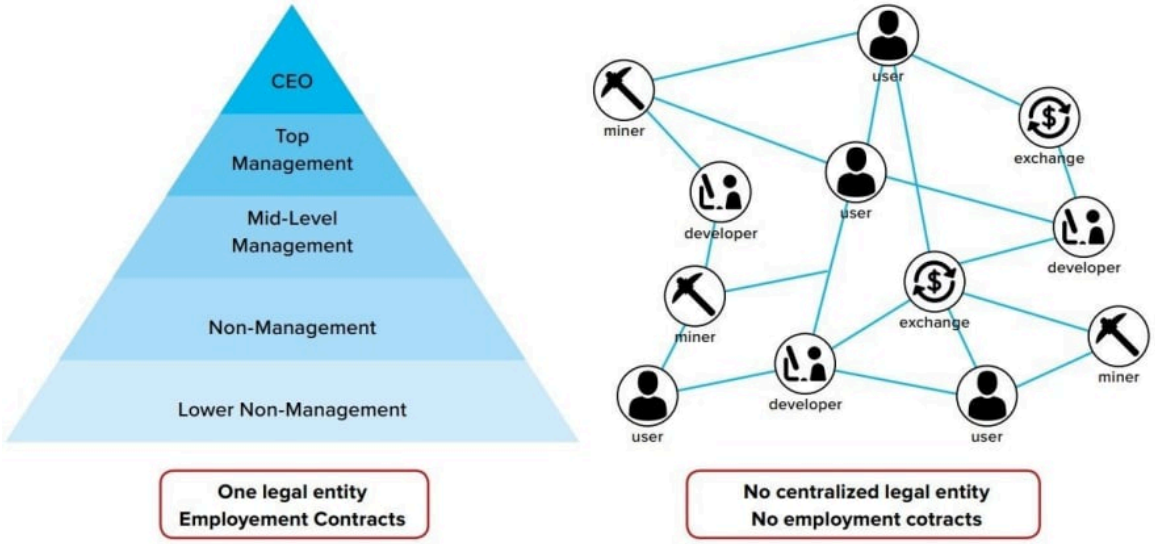


Figure 3. Comparing traditional organization and DAO

Em contraste, a DAO é ilustrada como uma rede descentralizada, onde todos os membros estão interconectados sem uma autoridade central dominante. Essa representação destaca a natureza distribuída das DAOs, na qual a governança é coletiva e as decisões são tomadas de forma colaborativa pelos participantes. A imagem enfatiza as diferenças fundamentais entre os modelos organizacionais, mostrando como as DAOs promovem maior participação, transparência e descentralização em comparação com as estruturas organizacionais tradicionais. Essa visualização reforça a compreensão de como a Bairro DAO busca inovar na gestão pública, adotando um modelo que incentiva o engajamento cidadão e a eficiência nos processos de tomada de decisão.

3. Trabalhos Correlatos

Este capítulo apresenta uma análise detalhada de trabalhos e iniciativas que exploram o uso de blockchain, contratos inteligentes e organizações autônomas descentralizadas (DAOs) em contextos similares ao do projeto. O objetivo é compreender os desafios, as soluções implementadas e os resultados obtidos por esses projetos, identificando práticas que podem ser incorporadas ou adaptadas para o desenvolvimento da plataforma. São analisados trabalhos correlatos que se destacam pela relevância e pelas contribuições significativas nas áreas de governança descentralizada, participação cidadã e transparência pública.

3.1. GovChain: Blockchain na Administração Pública

O estudo conduzido por Ølnes et al. (2017), intitulado "Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Public Services", investiga o potencial da tecnologia blockchain na administração pública. O objetivo principal é analisar como os governos podem utilizar a blockchain para aprimorar a eficiência, a transparência e a confiança nos serviços públicos, enfrentando problemas como burocracia excessiva, corrupção e falta de credibilidade nas instituições governamentais.

A pesquisa envolveu uma revisão abrangente da literatura existente e a análise de casos de uso em diferentes países. Os autores identificaram áreas-chave onde a tecnologia blockchain poderia ser aplicada na esfera governamental. Uma dessas áreas é a de registros

públicos, onde a implementação de registros imutáveis para propriedades, documentos oficiais e outros ativos pode garantir a integridade dos dados e facilitar o acesso por parte dos cidadãos e autoridades.

Outra aplicação relevante é a identidade digital. A criação de sistemas de identidade baseados em blockchain permitiria a autenticação segura dos indivíduos, dando ao cidadão controle sobre seus próprios dados pessoais e reduzindo o risco de fraude e roubo de identidade. No contexto da votação eletrônica, a blockchain pode ser utilizada para desenvolver sistemas que assegurem transparência, anonimato e resistência a fraudes, aumentando a confiança do público no processo eleitoral.

O estudo concluiu que a tecnologia blockchain tem o potencial de revolucionar a administração pública, mas também identificou desafios significativos que precisam ser superados. Um dos principais desafios é a interoperabilidade, ou seja, a necessidade de integração com sistemas existentes e entre diferentes organizações governamentais. A escalabilidade também é uma preocupação, uma vez que as limitações técnicas atuais podem dificultar o suporte a grandes volumes de dados e transações necessários em nível governamental. Questões regulamentares representam outro obstáculo. Há incertezas legais e a necessidade de regulamentações específicas que abranjam o uso da blockchain no setor público. Além disso, existe resistência cultural e organizacional à adoção de novas tecnologias, o que pode dificultar a implementação de soluções baseadas em blockchain. Para a Bairro DAO, os insights de GovChain são valiosos na identificação de oportunidades e obstáculos na aplicação da blockchain em serviços públicos. O projeto pode:

- Adaptar casos de uso, implementando registros transparentes de propostas, votações e execução de obras.
- Planejar a escalabilidade, desenvolvendo uma arquitetura que suporte crescimento no número de usuários e transações.
- Envolver stakeholders, promovendo o envolvimento de autoridades locais e cidadãos para facilitar a adoção.

3.2. Decidim: Plataforma de Participação Cidadã

Decidim é uma plataforma digital de código aberto criada pela Prefeitura de Barcelona em 2016, com o objetivo de promover a participação cidadã na tomada de decisões municipais (FUSTER MORELL et al., 2017). A iniciativa busca fortalecer a democracia participativa, permitindo que cidadãos influenciem diretamente políticas públicas, projetos e investimentos que afetam suas comunidades.

A plataforma foi desenvolvida utilizando tecnologias web modernas e princípios de design centrado no usuário. Decidim oferece funcionalidades que permitem aos cidadãos propor iniciativas, participar de debates públicos, votar em propostas e acompanhar a implementação de projetos. Todas as propostas e discussões são públicas e auditáveis, promovendo transparência e confiança no processo democrático. A plataforma é modular e extensível, possibilitando a integração com outras tecnologias, incluindo blockchain, para aprimorar a segurança e a imutabilidade dos registros.

Decidim teve ampla adoção em Barcelona, envolvendo milhares de cidadãos e resultando em diversas políticas e projetos implementados com base nas propostas e votações

realizadas. A plataforma também foi adotada por outras cidades e organizações ao redor do mundo, demonstrando sua eficácia em promover participação cidadã. O sucesso de Decidim destaca a importância de facilitar o envolvimento de diferentes segmentos da população e de fornecer ferramentas acessíveis para que os cidadãos participem ativamente da governança local.

3.3. Smart Dubai: Blockchain em Serviços Governamentais

A iniciativa Smart Dubai, lançada em 2016 pelo governo dos Emirados Árabes Unidos, tem como meta transformar Dubai na primeira cidade do mundo totalmente alimentada por blockchain (SMART DUBAI, 2016). O objetivo é melhorar a eficiência dos serviços governamentais, reduzir custos operacionais e promover a inovação tecnológica, posicionando Dubai como líder global em tecnologias emergentes.

O projeto envolve a implementação de blockchain em diversas áreas, incluindo pagamentos governamentais, registros de propriedade, licenças, documentos oficiais e serviços comerciais. Ao digitalizar e automatizar processos administrativos por meio da blockchain, o governo busca reduzir a burocracia, agilizar transações e eliminar a necessidade de documentos físicos. Isso inclui a gestão de escrituras e transações imobiliárias, a emissão e verificação de documentos oficiais de forma segura e eficiente, e a facilitação de processos empresariais, como registro de empresas e contratos.

A iniciativa resultou em significativas reduções de custos e ganhos de eficiência. Estima-se que a economia em horas de trabalho e recursos financeiros seja substancial, permitindo que o governo redirecione esforços para áreas mais estratégicas. A confiança pública nos serviços governamentais aumentou devido ao uso de registros imutáveis, promovendo transparência e responsabilidade. Além disso, Dubai consolidou sua posição como referência em adoção de tecnologias emergentes, atraindo investimentos e talentos globais.

A experiência de Dubai demonstra como a blockchain pode ser integrada em serviços governamentais em grande escala. A Bairro DAO pode aprender com a abordagem estratégica de Smart Dubai, alinhando o projeto com políticas públicas e objetivos governamentais. Estabelecer parcerias estratégicas com empresas e organizações pode fortalecer a implementação e fornecer recursos adicionais. Desenvolver soluções que sejam acessíveis e úteis para os cidadãos aumenta a adoção e o impacto positivo da plataforma. Além disso, considerar o contexto local e adaptar as soluções às necessidades específicas da comunidade garantirá maior relevância e eficácia.

3.4. Open Government Partnership: Transparência e Participação Cidadã

A Open Government Partnership (OGP) é uma iniciativa internacional lançada em 2011, que visa promover governos mais transparentes, participativos e responsáveis (OGP, 2021). Governos participantes comprometem-se a implementar planos de ação com reformas concretas em áreas como transparência fiscal, acesso à informação e participação cidadã. O Brasil é um dos países fundadores da OGP e tem desenvolvido iniciativas para aprimorar a governança pública.

A OGP funciona por meio da elaboração de planos de ação nacionais, nos quais cada país estabelece compromissos específicos com metas claras e mensuráveis. A iniciativa

promove a colaboração multissetorial, envolvendo governos, sociedade civil e setor privado. O monitoramento e a avaliação são componentes-chave, com acompanhamento dos progressos e avaliação independente dos resultados, garantindo que os compromissos sejam cumpridos e que os impactos sejam mensurados.

- Transparência: Abertura de dados e informações governamentais.
- Participação Cidadã: Envolvimento dos cidadãos na tomada de decisões.
- *Accountability*: Prestação de contas e responsabilidade governamental.

A OGP tem contribuído para maior transparência, com a abertura de dados governamentais e melhoria no acesso à informação. A iniciativa tem fortalecido o engajamento cidadão, criando canais para a participação ativa da população em processos decisórios. Isso tem resultado em políticas públicas mais alinhadas com as necessidades dos cidadãos e em maior confiança nas instituições. A implementação de mecanismos de prestação de contas e fiscalização também tem sido um instrumento eficaz no combate à corrupção. Os princípios e práticas da OGP podem orientar a Bairro DAO na promoção de uma governança local mais aberta e participativa. Definir compromissos claros e estabelecer metas específicas para transparência e participação pode direcionar os esforços do projeto. A inclusão da comunidade é essencial; envolver os cidadãos desde a concepção até a implementação do projeto garante que as soluções atendam às necessidades reais e promovam o senso de propriedade. A transparência nos processos, com a publicação de dados e informações de forma acessível e compreensível, aumenta a confiança e o engajamento da população.

3.5. MakerDAO: Um Caso de Sucesso em Governança Descentralizada

A MakerDAO é amplamente reconhecida como uma das DAOs mais bem-sucedidas no ecossistema blockchain (MAKERDAO, 2020). Ela gerencia a *stablecoin* DAI, um ativo digital totalmente descentralizado e lastreado por garantias on-chain. Este caso é um exemplo de como fundos podem ser gerenciados de forma segura e transparente sem depender de uma entidade centralizada.

- **Gestão Descentralizada:**
  - Todos os fundos e colaterais usados para emitir a *stablecoin* DAI são bloqueados em contratos inteligentes que operam sob regras definidas pela comunidade de governança.
  - A comunidade, por meio do token de governança MKR, vota nas mudanças de parâmetros, como taxas de juros e novos colaterais aceitos. Essas decisões são automaticamente implementadas pelos contratos inteligentes após as votações.
- **Transparência e Auditabilidade:**
  - Toda a gestão financeira é registrada na blockchain, permitindo que qualquer pessoa acompanhe as transações em tempo real.
  - Os contratos inteligentes imutáveis garantem que nenhuma decisão seja alterada ou revertida sem o consenso da comunidade.

- **Segurança Automática:**
  - Em caso de crises (como flutuações no valor dos colaterais), o sistema executa liquidações automáticas para proteger os fundos restantes e manter a estabilidade do DAI.

Assim como a MakerDAO gerencia colaterais para manter a estabilidade do token DAI, a DAO pode gerenciar recursos públicos de forma transparente e segura, garantindo que cada real investido em projetos seja rastreável e utilizado de acordo com as regras aprovadas pela comunidade. A experiência desta plataforma demonstra que é possível implementar um modelo de governança descentralizado, eficiente e resiliente, mesmo em sistemas complexos e com grandes volumes de fundos.

Um dos testes mais conhecidos do sistema ocorreu durante a "Quinta-Feira Negra" em março de 2020, quando o mercado de criptoativos enfrentou uma crise. Apesar das perdas iniciais, as ferramentas de governança e os contratos inteligentes da DAO garantiram a continuidade e estabilidade do sistema, mostrando a robustez do modelo descentralizado.

A experiência da MakerDAO é um exemplo poderoso de como fundos podem ser gerenciados exclusivamente por contratos inteligentes, eliminando o risco de controle centralizado. Ao adotar princípios semelhantes, a plataforma pode assegurar que recursos públicos sejam usados de maneira responsável e transparente, aumentando a confiança dos cidadãos no sistema.

4. Desenvolvimento

Este capítulo descreve as etapas de desenvolvimento do sistema da Organização Autônoma Descentralizada, detalhando as funcionalidades dos contratos inteligentes, scripts de apoio, e prototipagem para validação do modelo. O desenvolvimento deste projeto DAO tem como objetivo implementar uma solução descentralizada para governança e gestão financeira de uma comunidade. A escolha de cada tecnologia foi estratégica para atender às necessidades do projeto. Integrando tecnologias robustas como blockchain Ethereum, contratos inteligentes em Solidity, e ferramentas como Truffle e Ganache. O objetivo principal foi criar uma solução funcional para a governança descentralizada, permitindo a criação e votação de propostas, além de gerenciar a distribuição de fundos. Cada componente foi projetado para atender às necessidades específicas da organização, alinhado aos princípios apresentados no capítulo de fundamentação teórica.

4.1. Análise de Requisitos

Requisitos são uma descrição das necessidades para um determinado produto, onde o objetivo básico é identificar e documentar o que é realmente necessário, de forma a comunicar claramente essa informação tanto ao cliente quanto aos membros da equipe de desenvolvimento. A definição de requisitos de maneira não ambígua é de suma importância para que os riscos sejam identificados e não ocorram surpresas durante o desenvolvimento do produto (LARMAN, 2000). Os requisitos de um software podem ser classificados em Requisitos Funcionais (RF) e Requisitos Não Funcionais (RNF). Os Requisitos Funcionais são responsáveis por definir as funções e comportamentos do software, enquanto os Requisitos Não Funcionais dizem respeito às restrições de desenvolvimento, aspectos de

desempenho, interfaces com o usuário, confiabilidade, segurança, manutenibilidade, portabilidade e padrões a serem seguidos. Esta seção detalha os requisitos identificados para a DAO.

4.1.1. Requisitos Funcionais

Para o levantamento dos Requisitos Funcionais do projeto, foram considerados os recursos mínimos necessários para o funcionamento adequado da aplicação e as principais funcionalidades esperadas em uma plataforma descentralizada. Os requisitos foram definidos com base nas necessidades identificadas durante a pesquisa exploratória e refletem as funcionalidades essenciais para promover a participação cidadã e a transparência na gestão de serviços públicos.

ID	Descrição
RF-01	O sistema deve permitir que os membros da DAO submetam propostas para novos serviços.
RF-02	As propostas devem incluir um atributo de descrição contendo claras informações com justificativa, orçamento e cronograma.
RF-03	O sistema deve permitir que os membros da DAO votem nas propostas submetidas
RF-04	Cada membro deve ter um único token de voto para participar das decisões.
RF-05	O sistema deve calcular o quórum necessário para aprovação de uma proposta com base em regras predefinidas.
RF-06	Após aprovação, o sistema deve permitir a execução automatizada das ações associadas à proposta.
RF-07	O sistema deve liberar pagamentos de forma condicionada ao cumprimento de etapas das obras.

Table 1. Requisitos Funcionais

4.1.2. Requisitos Não Funcionais

Os Requisitos Não Funcionais estabelecem critérios de qualidade e restrições que o sistema deve atender para assegurar seu desempenho, segurança, usabilidade e conformidade com padrões. Para o projeto em questão, os RNFs foram definidos visando garantir a eficácia e a confiabilidade da plataforma, bem como a satisfação dos usuários.

ID	Descrição
RNF-01	O sistema deve garantir alta segurança contra fraudes e ataques cibernéticos, utilizando criptografia avançada.
RNF-02	O sistema deve ser capaz de processar múltiplas propostas e votações simultaneamente, garantindo escalabilidade.
RNF-03	O consumo de gas deve ser otimizado, minimizando os custos para os usuários ao interagir com os contratos.
RNF-04	O sistema deve garantir a imutabilidade de registros, impossibilitando alterações retroativas nas transações.
RNF-05	A implementação dos contratos inteligentes deve seguir os padrões ERC-20, garantindo compatibilidade com DREX.
RNF-06	A plataforma deve suportar atualizações nos contratos inteligentes sem comprometer os dados existentes ou a integridade do sistema.

Table 2. Requisitos Não-Funcionais

4.1.3. Escalabilidade

A escalabilidade é um fator crucial no desenvolvimento da plataforma, principalmente devido às limitações inerentes às blockchains públicas como o Ethereum. Por mais robusta que seja a rede, sua capacidade de processar transações simultâneas ainda apresenta desafios significativos, especialmente em sistemas com grande número de usuários.

A rede Ethereum, apesar das melhorias com o mecanismo de consenso Proof-of-Stake (PoS), enfrenta limitações na quantidade de transações por segundo (TPS) que podem ser processadas. Um aumento exponencial no número de usuários pode resultar em:

- **Atrasos na Rede:**
  - A alta demanda pode congestionar a rede, causando atrasos na validação de transações.
- **Altos Custos de Gás:**
  - Em momentos de congestionamento, as taxas de gas aumentam significativamente, tornando o uso inviável para muitos participantes.

A escolha de implementar a aplicação em um contexto local é proposital e estrategicamente alinhada às limitações de escalabilidade. Um público limitado facilita a administração do sistema e diminui a sobrecarga na rede Ethereum. Com um volume menor de transações simultâneas, os custos de gás são minimizados, mantendo a plataforma acessível para todos os membros da comunidade. O modelo reduz a complexidade das votações e aprovações, permitindo uma governança mais ágil e organizada.

Ao priorizar bairros como unidade de governança, a DAO maximiza a eficiência,

participação comunitária e transparência, sem comprometer o desempenho da plataforma.

4.2. Tecnologias

Com o objetivo de desenvolver um sistema com suporte ao DREX, a plataforma poderá automatizar pagamentos utilizando contratos inteligentes que liberam fundos em DREX conforme metas e condições previamente estabelecidas são atingidas. Todas as transações financeiras serão registradas na blockchain, permitindo auditorias e aumentando a confiança pública no gerenciamento dos recursos.

Na Figura 5, é ilustrado o funcionamento de uma transação por meio de contratos inteligentes utilizando os personagens Alice e Bob. A figura demonstra como Alice, desejando compartilhar dados com Bob, estabelece um contrato inteligente que define as condições de acesso e os termos da transação. O contrato inteligente atua como um intermediário autônomo e confiável, garantindo que as regras acordadas sejam executadas exatamente como programadas, sem a necessidade de intervenção de terceiros ou autoridades centrais. Este exemplo visual simplifica a compreensão de como contratos inteligentes podem automatizar processos e assegurar a integridade e transparência nas transações entre partes. A ilustração destaca a eliminação de intermediários tradicionais, reforçando a eficiência e a confiança proporcionadas pela tecnologia dos *smart contracts* nas interações descentralizadas.

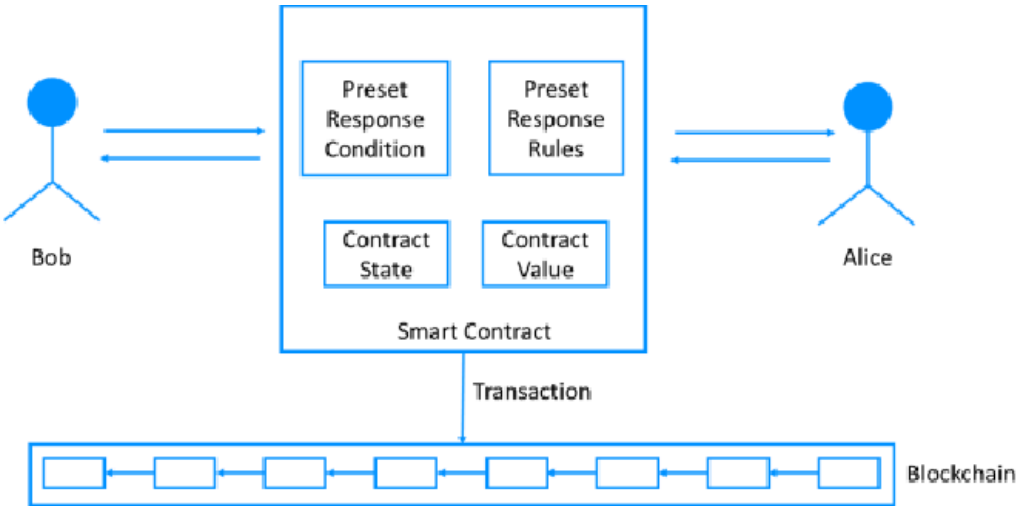


Figure 4. ***Smart Contract Interaction***

O projeto faz uso de um conjunto de tecnologias e ferramentas cuidadosamente escolhidas para assegurar a qualidade, a segurança e a eficiência no desenvolvimento de contratos inteligentes e no ecossistema da Bairro DAO. A linguagem Solidity foi utilizada para implementar os contratos inteligentes, como o *BairroGovernance*, responsável pela lógica de governança, o *Treasury*, que gerencia os fundos, e o *VoteToken*, associado ao poder de voto. Especialmente projetada para a Ethereum Virtual Machine (EVM), a linguagem oferece recursos seguros para manipulação de dados on-chain, garantindo integridade e clareza na execução de transações e processos decisórios.

Para tornar o desenvolvimento mais seguro e alinhado às melhores práticas, foram adotados os contratos do OpenZeppelin. Esses padrões são amplamente reconhecidos pela

comunidade Ethereum, reforçando a robustez e a confiabilidade dos contratos implementados. A organização do ciclo de desenvolvimento, testes e implantação dos contratos inteligentes ficou a cargo do Truffle, um framework que simplifica a compilação, a migração e a execução de scripts, assegurando a correta implantação dos contratos em ambientes de teste ou redes públicas.

A simulação de uma blockchain local foi realizada com o Ganache, permitindo testar o comportamento dos contratos em um ambiente controlado, sem custos de execução ou tempo de espera. Esse ambiente favoreceu a experimentação, o avanço manual de blocos e a verificação de estados, tornando o processo de validação do sistema mais rápido e eficiente.

A integração entre os contratos e o nível de automação do projeto foi facilitada pelo uso de JavaScript e Node.js. O JavaScript, aliado ao web3.js, atuou como ponte entre os contratos inteligentes e a lógica de alto nível, permitindo a criação de scripts para tarefas específicas, como criação de propostas, votação e execução de decisões. O Node.js, por sua vez, forneceu o ambiente necessário para executar essas ferramentas de desenvolvimento.

Por fim, a manutenção de um código legível, padronizado e consistente foi assegurada pelo uso do Prettier, em conjunto com o plugin prettier-plugin-solidity, que formata automaticamente o código fonte. Essa atenção à clareza do código reforça a seriedade do projeto, tornando o processo de leitura, revisão e melhoria mais simples e produtivo.

Em suma, o conjunto de tecnologias – Solidity, OpenZeppelin, Truffle, Ganache, JavaScript, Node.js, web3.js e Prettier – operou de maneira integrada, permitindo a criação de um ecossistema seguro, ágil e de fácil manutenção para o desenvolvimento e validação dos contratos inteligentes da plataforma.

4.3. Prototipagem

O protótipo desenvolvido representa uma versão funcional da DAO, incorporando e executando os smart contracts. A base deste sistema está nos contratos inteligentes escritos em Solidity. Estes contratos são implantados em uma blockchain, fornecendo uma plataforma imutável e auditável para a tomada de decisões. O coração do projeto é o contrato ***BairroGovernance***, que gerencia a governança, enquanto outros contratos, como ***VoteToken*** e ***Treasury***, fornecem suporte essencial. O ***VoteToken*** é usado para representar o poder de voto, e o ***Treasury*** é responsável por gerenciar fundos associados a propostas aprovadas. O contrato ***BairroGovernance*** foi projetado para possibilitar o ciclo completo de governança, desde a criação de propostas até a execução de ações correspondentes. Ele segue um fluxo lógico rigoroso, começando com a criação de uma proposta por um membro da DAO. A proposta inclui endereços de destino, valores financeiros, chamadas de função específicas e uma descrição. Após a criação, a proposta passa por um período de votação, onde os participantes utilizam seus tokens de voto para decidir seu destino. Esse processo é fundamentalmente democrático, garantindo que todas as decisões sejam tomadas de forma coletiva e transparente.

4.3.1. Desenvolvimento dos Smart Contracts

Os contratos foram desenvolvidos utilizando a linguagem Solidity, seguindo padrões de design e melhores práticas recomendadas pela comunidade Ethereum.

Contrato	Funções Principais	Responsabilidades
Governance	`propose(), vote(), executeProposal()`	Gerenciar propostas de votação
Treasury	`releaseInitialPayment(), releaseFinalPayment(), confirmCompletion()`	Gerenciar fundos e pagamentos
Token	`assignToken(), revokeToken()`	Gerenciar tokens de governança

Table 3. DAO' Smart Contracts

4.3.1.1. Contrato de Governança

O contrato ***BairroGovernance*** é o núcleo da governança descentralizada da Bairro DAO. Ele viabiliza a criação, votação e execução de propostas, estabelecendo um fluxo lógico que garante participação coletiva e transparente. A estrutura de dados utilizada organiza todas as informações necessárias para identificar o proponente, os endereços-alvo, os valores financeiros, as chamadas de função e o estado atual da proposta. A definição de estados – como `Pending`, `Active` e `Executed` – permite acompanhar o progresso de uma proposta ao longo do tempo, assegurando clareza no processo decisório.

```
struct Proposal
{
        uint256 id;
        address proposer;
        address[] targets;
        uint256[] values;
        bytes[] calldatas;
        string description;
        ProposalState state;
        uint256 votesFor;
        uint256 votesAgainst;
        uint256 startBlock;
        uint256 endBlock;
}
```

Figure 5. Estrutura da proposta

O atributo `description` desempenha um papel fundamental na comunicação do conteúdo de cada proposta. É por meio dele que o criador da proposta pode detalhar, de forma clara e completa, as informações essenciais que embasam a iniciativa. Isso inclui, por exemplo, a especificação dos valores monetários associados, prazos, expectativas de resultados, justificativas e quaisquer outros elementos que contribuam para o entendimento pleno da proposta por parte dos demais participantes. Dessa forma, o campo `description` se torna um canal central de transparência e clareza, garantindo que todos tenham acesso às

informações necessárias para tomar decisões bem embasadas.

A função `propose()` é fundamental, pois inicia todo o fluxo de governança. Ela recebe os parâmetros necessários para criar a proposta, atribui um identificador único e define o período de votação. Abaixo, um pequeno trecho do código ilustra essa função. Neste exemplo, o código foi sintetizado para destacar apenas os elementos essenciais.

```
function propose(
    address[] memory targets,
    uint256[] memory values,
    bytes[] memory calldatas,
    string memory description
) public returns (uint256) {
    uint256 proposalId = proposalCount++;
    uint256 startBlock = block.number + 1;
    uint256 endBlock = startBlock + 20; // exemplo simplificado para testes

    proposals[proposalId] = Proposal({
        id: proposalId,
        proposer: msg.sender,
        targets: targets,
        values: values,
        calldatas: calldatas,
        description: description,
        state: ProposalState.Pending,
        votesFor: 0,
        votesAgainst: 0,
        startBlock: startBlock,
        endBlock: endBlock
    });

    emit ProposalCreated(proposalId, msg.sender, targets, values, calldatas,
description, startBlock, endBlock);
    return proposalId;
}
```

Figure 6. Código do contrado de Governança

No contexto da DAO, essa função representa o ponto de partida do processo decisório. Ao chamá-la, um membro submete uma proposta para ser avaliada pelos demais participantes. Emite um evento `ProposalCreated` que notifica a rede (e qualquer observador externo) de que uma nova proposta foi criada. Eventos são importantes para indexar informações fora da blockchain e possibilitam que interfaces gráficas ou outros sistemas acompanhem as atividades do contrato.

Uma vez criada, a proposta aguarda o início do período de votação. A contabilização de votos e a eventual execução da proposta ocorrem posteriormente, por meio de funções como `vote()` e `executeProposal()`.

```
function executeProposal(uint256 proposalId) external {
    Proposal storage proposal = proposals[proposalId];
    ProposalState state = getProposalState(proposalId);
    require(
        state == ProposalState.Succeeded,
        "Proposal is not in a succeeded state"
    );

    // Execute proposal actions
    proposal.state = ProposalState.Executed;

    for (uint256 i = 0; i < proposal.targets.length; i++) {
        (bool success, ) = proposal.targets[i].call{
            value: proposal.values[i]
        }(proposal.calldatas[i]);
        require(success, "Transaction execution failed");
    }

    emit ProposalExecuted(proposalId);
}
```

Figure 7. Código de execução de proposta

A função `executeProposal` desempenha o papel crucial de efetivar as decisões aprovadas no processo de governança. Uma vez que a proposta atinge o estado `Succeeded` (ou seja, recebeu votos suficientes para sua aprovação), essa função atualiza o estado da proposta para `Executed` e executa cada uma das ações planejadas – enviando transações para os endereços-alvo com os valores e dados fornecidos. Caso todas as operações sejam concluídas com êxito, um evento (`ProposalExecuted`) é emitido, registrando de forma pública e imutável que a proposta foi efetivamente implementada. Isso garante que as deliberações coletivas do sistema de governança sejam colocadas em prática, fortalecendo a transparência e a autonomia do processo decisório.

A função `vote()` verifica se o participante possui tokens de governança e se ainda não votou naquela proposta, garantindo que cada membro exerça seu direito de voto de forma única. Caso as condições sejam atendidas, o voto é contabilizado de acordo com o saldo de tokens do votante, assegurando o poder de votação do usuário. Ao final do período de votação, se o quórum mínimo for alcançado e a maioria favorável obtida, a função `executeProposal()` aciona as transações especificadas, efetivando a decisão da comunidade.

Dessa forma, o contrato de governança não apenas organiza a lógica decisória, mas também zela pela integridade do processo, assegurando que o fluxo democrático seja respeitado e auditável por qualquer participante.

4.3.1.2. Contrato de Tesouraria

O contrato **Treasury.sol** é responsável por gerenciar os fundos da DAO e garantir que os pagamentos sejam liberados de maneira segura e condicional. Ele protege os ativos do sistema enquanto implementa a lógica necessária para pagamentos baseados no progresso de serviços

prestados.

O contrato, através da função `releaseInitialPayment()` libera um pagamento inicial para o prestador de serviços. Este é o primeiro passo do fluxo financeiro, garantindo que os fundos sejam liberados apenas se as condições forem atendidas.

Através da função `releaseFinalPayment()`, o contrato libera o pagamento final ao prestador de serviços após a conclusão do serviço e confirmação pelo mesmo. Assegura que o pagamento final só seja feito quando o prestador de serviços confirmar que o trabalho foi concluído. Essa abordagem protege os interesses da DAO e reduz o risco de desvios.

```
event InitialPaymentReleased(address serviceProvider, uint256 amount);
event FinalPaymentReleased(address serviceProvider, uint256 amount);
event ServiceCompleted(address serviceProvider);
```

Figure 8. Eventos do Contrato de Tesouraria

Os eventos `InitialPaymentReleased`, `FinalPaymentReleased` e `ServiceCompleted` representam ocorrências importantes no fluxo do contrato e, uma vez emitidos, tornam-se registros públicos e imutáveis na blockchain. Isso significa que todos os participantes da rede podem acessar, consultar e auditar esses eventos, garantindo maior transparência, rastreabilidade e confiança no processo. Cada evento, ao ser disparado, adiciona um carimbo permanente do momento em que ocorreu, do provedor de serviço envolvido e dos valores liberados, permitindo que qualquer interessado confirme o cumprimento dos acordos estabelecidos, bem como o ciclo de pagamentos e a conclusão dos serviços.

```
function releaseInitialPayment(
       uint256 amount
   ) public onlyOwner nonReentrant {
       // Checks
       require(!isInitialPaymentReleased, "Initial payment already released");
       require(
           fundToken.balanceOf(address(this)) >= amount,
           "Insufficient funds"
       );

       // Effects
       isInitialPaymentReleased = true;
       emit InitialPaymentReleased(serviceProvider, amount); // Emit event after
state change

       // Interactions
       fundToken.transfer(serviceProvider, amount);
   }
```

Figure 9. Contrato de realização de pagamento

A função `releaseInitialPayment` no contrato de tesouraria é responsável por liberar o pagamento inicial ao prestador de serviços, garantindo que a operação seja executada de forma segura e transparente. Antes da transferência, o código verifica se o pagamento inicial ainda não foi realizado e se há fundos suficientes no contrato. Caso as condições sejam atendidas, o estado do pagamento é atualizado para indicar que a parcela inicial foi liberada, e um evento (`InitialPaymentReleased`) é emitido, tornando o registro público e imutável na blockchain. Por fim, os fundos são efetivamente transferidos para o prestador de serviços, cumprindo o acordo de forma auditável e confiável.

4.3.1.3. Contrato de Token de Governança

O contrato desempenha um papel central no sistema DAO, servindo como o token de governança que define o poder de voto dos participantes. Implementado no padrão ERC20, ele garante compatibilidade com a infraestrutura Ethereum e facilita a integração com ferramentas e contratos baseados no mesmo padrão.

O token VOTE é utilizado como unidade de poder de decisão na DAO. Cada participante detém um número de tokens que corresponde à sua influência nas decisões tomadas por meio de propostas e votações. Essa abordagem não apenas garante transparência, mas também atribui responsabilidade proporcional ao peso de cada voto, incentivando a participação ativa dos membros.

No contexto do sistema, o contrato **VoteToken** é essencial para:

- **Distribuição de Poder de Voto**: Cada participante recebe um token representando seu poder de voto.
- **Segurança e Compatibilidade**: Como um token ERC20, o **VoteToken** herda a robustez do padrão, assegurando a integridade de transferências e consultas de saldo.
- **Interação com Outros Contratos**: O contrato **BairroGovernance** utiliza o saldo de **VoteToken** dos participantes para calcular votos a favor ou contra uma proposta.

O contrato foi implementado utilizando o padrão ERC20, com funcionalidades básicas de criação e transferência de tokens. Ele também oferece suporte a funções adicionais, como emissão de novos tokens, para o caso de novos moradores no bairro. Sua implementação assegura que cada morador receba um único VOTE token.

- **Proposta e Votação**:
    - Os proponentes devem possuir um saldo mínimo de **VoteToken** para criar propostas, garantindo compromisso financeiro ou reputacional com a comunidade.
    - Durante a votação, cada token representa um voto, e o saldo de tokens define a força da decisão de cada participante.
- **Quórum e Resultados**:
    - O saldo total de **VoteToken** em circulação é utilizado para calcular o quórum mínimo necessário para validar uma votação.

- Após o término do período de votação, os resultados são determinados com base na quantidade de votos favoráveis e contrários, proporcional aos saldos dos votantes.

O **VoteToken** introduz uma governança proporcional e escalável, permitindo que a influência de cada participante esteja diretamente vinculada ao número de tokens que ele possui. Isso incentiva a aquisição e retenção de tokens, além de criar um mercado interno de poder de decisão. Além disso, sua implementação no padrão ERC20 assegura interoperabilidade com soluções financeiras existentes, reforçando a eficiência do sistema.

No futuro, o **VoteToken** pode ser integrado com modelos de staking ou recompensas para engajar ainda mais os membros da DAO. Por exemplo, tokens poderiam ser ganhos por participação em atividades comunitárias ou retenção prolongada, reforçando a fidelidade ao sistema.

4.3.1.4. Contrato de Mock ERC

O **MockERC20** é um contrato simulado que representa uma *stablecoin*. Sua inclusão no projeto permitiu a realização de testes no sistema sem depender de tokens reais. Ele foi implementado com base no padrão ERC20, garantindo compatibilidade com outras ferramentas Ethereum. Esse contrato prepara o sistema para a integração futura com uma stablecoin, como BRZ ou DREX, para gerenciar fundos reais.

4.3.1.5. Contrato de Migrações

O contrato **Migrations** é um componente essencial para a implantação de contratos no Ethereum. Ele rastreia quais contratos já foram migrados, prevenindo duplicações. Embora seja trivial para desenvolvedores experientes, sua inclusão no projeto foi vital para garantir que a sequência de implantação fosse mantida.

4.3.2. Comandos de Configuração de Ambiente de Desenvolvimento

Compilar os contratos:

c. truffle compile

4. Rodar a blockchain local:
    a. ganache-cli
5. Executar:
    a. truffle migrate – reset: Faz a migração para a blockchain local
    b. truffle exec ./scripts/3_create_proposal.js: Executa os contratos

4.4. Execução

Esta etapa busca garantir que o sistema funcione conforme o esperado e esteja preparado para resistir a possíveis vulnerabilidades. Através de um ambiente de teste controlado, simulamos cenários reais de uso, verificando a corretude funcional, a segurança e a eficiência dos contratos. A validação foi conduzida em um ambiente de desenvolvimento local, utilizando ferramentas como o Truffle e Ganache.

4.4.1. Comandos de Execução e Verificação de Logs

Comando Truffle Compile:

- `truffle compile`

- **Comando Truffle Migrate:**
  - `truffle migrate --reset`
- **Comando Truffle Exec:**
  - `truffle exec ./scripts/3_create_proposal.js`

4.4.2. Testes

Os testes foram divididos em etapas que cobriram desde funções individuais até fluxos completos do sistema. Destaca-se a importância do script `3_create_proposal.js`, que simula o ciclo de vida completo de uma proposta, permitindo testar as interações entre os contratos e os usuários.

4.4.2.1. Script de Criação de Proposta

O script `3_create_proposal.js` automatizou o ciclo de vida completo de uma proposta. Abaixo, descrevemos os passos executados pelo script:

```
vitorpchavess@MacBook-Pro-de-Vitor DAO % truffle exec ./scripts/3_create_proposal.js

Using network 'development'.

Step 1: Checking proposer's VoteToken balance...

Proposer's VoteToken balance: 1
Checking voters' VoteToken balances...

Voter 0xA9ed8C6AF06a4adF2B91fC0578514301499d5783 has 1 VoteToken(s).
Voter 0x4166A6E1059D514FB2A1bA8d00530ff589340691 has 1 VoteToken(s).
Voter 0x5660e52Ac28c391D970C5fce0D40C8bEB06F5fD6 has 1 VoteToken(s).
Voter 0x29ae42Ef3e181b01225540bfea401f5b532e3540 has 1 VoteToken(s).
Voter 0xDAa6FF6C001993508423AA06a626C36304604a02 has 1 VoteToken(s).
Step 2: Creating initial payment proposal...

Initial payment proposal created successfully! Proposal ID: 0

Step 3: Simulating voting on initial proposal...

Voter 0xA9ed8C6AF06a4adF2B91fC0578514301499d5783 voted in favor.
Voter 0x4166A6E1059D514FB2A1bA8d00530ff589340691 voted in favor.
Voter 0x5660e52Ac28c391D970C5fce0D40C8bEB06F5fD6 voted in favor.
Voter 0x29ae42Ef3e181b01225540bfea401f5b532e3540 voted in favor.
Voter 0xDAa6FF6C001993508423AA06a626C36304604a02 voted in favor.
All votes cast successfully.

Step 4: Advancing blocks to end voting period...

Advanced 17 blocks.

Advanced 17 blocks.

Proposal state after advancing blocks: 3
Step 5: Executing initial payment proposal...

Initial payment executed successfully.
```

Figure 10. Script de execução I

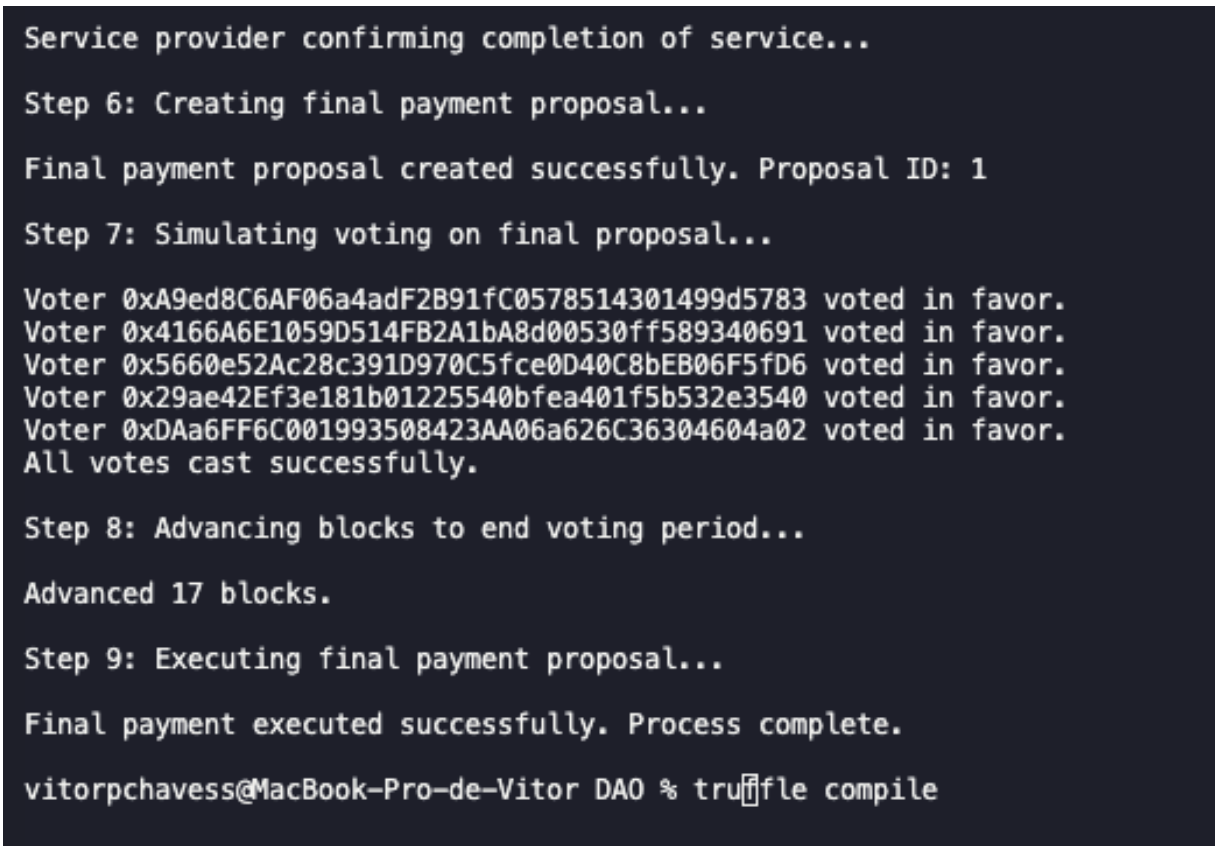


Figure 11. Script de execução II

1. **Validação de Saldos**: O script inicia verificando se o proponente e os votantes possuem saldo de tokens VOTE. Caso algum participante não possua o token, o script interrompe a execução e retorna um erro, simulando a impossibilidade de criar uma proposta sem o compromisso financeiro necessário.
2. **Criação de Proposta**: Uma proposta é criada utilizando a função `propose()` do contrato de governança. Os parâmetros incluem:
    a. **Valores financeiros**: Define os montantes envolvidos nas transações.
    b. **Chamadas de função**: Codifica, em formato ABI, as funções que serão executadas, como `releaseInitialPayment()`.
3. **Simulação de Votação**: Os membros da DAO, representados por contas simuladas, participam da votação. Cada participante utiliza seus tokens para votar a favor ou contra a proposta. O script registra cada voto e verifica a consistência dos dados, garantindo que as regras de votação sejam respeitadas.
4. **Avanço de Blocos**: Para simular o decorrer do tempo na blockchain, o script utiliza o método `evm_mine` do Ganache CLI, avançando o número de blocos necessários para atingir o fim do período de votação. Isso permite testar a transição de estados da proposta, de ativa para sucedida ou derrotada.
5. **Atualização e Execução da Proposta Inicial**: Após o término do período de votação, o estado da proposta é atualizado com base nos votos recebidos e no quórum atingido. Se a proposta for aprovada, o script chama a função `executeProposal()`, que aciona as transações especificadas. No caso, ocorre a liberação do pagamento inicial para o prestador de serviços através do contrato de tesouraria.

O prestador de serviços confirma a conclusão da etapa inicial, o que permite a criação de uma nova proposta para o pagamento final. Essa confirmação pode ser realizada através de um evento ou interação externa com o sistema.

6. **Criação da Proposta Final:** Similar ao passo 2, uma nova proposta é criada utilizando a função `propose()` do contrato ***BairroGovernance***, desta vez para liberar o pagamento final.
7. **Simulação de Votação na Proposta Final:** Os membros da DAO novamente votam na proposta final utilizando seus tokens de governança. O script utiliza novamente a função **vote()** para registrar os votos favoráveis. Todos os votos são contabilizados corretamente.
8. **Avanço dos Blocos:** Assim como no passo 4, o script avança os blocos necessários para finalizar o período de votação da proposta final. A simulação garante a transição do estado da proposta para *Succeeded*, permitindo sua execução. 17 blocos foram avançados com sucesso.
9. **Confirmação e Pagamento Final**: O fluxo é repetido para uma segunda proposta, que visa liberar o pagamento final. Esta etapa só é executada após a confirmação do prestador de serviços de que o trabalho foi concluído, assegurando que os fundos são liberados de acordo com o progresso real do projeto.

Este script foi essencial para validar não apenas as funções isoladas, mas também a interação entre elas em um cenário completo de uso, desde a criação da proposta até a execução dos pagamentos.

4.5. Considerações Finais

4.5.1. Desafios

Um desafio técnico e operacional significativo é garantir que os registros digitais na blockchain reflitam com precisão as atividades realizadas no mundo real, ou seja, as operações *off-chain*. Há uma necessidade de mecanismos confiáveis que validem e verifiquem os dados inseridos na blockchain, evitando fraudes ou discrepâncias. A utilização de oráculos, sensores IoT e outras tecnologias de validação externa pode ser explorada para conectar eventos do mundo físico aos contratos inteligentes. Por exemplo, no caso de uma obra pública, é necessário confirmar que determinada etapa foi concluída conforme especificado antes de liberar o pagamento correspondente. Estabelecer processos de verificação independentes, possivelmente envolvendo auditorias externas ou participação comunitária na fiscalização, pode reforçar a confiabilidade do sistema.

Promover a compreensão sobre o DREX e sua utilização dentro da plataforma é outro desafio significativo. Muitos cidadãos podem não estar familiarizados com moedas digitais ou podem ter desconfiança em relação a elas. Oferecer educação e suporte aos usuários é essencial para incentivar a participação cidadã e a adoção da tecnologia. Estratégias como oficinas educativas, tutoriais online, suporte técnico e canais de atendimento podem ajudar a superar barreiras tecnológicas e culturais. Além disso, é importante abordar questões de inclusão digital. Nem todos os membros da comunidade têm acesso fácil a dispositivos

tecnológicos ou à internet. Desenvolver soluções que sejam acessíveis mesmo em ambientes com limitações tecnológicas, ou promover iniciativas que melhorem a infraestrutura digital local, pode ser necessário para garantir que a plataforma seja inclusiva.

4.5.2. Trabalhos futuros

Os trabalhos futuros para o projeto incluem a implementação de uma interface gráfica que permita aos cidadãos interagirem de forma intuitiva e acessível com a plataforma, seja por meio de uma aplicação web ou móvel. A autenticação segura de usuários e a integração com carteiras digitais são prioridades para garantir uma experiência confiável e fluida, possibilitando o gerenciamento de tokens. Além disso, planeja-se a criação de visualizações gráficas para apresentar dados e estatísticas de maneira clara e compreensível. Esses esforços visam consolidar a relação entre os registros digitais na blockchain e os eventos do mundo real, utilizando tecnologias como oráculos para validar e refletir com precisão os avanços e execuções dos projetos.

Um dos desafios enfrentados durante o desenvolvimento foi o custo elevado de transações na rede Ethereum, especialmente em cenários com grande volume de interações. Para mitigar essa limitação, o projeto explorará alternativas de blockchain que ofereçam custos mais baixos sem comprometer a segurança e a descentralização. Entre as opções consideradas, redes de segunda camada como Arbitrum e Optimism se destacam por utilizarem rollups, que processam transações fora da cadeia principal e consolidam os resultados na blockchain principal, reduzindo significativamente as taxas de gas e aumentando a eficiência.

A adoção dessas soluções permitirá que a DAO evolua para um sistema mais acessível e escalável, mantendo os princípios de transparência e governança descentralizada que definem o projeto. Essa abordagem visa superar as limitações técnicas e econômicas atuais, posicionando a plataforma como uma ferramenta viável e inovadora para o gerenciamento de recursos e projetos públicos em comunidades, garantindo uma experiência mais sustentável e eficiente para os usuários.

5. Conclusão

Este trabalho explorou e demonstrou a viabilidade técnica e prática da utilização de Organizações Autônomas Descentralizadas (DAOs) como uma solução inovadora para promover transparência e engajamento cívico em atividades públicas de nível local. O estudo apresentou o desenvolvimento da plataforma Bairro DAO, uma aplicação prática da tecnologia blockchain voltada para a gestão descentralizada de serviços públicos, permitindo que os cidadãos participem ativamente em processos como a submissão de propostas, monitoramento financeiro e operacional, além do gerenciamento transparente dos recursos alocados.

Ao longo do trabalho, foram abordados fundamentos teóricos e práticos necessários para a implementação da DAO, destacando o potencial da blockchain em reduzir custos de verificação e assegurar que todas as transações e decisões sejam registradas de forma imutável e auditável. Essa característica não apenas aumenta a confiança nos processos, mas também proporciona um modelo de governança que distribui o poder de decisão entre os membros da comunidade, eliminando intermediários e minimizando oportunidades de corrupção.

A implementação da plataforma representa uma ruptura significativa com os modelos tradicionais de organização e gestão pública, ao integrar contratos inteligentes e um sistema de governança transparente e participativo. Contudo, o sucesso dessa iniciativa depende de uma mudança de mentalidade tanto por parte dos gestores públicos quanto dos cidadãos. Resistências à mudança, desconfiança em sistemas descentralizados e falta de familiaridade com tecnologias digitais são desafios a serem superados. Para enfrentar essas barreiras, é essencial promover uma cultura de inovação e aprendizado contínuo. Envolver líderes comunitários, educadores e influenciadores locais pode ser uma estratégia eficaz para difundir os valores e as vantagens das dos sistemas descentralizados, construindo confiança e adesão ao modelo.

Além disso, a consolidação de uma DAO eficiente e sustentável exige abordagens multidisciplinares que integrem aspectos técnicos, legais, sociais e educacionais. Colaborações entre desenvolvedores, gestores públicos, juristas, especialistas em segurança digital, educadores e a própria comunidade são cruciais para criar uma plataforma robusta e alinhada às reais necessidades dos cidadãos. Essa sinergia pode não apenas garantir o sucesso do sistema, mas também estabelecer um modelo replicável que inspire novas iniciativas em diferentes contextos governamentais.

Por fim, este trabalho contribui para o avanço do conhecimento e das práticas relacionadas às organizações autônomas descentralizadas, demonstrando como a tecnologia blockchain pode ser uma ferramenta transformadora para fortalecer a governança pública, aumentar a transparência e fomentar a participação cidadã. O futuro da Bairro DAO é promissor, mas depende do comprometimento coletivo em superar os desafios apresentados e aproveitar as oportunidades de inovação para criar uma sociedade mais justa, participativa e eficiente.

6. Referências

ANTONOPOULOS, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, 2017.

ARCHANA PRASHANTH JOSHI MENG HAN, Yan Wang. survey on security and privacy issues of blockchain technology. v. 1, p. 121–147, 2018.

ATZEI, Nicola; BARTOLETTI, Massimo; CIMOLI, Tiziana. A Survey of Attacks on Ethereum Smart Contracts (SoK). In: *Proceedings of the 6th International Conference on Principles of Security and Trust (POST)*, Springer, 2017. p. 164-186.

AZARIA, Asaph et al. MedRec: Using Blockchain for Medical Data Access and Permission Management. In: *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016. p. 25-30.

BANCO CENTRAL DO BRASIL. Real Digital - DREX. 2023. Disponível em: https://www.bcb.gov.br/drex. Acesso em: 1 nov. 2024.

BUTERIN, Vitalik. A Next-Generation Smart Contract and Decentralized Application Platform. *Ethereum White Paper*, 2014. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 1 nov. 2024.

CIVIC. Civic: Secure Identity for Web3. Disponível em: https://www.civic.com/. Acesso em: 17 dez. 2024.

ETHEREUM FOUNDATION. Solidity Documentation. 2021. Disponível em: https://docs.soliditylang.org/. Acesso em: 1 nov. 2024.

FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2018.

FUSTER MORELL, Mayo et al. Citizen Participation in the City of the Future: The Case of Decidim Barcelona. In: *2017 Smart Cities Symposium Prague (SCSP)*. IEEE, 2017.

HARDY, Stephen; MAURO, John. Blockchain Voting: Election Integrity in the Digital Age. *Journal of Cyber Policy*, v. 2, n. 3, p. 306-328, 2017.

JÄRVINEN, Joni et al. Blockchain in Practice: Lessons from a Groundbreaking Supply Chain Implementation. *IEEE Software*, v. 36, n. 4, p. 55-61, 2019.

JENTZSCH, Christoph. Decentralized Autonomous Organization to Automate Governance. *White Paper*, 2016. Disponível em: https://download.slock.it/public/DAO/WhitePaper.pdf. Acesso em: 1 nov. 2024.

KOSHY, George et al. Blockchain-Based Supply Chain Management: A Systematic Mapping Study. In: *2018 International Conference on Emerging Technologies (ICET)*. IEEE, 2018. p. 1-6.

LEE, Charlie. Litecoin - Open Source P2P Digital Currency. 2011. Disponível em: https://litecoin.org. Acesso em: 1 nov. 2024.

MAKERDAO. MakerDAO: The Maker Protocol. Disponível em: https://makerdao.com/en/. Acesso em: 17 dez. 2024.

MORALIS ACADEMY. DAO vs Traditional Organization. *Moralis Academy Blog*, 2021. Disponível em: https://academy.moralis.io/blog/dao-vs-traditional-organization. Acesso em: 1 nov. 2024.

MUSLIMIN, Muslimin; NAZIEF, Budi Rahardjo. Stable Cryptocurrency: Review of the Existing Stablecoins. In: *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*. IEEE, 2020. p. 235-240.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 1 nov. 2024.

NARAYANAN, Arvind et al. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

OGP - Open Government Partnership. What is Open Government? 2021. Disponível em: https://www.opengovpartnership.org/. Acesso em: 1 nov. 2024.

ØLNES, Svein; UBACHS, Jelmer; JANSEN, Arild. Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Public Services. *Government Information Quarterly*, v. 34, n. 3, p. 355-364, 2017.

REGNER, Ferdinand; NAGEL, Jan; REPPEL, Alexander. Blockchain-Based Tokens and Their Impact on Financing Decisions. *Business Transformation through Blockchain*, p. 183-204, 2019.

SCHÄR, Fabian. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, v. 103, n. 2, p. 153-174, 2021.

SCHWARTZ, David; YOUNGS, Noah; BRITO, Arthur. The Ripple Protocol Consensus Algorithm. *Ripple Labs Inc.*, 2014.

SIEGEL, David et al. Understanding the DAO Attack. 2016. Disponível em: https://www.coindesk.com/understanding-dao-hack-journalists. Acesso em: 1 nov. 2024.

SMART DUBAI. Dubai Blockchain Strategy. 2016. Disponível em: https://www.smartdubai.ae/initiatives/blockchain. Acesso em: 1 nov. 2024.

SZABO, Nick. The Idea of Smart Contracts. 1997. Disponível em: https://nakamotoinstitute.org/the-idea-of-smart-contracts/. Acesso em: 1 nov. 2024.

TRANSFERO SWISS. BRZ Token. 2021. Disponível em: https://brztoken.io/. Acesso em: 1 nov. 2024.

VRIGNAUD, P.; SALKELD, P.; CAMPBELL, T. Bitcoin Energy Consumption: An Improved Methodology. *International Journal of Energy Economics and Policy*, v. 9, n. 6, p. 432-439, 2019.

WOOD, Gavin. Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, 2014.

YAKOVENKO, Anatoly. Solana: A New Architecture for a High Performance Blockchain. *White Paper*, 2018. Disponível em: https://solana.com/solana-whitepaper.pdf. Acesso em: 1 nov. 2024.

ZHENG, Zibin et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017. p. 557-564.

APÊNDICE B - Código Fonte

O código utilizado para desenvolver o sistema da DAO está disponível na plataforma GitHub através do link: `https://github.com/VitorPChaves/dao/tree/main`