UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

MESTRADO ACADÊMICO EM COMPUTAÇÃO

DELANO JOSÉ HOLANDA MAIA

UMA SOLUÇÃO PARA CROWDFUNDING COM TRANSPARÊNCIA EM INVESTIMENTOS BASEADA EM BLOCKCHAIN

QUIXADÁ

2022

DELANO JOSÉ HOLANDA MAIA

UMA SOLUÇÃO PARA CROWDFUNDING COM TRANSPARÊNCIA EM INVESTIMENTOS BASEADA EM BLOCKCHAIN

Dissertação apresentada ao Curso de Mestrado Acadêmico em Computação do Programa de Pós-Graduação em Computação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em computação. Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Emanuel Ferreira Coutinho

QUIXADÁ

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M185s Maia, Delano José Holanda.
Uma Solução para crowdfunding com transparência em investimentos baseada em blockchain / Delano José Holanda Maia. – 2022.
143 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Campus de Quixadá, Programa de Pós-Graduação em Computação, Quixadá, 2022.
Orientação: Prof. Dr. Emanuel Ferreira Coutinho.

1. Blockchains (Base de dados). 2. Contrato Inteligente. 3. Crowdfunding. 4. Auditoria. I. Título.
CDD 005

DELANO JOSÉ HOLANDA MAIA

UMA SOLUÇÃO PARA CROWDFUNDING COM TRANSPARÊNCIA EM INVESTIMENTOS BASEADA EM BLOCKCHAIN

Dissertação apresentada ao Curso de Mestrado Acadêmico em Computação do Programa de Pós-Graduação em Computação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em computação. Área de Concentração: Ciência da Computação

Aprovada em: 02 de Setembro de 2022

BANCA EXAMINADORA

Prof. Dr. Emanuel Ferreira Coutinho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Glauber Dias Gonçalves
Universidade Federal do Piauí (UFPI)

Prof. Dr. Gabriel Antoine Louis Paillard
Universidade Federal do Ceará (UFC)

Prof. Dr. Leonardo Oliveira Moreira
Universidade Federal do Ceará (UFC)

Dedico a minha família, em especial minha mãe Oziene. Ela sempre acreditou que o melhor caminho a se seguir é sempre pelos estudos, por ele alcançamos o mundo.

AGRADECIMENTOS

Primeiramente a Deus, pois ele sempre me mostra os melhores caminhos e sem a presença dele em minha vida esse trabalho não poderia ser executado.

Ao meu orientador, Emanuel Coutinho, por sempre me apoiar durante todas as etapas desse trabalho. Sinto por ele uma gratidão por todos os ensinamentos e também o companheirismo para conseguir encarar e superar todos os obstáculos que sugiram durante esse trabalho. Muito obrigado!

A minha família que sempre está pronta para fazer o impossível para me ajudar durante as adversidades da vida. Eles me ofereceram toda a ajuda e incentivo necessário na busca da vitória nessa jornada.

Por fim, agradeço àqueles que me ajudaram na concepção desse trabalho, seja com palavras amiga, seja com comentários importantes para a construção do mesmo.

“Você ganha força, coragem e confiança através de cada experiência em que você realmente para e encara o medo de frente.”

(Eleanor Roosevelt)

RESUMO

O surgimento de *startups* vem sendo cada vez mais comum no cenário mundial. Muitas ideias boas acabam surgindo em meio aos cenários que passamos no dia a dia. Na grande maioria das vezes, a pessoa ou grupo que pensou e idealizou certa ideia de produto ou serviço, não coloca o projeto adiante por falta de dinheiro para, por exemplo, custos iniciais com prototipagem. Com isso, ideias promissoras acabam sendo esquecidas e perdidas ao longo do tempo. Sites de financiamento coletivo onde várias pessoas ajudam um projeto a sair do papel são facilmente encontrados na internet, os chamados *crowdfunding*. Neles podemos encontrar projetos de jogos, produtos inovadores ou até mesmo já comuns, mas com uma nova abordagem, sejam com maior facilidade de uso ou com redução de custos. Com o intermédio desses sites temos muitas formas de pagamento, cartão de crédito, boleto bancário, PIX, transferências bancárias ou *criptomoedas*. A *blockchain* se destaca com aplicações em *criptomoedas*, utilizando-se de contratos inteligentes agrega credibilidade às transações realizadas mesmo que de forma descentralizada. Os contratos inteligentes passaram a ser utilizados devido à adição da customização oferecida às transações, abrindo caminho na busca de soluções *blockchain* para problemas encontrados na sociedade. O objetivo deste trabalho é propor uma arquitetura e solução para o problema de rastreabilidade do dinheiro investido pelos financiadores dos projetos, oferecendo um pouco mais de controle do investimento, um poder de decisão na hora em que o gerente do projeto começar a empregar o dinheiro arrecadado. Por fim, temos uma análise de custos financeiros e de tempos de transações na rede Ethereum, ajudando aos investidores entenderem para onde vai o recurso arrecadado.

Palavras-chave: Blockchain. Contrato Inteligente. Crowdfunding. Auditoria.

ABSTRACT

The emergence of startups has been increasingly common on the world stage. Many good ideas end up emerging in the midst of scenarios that we go through on a daily basis. In most cases, the person or group who determined and idealized an idea for a product or service, do not put the project ahead due to lack of money for, for example, initial costs with prototyping. With this, promising ideas end up being forgotten and lost over time. Sites where several people find a project coming out of the paper are easily found on the internet, called crowdfunding. In them we can find game projects, innovative or even common products, but with a new approach, either with greater ease of use or with reduced costs. Through these sites we have many forms of payment, credit card, bank slip, PIX, bank transfers or cryptocurrencies. The blockchain stands out with applications in cryptocurrencies, using smart contracts, it adds credibility as transactions carried out, even if in a decentralized way. Smart contracts began to be used due to the addition of customization offered to transactions, paving the way in the search for blockchain solutions to problems encountered in society. The objective of this work is to propose an architecture and solution to the problem of traceability of the money invested by project financers, offering a little more control over the investment, a decision-making power when the project manager starts to spent the money raised. Finally, we have an analysis of financial costs and transaction times on the Ethereum network, helping investors to understand where the funds raised are going.

Keywords: Blockchain. Smart Contract. Crowdfunding. Audit.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

CVM	Comissão de Valores Mobiliários
SETI	*Search for ExtraTerrestrial Inteligence*
PoW	*Proof-of-Work*
ETF	Fundo de Investimento Inovador
P2P	*Peer-to-peer*
PoS	*Proof-of-Stake*
BFT	*Byzantine Fault Tolerance*
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
CNPJ	Cadastro Nacional de Pessoas Jurídicas
MSP	*Membership Service Provider*
ETH	Ether
DoS	*Denial of Service*
IoT	*Internet of Things*
DML	*Data Manipulation Language*
SQL	*Structure Query Language*
Embrapa	Empresa Brasileira de Pesquisa Agropecuária
SAIC	Sistema de Acompanhamento de Instrumentos Contratuais
Serpro	Serviço Federal de Processamento de Dados
cUSD	*Celo Dollar*
ICOs	*Initial Coin Offerings*
OOAD	Análise e Design Orientados a Objeto
AoN	Tudo ou Nada
KIA	Mantenha o Tudo
SGS	Esquema de Metas Esticadas
STO	*Security Token Offering*
SMA	Social Media Analítica
EPI	Equipamento de Proteção Pessoal
CRUD	*Create - Read - Update - Delete*
API	*Application Programming Interface*
RF	Requisitos Funcionais

RNF	Requisitos Não Funcionais
EVM	*Ethereum Virtual Machine*
ABI	*Apliccation Binary Interface*

SUMÁRIO

1 INTRODUÇÃO

Existem diversas formas no mercado para investimentos, desde ações na bolsa de valores, mercado imobiliário, dentre outros. Por muito tempo, acreditava-se que deixar o dinheiro na poupança seria uma boa forma de fazer ele render. Para Cunha *et al.* (2009) o papel do empreendedor sempre foi de fundamental importância na sociedade, porém se intensificou nas últimas décadas, em decorrência dos avanços tecnológicos e das novas exigências da sociedade do conhecimento, cuja competitividade exige ação empreendedora, inovação e estruturação de sistemas de inovação.

Diante de cenários econômicos cada vez mais competitivos, empreender se torna uma tarefa difícil quando não se consegue obter o crédito necessário para iniciar determinado projeto (WILL *et al.*, 2016). A partir desse percalço, empreendedores emergentes estão buscando alternativas para a falta de crédito por meio do *crowdfunding* (BUYSERE *et al.*, 2012).

O *crowdfunding* pode ser descrito com um processo em que o público colabora para o financiamento de um projeto (FELINTO, 2013). Pequenos empreendimentos, cujas produções dependem de inovação, já aderem ao *crowdfunding* há algum tempo e, de acordo com (MOLLICK; ROBB, 2016), como consequência da falta de garantia exigida pelas instituições tradicionais de crédito, o financiamento à inovação desses negócios ocorre de forma limitada, mas promissora.

Boa parte das opções tradicionais de financiamento exigem diversas garantias e custos altos relativos ao desenvolvimento do negócio em questão, porém, no *crowdfunding*, acontece o inverso. Basta o empreendedor desenvolver um plano de viabilidade de seu negócio e enviar para uma plataforma de financiamento, a qual aprovará ou não o empreendimento e o disponibilizará ao público (FELIPE, 2015). O apoio que a "multidão" fornece aos negócios coletivos, seja em nível de alocação de recurso financeiro e de expertise, seja de divulgação (HU *et al.*, 2015), tem disseminado o *crowdfunding* como um mecanismo capaz de superar as limitações financeiras tradicionais, especialmente do financiamento para os pequenos negócios e os empreendedores individuais (COSH *et al.*, 2009).

1.1 Motivação

De acordo com ANBIMA (2017), em 13 de Julho de 2017, a Comissão de Valores Mobiliários (CVM) editou a instrução n° 588, que regulamenta as operações de *crowdfunding*,

referentes à oferta pública de distribuição de valores mobiliários de emissão de sociedades empresárias de pequeno porte realizada com dispensa de registro por meio de plataforma eletrônica de investimento participativo. O jornal Comércio (2018) comenta que após se passar um ano da sua regulamentação, o investimento colaborativo em novas empresas está mudando de patamar no Brasil. Com R$ 50 milhões já levantados junto a pequenos investidores, o *equity crowdfunding* - uma espécie de "vaquinha" *online* que recruta investidores pela Internet - evolui para além do circuito de *startups* de tecnologia. Chega agora a companhias da economia real, financiando até projetos imobiliários e proporcionando cheques mais gordos aos empreendedores.

O *equity crowdfunding* segundo EqSeed (2022), possibilita que um conjunto de investidores financie empresas em troca de participação nelas. Com o *equity crowdfunding*, investidores fornecem fundos para uma empresa e recebem uma parte da mesma na forma de participação societária (*equity*) ou de títulos conversíveis de dívida que, no futuro, podem ser convertidas em participação societária (*equity*) da empresa investida.

A respeito dos retornos obtidos no *equity crowdfunding*, o Investimento... (2016) fala que eles são de médio e longo prazo e o investimento é de alto risco, mas possuem seus atrativos. A modalidade é vista como uma oportunidade de diversificar a carteira e ingressar no universo das *startups* sem colocar todo o dinheiro e suor. Conforme Fernando Rizzo, da plataforma Broota, "Sem a plataforma de *equity*, é muito difícil entrar nesse mercado, que na maioria das vezes, é formado por investidores anjos, que são muito ricos".

Como definido por Mollick e Kuppuswamy (2014), o *crowdfunding* se refere aos esforços de indivíduos e grupos empresariais - cultural, social e com fins lucrativos - para financiar seus empreendimentos, recorrendo a contribuições de valores relativamente pequenos, de um número grande de indivíduos, utilizando uma plataforma na Internet, sem intermediários financeiros padrão.

Existem muitas pessoas criativas ou visionárias que em muitos casos acabam tendo ideias de produtos ou serviços revolucionários, com grande chances de sucesso, mas que por conta da falta de recursos financeiros são levados a deixar suas ideias de lado. Com a ajuda dessas "vaquinhas", pessoas se agrupando para alcançar um montante de dinheiro, existe assim uma maior facilidade. Elas oferecem uma oportunidade para tais pessoas seguirem seus sonhos tirando o projeto do papel.

Em plataformas como a citada Broota[1] existem diversos projetos, uma forma de

[1] http://www.broota.com.br/ - Acesso em: 08 set. 2022

vitrine para investidores, possibilitando a leitura de detalhes dos projetos e auxiliando-os na familiarização com a ideia a ser desenvolvida. Caso haja algum interesse, o investimento pode ser feito na própria plataforma. O dinheiro arrecadado é administrado pela própria plataforma, situação que acaba por deixar o investidor às escuras com relação a como seu investimento será de fato utilizado dentro do projeto.

Com isso, tem-se que uma forma de auditoria para os gastos em relação ao projeto como um todo, considerando os valores pagos com o dinheiro investido no projeto, ajudaria na transparência por parte da equipe idealizadora do projeto e também na confiabilidade por parte do investidor. Exemplos de aplicações simples, que ofereçam garantia de integridade dos dados e também a possibilidade de rastreabilidade são encontrados na tecnologia *blockchain*. *Blockchain* consiste em um conceito tecnológico que foi popularizado em 2008 e tinha como principal propósito, inicialmente, dar suporte à criação da *criptomoeda* Bitcoin (NAKAMOTO, 2008).

A *blockchain* em sua essência é um *ledger* (livro-razão) público que permite o registro imutável em cadeia de blocos, armazenando o registro histórico das transações por criptografia e preservando as identidades e as chaves de segurança dos usuários (LYRA; MEIRINO, 2017). Os integrantes da rede possuem uma cópia exata desse livro-razão de registro de transações e contratos, garantindo assim a autenticidade dos dados inseridos e a grande dificuldade de alteração por conta do encadeamento de blocos.

O Bitcoin funciona como um sistema de caixa eletrônico descentralizado, supostamente projetado e desenvolvido por Satoshi Nakamoto, que apresentou a moeda e a tecnologia *blockchain* ao mundo em 2008, por meio de seu artigo *Bitcoin: A Peer-to-Peer Electronic Cash System* (BARBER *et al.*, 2012). Embora não tenha sido especificada no artigo de Nakamoto, a terminologia *blockchain* refere-se a uma cadeia de blocos, uma série de blocos de dados que são encadeados criptograficamente (MATTILA, 2016).

No entendimento de Veuger (2018), a principal característica inovadora da tecnologia *blockchain* é a capacidade de rastrear transações em bases de dados descentralizadas e públicas, reduzindo a possibilidade de fraude. Justamente, o que é buscado na proposta deste trabalho, é a possibilidade da aplicação ofertar mais transparência aos investidores. O *ledger* distribuído fornece um registro quase imutável e garante a rastreabilidade das transações uma vez que será muito difícil manipular os dados na *blockchain*, tendo em vista que as mudanças são imediatamente refletidas em todas as cópias da razão pela rede e elas são vinculadas à transação

anterior (BATUBARA *et al.*, 2018).

Muitos dos aspectos inovadores da tecnologia *blockchain* (por exemplo, contratos inteligentes) são relativamente novos (BOSU *et al.*, 2019). Embora o número de projetos de software com *blockchain* tenha crescido nos últimos dois anos, muitas ferramentas e bibliotecas que possam suportar seu desenvolvimento ainda estão em fase de desenvolvimento. Como a *blockchain* é uma tecnologia nova, há escassez de desenvolvedores com domínio suficiente em comparação com a maioria dos domínios não *blockchain* (ABREU, 2020).

Juntamente com a *blockchain* tem-se os contratos inteligentes (*Smart Contracts*) que de acordo com Carvalho e Ávila (2019) nada mais são do que os contratos codificados e colocados em uma base de dados de execução automática e autônoma. A Figura 1 exibe características de um contrato inteligente, neste trabalho foram exploradas algumas delas como: segurança e alta confiança.

Com o uso dessa tecnologia, é garantido ao investidor uma forma de transparência do projeto em relação ao financeiro. Compras de todos os tipos ficam identificadas nos blocos, valores passam a ser imutáveis, aumentando assim a confiabilidade da aplicação utilizada. Para o criador do projeto, obter mais confiança dos investidores pode atrair mais recursos ajudando na concretização dos seus objetivos.

Figura 1 – Benefícios dos Contratos Inteligentes.

Fonte: o autor.

1.2 Objetivos

Neste contexto, este trabalho leva em consideração conceitos de Engenharia de Software e apresenta um modelo de arquitetura fazendo uso da tecnologia *blockchain*. A arquitetura da aplicação *blockchain* utiliza contratos inteligentes para rastrear o dinheiro arrecadado pelo projeto *crowdfunding*. Esse tipo de aplicação gera transações e cada uma delas tem um custo de processamento computacional para ser agregada na rede. Com isso, o objetivo principal deste trabalho é propor uma solução para *crowdfunding* de forma integrada com uma rede *blockchain* buscando melhorias no processo de investimentos em projetos com colaboração coletiva.

Os objetivos específicos deste trabalho são: (i) desenvolver uma infraestrutura que sustente as necessidades da proposta; (ii) propor uma arquitetura que servirá como referência; (iii) desenvolver uma aplicação para publicar os projetos em busca de financiamento, listá-los para conhecimento dos possíveis investidores; (iv) confeccionar um cenário de avaliação da proposta; e (v) realizar um estudo dos custos gerados nas transações, sejam eles financeiros ou de tempo.

Como foco principal da pesquisa tem-se a busca em construir uma solução que utiliza a tecnologia *blockchain* e assim responder às seguintes questões:

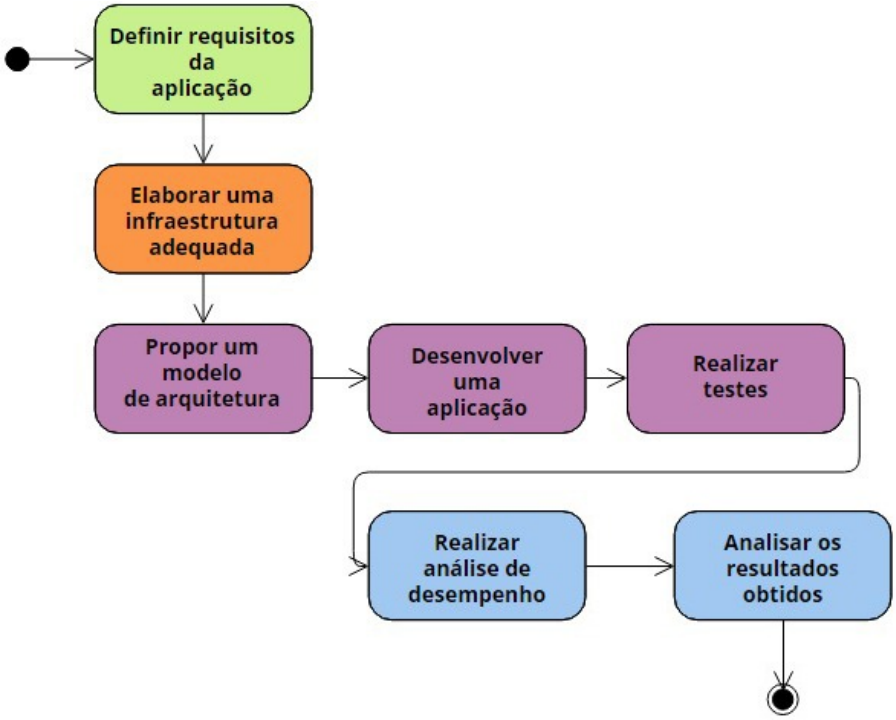
- Questão 1: quais os principais desafios tecnológicos que os investidores e os criadores de projeto podem enfrentar para alterar a forma que o *crowdfunding* possui em gestão financeira utilizando a tecnologia *blockchain*?
- Questão 2: é possível desenvolver uma solução baseada em *blockchain* que contemple confiabilidade, transparência e segurança, buscando um maior número de investidores para projetos inovadores?

1.3 Metodologia

Levando em consideração os objetivos elencados anteriormente, o trabalho foi subdividido em pequenas etapas buscando cumpri-los. Três atividades consideradas importantes foram realizadas na fase inicial da pesquisa em busca da compreensão dos conceitos relacionados a tecnologia abordada. Atividades como levantamento da bibliografia da *blockchain*, análise de ferramentas e tecnologias e não menos importante: uma busca aos trabalhos relacionados. O foco dessas etapas sempre esteve voltado para o desenvolvimento de uma solução que faça uso da tecnologia *blockchain*.

Seguindo o trabalho, a Figura 2 apresenta uma visão mais completa por meio de um diagrama de atividades de como ocorreu a execução das atividades.

Figura 2 – Fluxo das atividades realizadas



Fonte: o autor.

A seguir, uma descrição de cada etapa de forma detalhada é apresentada:

- **Definir requisitos da aplicação:** Em busca de uma melhor utilização da *blockchain* em uma aplicação *crowdfunding* foram levantados alguns requisitos que seriam cruciais e indispensáveis na validação do trabalho. Com a exploração dos requisitos, foi possível ter uma ideia do que era necessário para desenvolver a aplicação de forma funcional;
- **Elaborar uma infraestrutura adequada:** Durante o estudo realizado neste trabalho, mostrou-se importante a criação de uma infraestrutura que englobe as exigências da proposta. Essa etapa utilizou ferramentas que possibilitaram a utilização da tecnologia baseada em *blockchain* no intuito de gerar a estrutura necessária. Isso se deu na busca de um ambiente que possibilite aos projetistas e investidores uma interação com a aplicação parecida com a já existente nos sites de *crowdfunding* comum. As funcionalidades listadas como importantes foram desenvolvidas de forma que ficassem semelhantes ao modelo tradicional, mantendo de forma transparente aos usuários uma *blockchain* se comportando como *back-end* que interage com o *front-end* da aplicação;
- **Propor um modelo de arquitetura:** A forma como as entidades participantes da aplica-

ção trocam, alteram ou guardam os dados na rede *blockchain* deve ser definida para este trabalho. Levando isso em consideração, um modelo de arquitetura foi desenvolvido buscando organizar as funcionalidades presentes no ambiente, as interações entre as diferentes entidades e onde os dados ficariam alocados. Esse modelo ajudou no desenvolvimento da aplicação *web*;

- **Desenvolver uma aplicação:** Logo após o levantamento de requisitos, a montagem da infraestrutura e a definição de uma proposta de arquitetura, o desenvolvimento da aplicação foi iniciado. A infraestrutura precisará trocar mensagens com uma *blockchain* enviando os dados dos projetos para serem armazenados e depois consultados. O acesso aos projetos dentro da rede *blockchain* é dado às entidades via Internet, utilizando funcionalidades existentes na aplicação *web*. Funcionalidades como listar e exibir características dos projetos, além de obter interação com eles;
- **Realizar testes:** Nessa etapa foram realizados testes de funcionalidades utilizando uma rede *blockchain* de testes visando a implantação de um sistema com comportamento estável. A etapa de testes no desenvolvimento de um sistema é sempre de muita importância quando se almeja um software de qualidade. Em aplicações que utilizam *blockchain* a realização de testes se mostra ainda mais importante, pois dependendo de onde o erro está, a ação de realizar alterações no código se torna financeiramente onerosa;
- **Realizar uma análise de desempenho:** Nesta etapa foi realizado um estudo empírico com foco nas transações realizadas pela aplicação, analisando o seu desempenho. A cada transação realizada, alguns dados foram coletados: tempo que levou para validação do bloco na cadeia e custos gerados em sua execução. Assim compreendendo um pouco mais sobre como se comportam sistemas que utilizam *blockchain*. Essa tarefa buscou identificar pontos de gargalos na aplicação. Com os dados foi possível determinar a média, mediana, desvio padrão, valores máximos e mínimos de tempo e custos das transações;
- **Analisar os resultados obtidos:** Como última etapa, foram reunidas todas as informações e avaliados os resultados, sempre buscando saber se houve benefício no emprego da tecnologia *blockchain* como solução para o problema apontado neste trabalho. Também foram gerados gráficos e relatórios que ajudaram na visualização dos resultados e suas interpretações.

1.4 Contribuições

Diante das pesquisas feitas com uma boa bibliografia, juntamente com os conhecimentos adquiridos ao logo do desenvolvimento aplicando os conceitos vistos, é possível listar algumas contribuições desse trabalho como:

- Desenvolvimento de uma arquitetura mostrando as principais entidades em uma solução *web*, com base em *blockchain*, para ser usada como referência e ajudar na compreensão do uso da tecnologia em novas aplicações (Subseção 4.1);
- Definição de uma solução em *blockchain* para ajudar investidores *crowdfunding* a terem mais poderes em seus investimentos, além de serem capazes de fazer suas próprias auditorias em relação ao dinheiro gasto no desenvolvimento do projeto investido (Subseção 5.1);
- Uma aplicação *web* desenvolvida com o intuito de fazer demonstrações práticas da solução utilizando tecnologia *blockchain* para obter mais segurança e confiabilidade nos investimentos coletivos (Subseção 5.1.3);
- Mostrar e utilizar ferramentas capazes de analisar transações *blockchain*, com o detalhamento dos dados obtidos e ajudar em novas aplicações com a tecnologia (Subseção 5.1.4).

Como contribuições científicas é possível se destacar:

- Uma análise detalhada da aplicação consideração o tempo e os custos das transações realizadas dentro de uma aplicação *web* se comunicando com a rede *blockchain*, mostrando assim o desempenho da aplicação (Subseção 5.3);
- Um modelo analítico para cenários de utilização da aplicação (Subseção 5.5);
- Uma base de dados resultante de operações de chamadas de métodos da aplicação para utilização posterior em desempenho (Apêndice A).

1.5 Organização do Trabalho

O restante do documento está dividido nos seguintes capítulos: No Capítulo 2 é apresentada a descrição do domínio de *crowdfunding*, os conceitos relacionados a *blockchain* e contratos inteligentes levantados através da pesquisa bibliográfica. No Capítulo 3, é realizada uma revisão sistemática visando obter um retrato do estado da arte a respeito do uso da tecnologia *blockchain* e também alguns trabalhos relacionados são discutidos para melhorar o entendimento

do cenário trabalhado. No Capítulo 4, são apresentadas as análises iniciais do trabalho, os detalhes da arquitetura proposta e os requisitos para o desenvolvimento da solução. No Capítulo 5, são apresentadas as etapas realizadas para o desenvolvimento da solução criada, além das análises, discussão a respeito das experiências vivenciadas com a tecnologia *blockchain*, limitações e ameças a validade da proposta. Por fim, o Capítulo 6, apresenta as conclusões deste trabalho e perspectivas de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os conceitos utilizados na confecção deste trabalho, buscando um melhor detalhamento sobre cada tecnologia envolvida. A Seção 2.1 explica sobre o surgimento do *crowdfunding* e suas características. A Seção 2.2 detalha o surgimento do *blockchain* e sua aplicabilidade. A Seção 2.3 conceitua os contratos inteligentes além de comentar alguns exemplos dos mesmos. A Seção 2.4 apresenta uma ideia geral da rede *blockchain* escolhida para utilização deste trabalho. A Seção 2.5 mostra arquiteturas de sistemas que adotaram o uso de *blockchain*. A Seção 2.6 comenta a respeito de projetos em áreas diversificadas com uso de *blockchain*. Por fim, a Seção 2.7 analisa o processo de adoção da tecnologia *blockchain*.

2.1 *Crowdfunding*

Para Steffen (2015) o *crowdfunding*, ou financiamento coletivo, numa tradução livre adotada pelos brasileiros, tem sua origem no *crowdsourcing*, uma forma de desenvolver soluções e resolver problemas de forma coletiva usando os recursos da internet para aproximar pessoas que, fisicamente distantes, podem atuar em conjunto. O desenvolvimento do sistema GNU/Linux talvez seja um dos melhores exemplos de *crowdsourcing* aplicado ao desenvolvimento de soluções, mas este modelo pode ser aplicado a qualquer situação ou problema. Interessante recordar também que o programa *Search for ExtraTerrestrial Inteligence* (SETI), pesquisa por inteligência extraterrestre, numa tradução livre – lançou mão do *crowdsourcing* para o processamento de informações captadas, usando protetores de tela que, quando acionados nos computadores pessoais das pessoas, utilizavam o poder de processamento para os cálculos necessários.

O *crowdfunding*, portanto, é classificado por Potenza e Oliveira (2016) como mais um fenômeno financeiro que surge a partir dos anseios e da inovação dos próprios agentes econômicos. É uma forma de investimento disruptivo, no sentido de que quebra com as regras tradicionais de financiamento de empresas, e especialmente com o formalismo e tecnicismo associado às ofertas públicas de participações. E não é surpreendente que o seu nascimento encontre tanta resistência tanto por investidores institucionais quanto pelos reguladores (que são sempre bastante cautelosos com novas formas de acesso à poupança pública).

Ele também pode ser definido como uma forma de captação de recursos que utiliza a

força e a mobilização das massas (a "*crowd*"), baseado em campanhas intensas e direcionadas de marketing do produto em desenvolvimento pelo empreendedor (POTENZA; OLIVEIRA, 2016). As massas são alcançadas principalmente pela internet, fruto do que pode ser descrita como a maior transformação nos meios de comunicação na era moderna: a habilidade de comunicação instantânea de um empreendedor com milhões de potenciais investidores (os *crowdfunders*), e a consequente redução dos custos de entrada nos mercados de tecnologia (EPSTEIN, 2015).

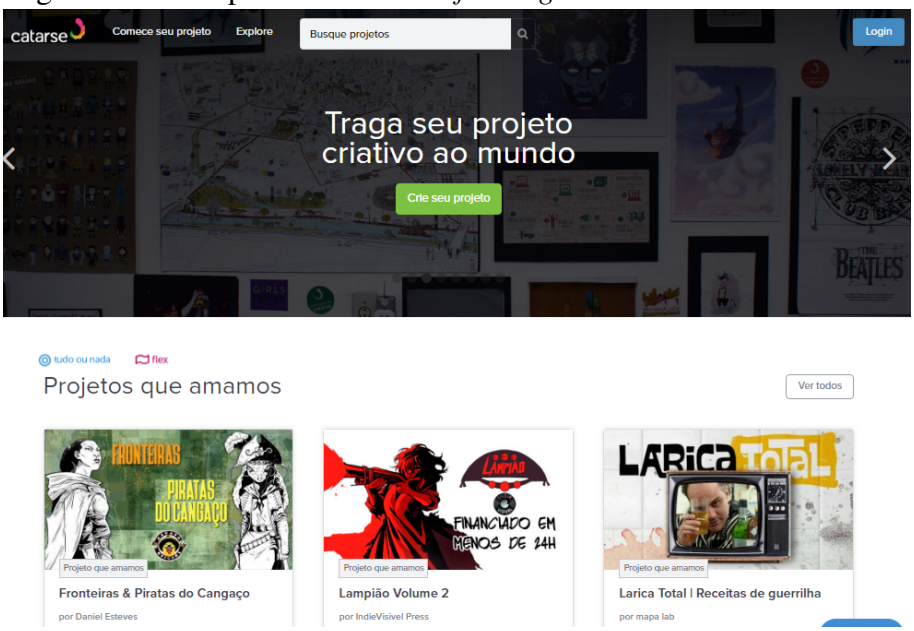
Um dos exemplos mais bem sucedidos e conhecidos do grande público foi a campanha presidencial do presidente dos Estados Unidos, Barack Obama, em 2008, quando o então candidato conseguiu arrecadar em torno de 272 milhões de dólares através de mais de 2 milhões de pessoas, a maioria contribuindo com pequenas quantias (HOWE, 2009). O feito só foi possível graças ao trabalho de sua equipe voltado para a internet e a criação de ferramentas para esse ambiente, criando uma relação com o público que ali se encontrava e gerando conteúdo específico para o mesmo (SBEGHEN, 2012).

A Figura 3 apresenta um exemplo de um site voltado ao *crowdfunding* que nasceu para incentivar a criatividade, a arte, o ativismo, a ciência e o empreendedorismo (CATARSE, 2022). Nesse site a prioridade são projetos que trazem novas perspectivas, projetos disruptivos, que geram diversidade e promovem debates saudáveis para a sociedade. Tida como a primeira plataforma de financiamento coletivo para projetos criativos no Brasil, o Catarse entrou no ar em 17 de janeiro de 2011. O site conta com quase um milhão de pessoas que já apoiaram em pelo menos um dos projetos disponibilizados. O manifesto de fundação diz que o site nasce de uma dor: ver gente brilhante com projetos engavetados.

O *crowdfunding* não é apenas uma reunião de pessoas para a promoção de ideias, mas sim a reunião de potenciais financiadores para a viabilização de projetos cujo objetivo é arrecadar dinheiro de diversas pessoas para a realização de um evento, ideia ou produto (COLLINS; PIERRAKIS, 2012). Os projetos necessitam ter um foco específico, devem ser realizados por pessoas com experiência e capacidade de construir o que propõem, obrigatoriamente precisam ter prazos de execução com início e fim, e também oferecer recompensas, sejam elas financeiras ou não, para as pessoas que doarem recursos e, acima de tudo, devem ser capazes de atrair a atenção e apoio na rede, de forma a transformar esta atenção em recursos doados (STEFFEN, 2014).

Juntar diversas pessoas no intuito de financiar um projeto é um fato que acontece já há algum tempo. Lawton e Marom (2010) citam a criação de uma loteria francesa e o pedido

Figura 3 – Exemplo de Site *Crowdfunding*.



Fonte: adaptado de (CATARSE, 2022)

de doações por parte do editor do jornal *New York world*, Joseph Pulitzer, para a construção da estátua da liberdade. Apesar da ideia ser anterior ao advento da internet, o princípio toma força ainda maior quando aliado à rede mundial interligada que permite uma interação ainda maior entre pessoas e ideias.

De acordo com Lima (2013), o modelo operacional do *crowdfunding* requer muitas pessoas dispostas a financiar algum projeto. De forma simplificada funciona da seguinte maneira: projetos são enviados para a aprovação das plataformas virtuais, isto é, sites que são como uma vitrine dos projetos existentes, uma vez aprovados, eles são publicados e possuem uma meta de fundos a serem arrecadados. Qualquer pessoa interessada em investir dinheiro no projeto em questão pode ajudar a realizá-lo.

Para os criadores de projetos, Felinto (2013) acredita que o *crowdfunding* abre todo um leque de novas possibilidades de financiamento das suas ideias. Para o público, oferece um sentido de participação antes impensável. O investidor sente-se como um co-criador, autêntico colaborador do processo produtivo, capaz mesmo de ajudar a determinar os destinos das obras/produtos que admira.

Este modelo de investimento permite que pequenos e médios empresários distribuam o risco em muitos investidores, devendo pequenas quantias a cada um (BUYSERE *et al.*, 2012). Com ele existe a possibilidade de divisão dos custos de produção entre diversas pessoas de lugares, costumes diferentes e totais desconhecidos.

2.2 *Blockchain*

O conceito da *blockchain* de acordo com Chicarino *et al.* (2017) começa a deixar claro que vai muito além da inovação tecnológica. Está causando um grande impacto, primeiramente mudando a forma de fazer negócios de modo centralizado para uma forma descentralizada, conferindo confiabilidade na realização de transações entre agentes distribuídos e mutuamente não confiáveis, sem a necessidade de uma entidade intermediária confiável por ambos.

Já Ferreira *et al.* (2017) comenta que *blockchain* consiste em uma cadeia cronologicamente ordenada de blocos protegidos pela resolução de *Proof-of-Work*. O encadeamento é feito adicionando o *hash* do bloco anterior ao bloco atual. O alinhamento dos blocos de forma cronológica faz com que uma transação não possa ser alterada com antecedência sem alterar seu bloco e todos os blocos a seguir (AITZHAN; SVETINOVIC, 2016).

O primeiro bloco da *blockchain*, o gênese, tem por identificador o resultado de uma função *hash* baseada no seu conteúdo. Cada bloco subsequente a ele possui um campo com o identificador do bloco anterior, cujo conteúdo é considerado no cálculo do seu identificador (ZHENG *et al.*, 2017). O mecanismo utilizado para validação de blocos, ou mineração no caso do Bitcoin, é denominado *Proof-of-Work* (PoW) (WOOD *et al.*, 2014). A validação de um bloco, portanto, depende da validação de blocos anteriores, constituindo assim o encadeamento de blocos que dá origem a *blockchain*.

Blockchain atualmente vem sendo bastante discutida tanto na indústria quanto na academia. E essa discussão está atingindo todos os setores da sociedade. Um exemplo desse efeito é a proposição de projetos baseados em blockchain em algumas cidades, como Dubai - Projeto de Registro Comercial Dubai Blockchain, Estocolmo - e-krona e Toronto - Fundo de Investimento Inovador (ETF) (XIE *et al.*, 2019).

Blockchain possui alguns recursos que a tornam uma tecnologia atraente para enfrentar diversos desafios (XIE *et al.*, 2019): descentralização, pseudonimato, transparência, democracia, segurança e imutabilidade. Essas características possibilitam que diversas áreas melhorem seus processos e tenham uma maior segurança na gestão dos dados. Áreas como finanças, saúde, educação e logística estão se apropriando da *blockchain* para o incremento de suas atividades e aplicações. Assim, *blockchain* abriu uma série de possibilidades para empresas nas quais o valor pode ser transferido diretamente entre os participantes da rede pela internet, de maneira fácil como pagar em dinheiro e conveniente como usar mensagens instantâneas sem intermediários centralizados (ASTE *et al.*, 2017).

Em geral, nossa sociedade é centralizada, com hierarquias institucionais para governar atividades de nossas comunidades socioeconômicas (ASTE *et al.*, 2017). Nesse contexto, a *blockchain* possibilita novos modelos de negócios, novos processos de trabalho e de produção nos quais o acesso e o compartilhamento tratam propriedade. E assim, a *blockchain* cria a oportunidade para a geração de um nível de confiança necessário entre partes desconhecidas e anônimas, permitindo a negociação sem intermediários (COUTINHO *et al.*, 2020).

A apresentação dos conceitos até então teve o intuito de entender a *blockchain*. Mesmo assim, buscando um melhor entendimento do seu potencial e uma análise de sua estrutura, as próximas seções detalharão a tecnologia com mais profundidade.

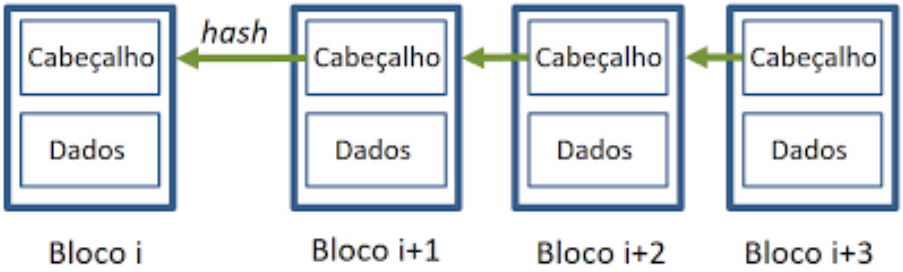
2.2.1 Surgimento e Definição de Blockchain

De acordo com Ulrich (2014) e Lucena e Henriques (2016), originalmente a *blockchain* foi idealizada por um programador anônimo sob o pseudônimo de Satoshi Nakamoto, em 2009, como uma forma de resolver o problema do "gasto duplo", pois nas transações *online* sempre era necessário um terceiro para intermediá-las, mas para sua *criptomoeda* virtual, o Bitcoin, esse problema foi resolvido removendo a necessidade do intermediário. Lucena e Henriques (2016) comentam que Nakamoto propôs que ao armazenar toda as transações em uma lista encadeada e de acesso livre para qualquer membro da rede, os dados se tornariam públicos e removeria a necessidade de um intermediário gerenciador para a rede e para as transações. Assim formou-se o conceito inicial da *blockchain*, originalmente o livro-razão não centralizado das transações Bitcoin.

Mesmo antes de Nakamoto, experimentos com cadeia de blocos criptograficamente protegidas foram registrados pela primeira vez no trabalho de Haber e Stornetta (1991), onde o objetivo era desenvolver um sistema que os *timestamps* de documentos não pudessem ser adulteradas. Porém, foi apenas em 2008 que uma pessoa ou entidade sob o pseudônimo de Satoshi Nakamoto publicou um artigo para introduzir o Bitcoin, uma *criptomoeda* baseada em uma moeda imutável e o razão público descentralizado que ficou conhecido como *blockchain* (NAUMOVA *et al.*, 2019). A Figura 4 ilustra a estrutura de blocos encadeados.

Os valores do *hash* são únicos e fraudes podem ser efetivamente prevenidas, uma vez que as mudanças em um bloco na cadeia mudariam imediatamente o respectivo valor do *hash* (NOFER *et al.*, 2017). De acordo com FOROUZAN Behrouz A.; MOSHARRAF (2013. E-book.) "[...] uma função de *hash* pega uma entrada de dados, m, e processa uma cadeia de

Figura 4 – Estrutura básica de uma *Blockchain*



Fonte: adaptado de (CONCEIÇÃO; PAULA, 2019).

tamanho fixo conhecida como *hash*", ou seja, essa função de mão única gera uma cadeia de tamanho fixo que torna improvável de retornar ao valor de entrada (*input*), por isso mão única (BOVÉRIO; SILVA, 2018).

Lucena e Henriques (2016) explicam que a *blockchain* utiliza a função *hash* com o intuito de impossibilitar modificações dos arquivos digitais armazenados dentro deles. Cada novo bloco utiliza a saída (*output*) da função do bloco anterior para gerar um novo bloco, interligando todos os blocos, por isso o nome *blockchain*. Dessa maneira qualquer modificação dentro de um bloco já adicionado à rede afetaria todos os blocos depois dele, sendo assim facilmente identificado por todos na rede.

O *timestamp* tem como finalidade dificultar e impossibilitar fraudes na *blockchain*. Naumova *et al.* (2019) explica que "o *timestamp* prova que os dados devem ter existido no momento para entrar no *hash*", ou seja, comprovando a existência na hora do registro na *blockchain*. Cada bloco contém um carimbo de data/hora (*timestamp*), o valor de *hash* que é computado usando um algoritmo de *hash* ou prova de trabalho conhecido (por exemplo, SHA-256, Ethash e Equihash) e o *hash* do bloco anterior chamado bloco pai, por fim um "*nonce*", que é um número aleatório para verificar o *hash* (NOFER *et al.*, 2017).

2.2.2 Estrutura da Blockchain

Dissociada da *criptomoeda*, a *blockchain* é apenas uma estrutura de dados, ou seja, é uma forma definida de como os dados são unidos e armazenados, muito similar ao banco de dados, porém descentralizada (LEWIS, 2018). Para Viana *et al.* (2020), essa estrutura descentralizada beneficia o sistema em relação à segurança, mas perde em rapidez de processamento, pois todos os nós da rede validam a mesma informação para garantir sua veracidade. A tecnologia *blockchain* pode ser aplicada a quaisquer valores de caráter digital, como por exemplo certificados, contratos, arquivos ou qualquer outro que se deseje.

2.2.2.1 Rede Peer-to-Peer

Numa perspectiva de alto nível, para Kamienski *et al.* (2005), uma rede *Peer-to-peer* (P2P) pode ser considerada uma rede *overlay*, uma vez que funciona como uma rede virtual, formada pela interconexão dos nós (*peers*), executando sobre a infraestrutura de uma rede física. A característica básica de uma rede P2P é que existe um grupo de nós com interesses comuns que estão conectados através do mesmo sistema de comunicação. Outras características dessa rede são: (i) os nós são conectados de forma aleatória, não há restrição sobre o número de nós que participam da rede; (ii) a conexão de um nó à rede se estabelece através de outro nó que já pertença à rede; (iii) os nós podem se unir e sair da rede a qualquer momento sem prévio conhecimento dos demais membros.

Não existe unanimidade na definição de uma rede P2P, assim a definição acaba sendo dependente do contexto em que a tecnologia é empregada (DETSCH, 2005). De forma geral, entretanto, estabelece-se que redes P2P são redes virtuais que funcionam na internet com o objetivo de compartilhar recursos entre os participantes, sendo que, por princípio, não há diferenciação entre os participantes (ROCHA *et al.*, 2004).

Uma *blockchain* por definição é composta por uma rede P2P, em que cada máquina participante atua como um nó (*peer*) na rede, ou seja, a *blockchain* é uma rede descentralizada com vários nós conectados (SHARPLES; DOMINGUE, 2016), em que os dados armazenados são replicados automaticamente ou com base no comportamento dos usuários na rede P2P (XU *et al.*, 2017). A natureza da topologia P2P na *blockchain* ajuda a compartilhar os recursos e reduzir os riscos de segurança (ALAMMARY *et al.*, 2019).

2.2.2.2 Criptografia

A segurança da informação segundo Sousa (2019) sempre foi indispensável à vida das pessoas, isso pode ser comprovado em atitudes como: realizar treinos fechados à imprensa antes de um grande jogo, não divulgar sua senha do banco para ninguém, ou até mesmo rasgar bilhetes confidenciais logo após sua leitura. Por tal motivo, um dos principais critérios para se avaliar a qualidade de um sistema, é sua segurança.

Quando se tem o interesse em assegurar a confiabilidade da informação, é imprescindível garantir a segurança desta em sistemas e serviços computacionais (BARCELOS; MARTINS, 2020). Neste cenário, surgem alguns fundamentos de segurança da informação

(OLIVEIRA, 2012):

- Disponibilidade: uma informação deve estar disponível para acesso no momento desejado;
- Integridade: o conteúdo da mensagem não deve ser alterado.
- Controle de acesso: o conteúdo da mensagem deve ser acessado somente por pessoas autorizadas;
- Autenticidade: a identidade de quem está enviando a mensagem deve ser garantida;
- Não-repudiação: deve-se prevenir que terceiros neguem o envio e/ou recebimento de uma mensagem;
- Privacidade: deve-se impedir que pessoas não autorizadas tenham acesso ao conteúdo da mensagem.

Existem dois métodos que são bem comuns ao se falar em criptografia que são os simétricos e assimétricos. A criptografia simétrica baseia-se em dois elementos principais: o algoritmo de cifragem e a chave criptográfica (BARCELOS; MARTINS, 2020). Esse modelo também é caracterizado pela utilização de apenas uma chave tanto para a encriptação da mensagem original, quanto para a decodificação da mensagem encriptada. O principal atributo desta metodologia é a garantia de privacidade, dado que apenas os detentores da chave conseguirão ter acesso à mensagem original (SOUSA, 2019).

De acordo com Romagnolo (2017) uma chave criptográfica é um valor secreto que modifica a saída em um algoritmo de encriptação. Funciona como a fechadura da porta da frente de uma casa, que possui uma série de pinos. Cada um desses pinos possui múltiplas posições possíveis. Quando alguém põe a chave na fechadura, cada um dos pinos é movido para uma posição específica. Se as posições ditadas pela chave são as que a fechadura precisa para ser aberta, ela abre, caso contrário, não.

Para Barcelos e Martins (2020) na criptografia assimétrica são utilizadas duas chaves, uma pública e outra privada, diferentes e complementares. A chave pública, como o próprio nome insinua, pode estar acessível a qualquer pessoa que deseje se comunicar de modo seguro, porém a chave privada deve ficar em posse somente de cada titular. A chave privada é responsável por decodificar uma mensagem criptografada para ele com a sua respectiva chave pública. Desta maneira, é garantida a confiabilidade da mensagem, desde que a chave privada esteja segura, posto que quem possuir acesso a esta chave terá acesso à mensagem (OLIVEIRA, 2012). A vantagem deste método é a segurança, já que não é necessário e nem prudente compartilhar a chave privada. Por outro lado, a desvantagem é que o tempo de processamento de mensagens

neste tipo criptografia é maior que na criptografia simétrica (OLIVEIRA, 2012).

Outra aplicação considerada importante por Sousa (2019) da criptografia assimétrica é a geração de assinaturas digitais. Estas são baseadas em sua chave privada e podem ser verificadas por qualquer um que possua a respectiva chave pública.

A criptografia apoia fortemente a *blockchain* para cumprir os requisitos de segurança do sistema e das aplicações (ABREU, 2020). Dentre os recursos mais utilizados, destacam-se as funções *hash* e as assinaturas digitais (GREVE *et al.*, 2018). A assinatura digital no entendimento de Barcelos e Martins (2020), consiste em um processo de inversão do sistema de criptografia assimétrica. O autor assina uma mensagem usando sua chave privada para cifrá-la e ela pode ser decifrada utilizando a chave pública do autor, confirmando sua identidade e reconhecendo que a mensagem não foi adulterada, uma vez que utiliza funções *hash* no processo. Este método assegura a autenticidade, integridade e não-repudiação da mensagem, entretanto, não assegura sua confidencialidade, pois é decifrada utilizando a chave pública do emissor (OLIVEIRA, 2012).

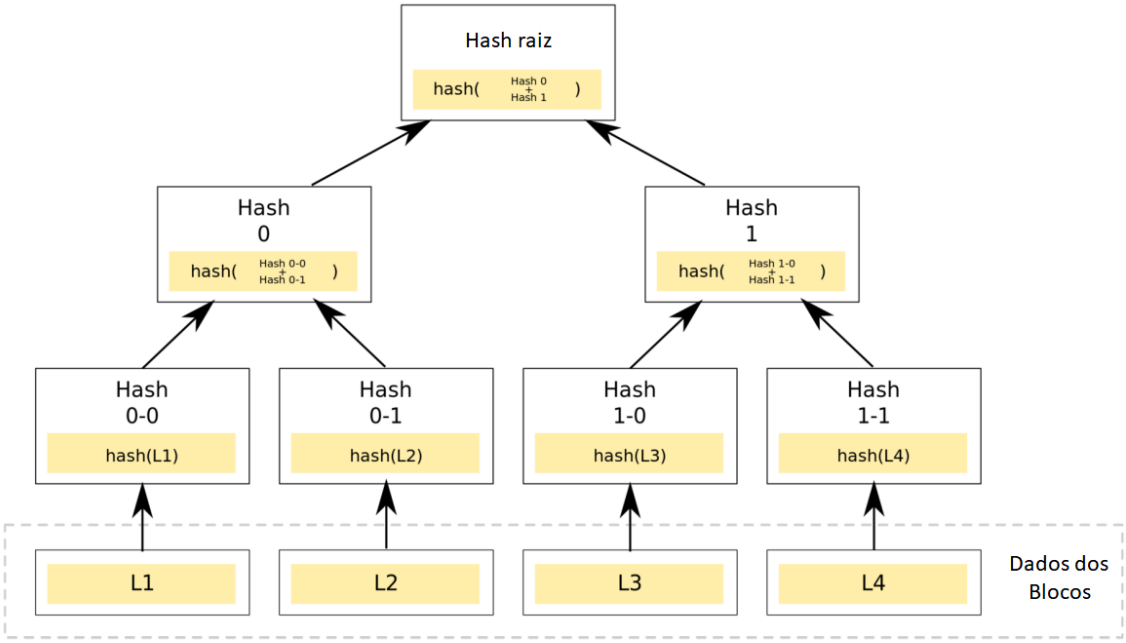
O tipo de criptografia mais empregado de acordo com Sousa (2019), é a função *hash*. Esta técnica encripta uma mensagem de uma maneira tal, que esta não pode retornar ao seu formato original por intermédio de uma função inversa, pelo fato da primeira função ser capaz de gerar um mesmo resultado para diferentes mensagens de entrada. Apesar da mensagem não poder retornar ao seu estado original, a verificação do resultado gerado para uma dada mensagem, é facilmente obtido ao se aplicar a tal mensagem na função *hash*. Já segundo Ishmaev (2017), uma função *hash* é essencialmente uma função matemática que dada uma entrada de dados de qualquer tamanho, produz uma saída de tamanho limitado que pode ser computável com eficiência (em um período de tempo razoável).

2.2.2.3 Árvore de Merkle

Uma árvore de Merkle para Matsumine (2019) é uma árvore binária formada inteiramente por valores de saída de um *hash* criptográfico, tal que cada folha da árvore é rotulada com o *hash* de um bloco de dados correspondente e cada nó que não seja uma folha é rotulado com o *hash* de seus nós filhos. É possível perceber que qualquer alteração em algum dos blocos de dados, produz um valor diferente do valor do *hash* esperado de um bloco íntegro e, devido a sucessão de cálculos de *hash* que se seguem a partir desse primeiro *hash*, todos os níveis superiores seriam afetados e produziriam um valor diferente, consequentemente uma raiz

diferente e assim uma árvore de Merkle diferente.

Figura 5 – Exemplo de uma árvore de Merkle formada a partir dos blocos de dados L1, L2, L3 e L4



Fonte: adaptado de (MATSUMINE, 2019).

Considerando a Figura 5 que Matsumine (2019) utiliza como exemplo, suponha que se deseja enviar o bloco L4 para o respectivo par da comunicação. Para isso, a árvore de Merkle é construída utilizando os blocos L1, L2, L3 e L4 e então é produzida uma prova para o bloco L4. Esta prova contêm o bloco L4, o *Hash* 1-0 e o *Hash* 0, uma vez que o caminho de L4 até a raiz passa pelo *Hash* 1-1, *Hash* 1 e finalmente chega-se ao *Hash* raiz. O par da comunicação que receberá o bloco L4, tem consigo uma cópia íntegra do *Hash* raiz (calculada a partir de L1 até L4 íntegros e obtida de um terceiro confiável). Após o par receber o bloco L4 junto a sua respectiva prova, o verificador calcula o *hash* de L4 e utilizando *Hash* 1-0 da prova, calcula *Hash* 1 e em posse desse *hash*, utiliza *Hash* 0 da prova para obter *Hash* raiz, o qual será comparado com *Hash* raiz e caso sejam iguais, o bloco L4 é considerado válido, caso contrário ele é descartado.

2.2.3 Consenso

Em sistemas de computação distribuídos, um componente, como um servidor, pode aparecer tanto como falho quanto funcional a um sistema de detecção de falhas (BARCELOS; MARTINS, 2020). Estes componentes podem apresentar diferentes sintomas a diferentes observadores, isto é conhecido como “falha bizantina”. É difícil para os outros componentes

declararem que o servidor falhou e o desligarem da rede, por que eles primeiramente precisam obter consenso a respeito de qual componente falhou, sendo conhecido como “falha bizantina” (DRISCOLL *et al.*, 2004).

Em *blockchain* as transações do livro de registros são verificadas por vários clientes ou “validadores” na rede ponto a ponto da *criptomoeda*, usando um dos muitos algoritmos de consenso que existem para resolver o problema de confiabilidade em uma rede envolvendo vários nós não confiáveis (BACH *et al.*, 2018). Nesta rede não há nó central que garanta que os registros das transações em nós distribuídos sejam todos iguais. Os nós precisam não confiar em outros. Assim, algumas abordagens são necessárias para garantir que os registros em nós diferentes sejam consistentes (ZHENG *et al.*, 2018).

Os algoritmos de consenso mais amplamente usados são o algoritmo PoW e o algoritmo *Proof-of-Stake* (PoS), traduzidos como Prova de Trabalho e Prova de Participação respectivamente. No entanto, também existem outros algoritmos de consenso que utilizam implementações alternativas de PoW e PoS, bem como outras implementações híbridas e algumas estratégias de consenso totalmente novas (BACH *et al.*, 2018).

2.2.3.1 Problema do Gasto Duplo

Sendo um sistema descentralizado, a *blockchain* não precisa de uma autoridade externa. Ao invés disto, ele garante a confiabilidade e a consistência dos dados e das transações através de um mecanismo de consenso (LI *et al.*, 2020). Isso é feito de forma a evitar o problema do gasto duplo. O gasto duplo é um dos maiores problemas em produtos digitais, que seria um usuário gastar/utilizar/compartilhar duas vezes o mesmo produto. Por exemplo, se existe um arquivo mp3 ou um e-book em um computador, pode-se copiar esse arquivo milhares de vezes livremente e envia-lo para milhares de pessoas diferentes. Para uma moeda digital, a possibilidade de cópia ilimitada significaria uma rápida morte hiperinflacionária (JOSELLI, 2018).

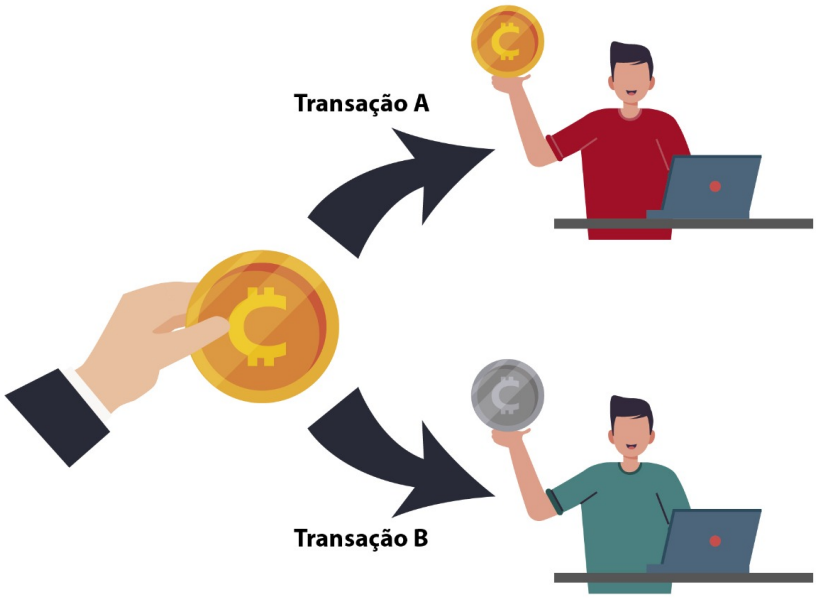
O Bitcoin foi o primeiro sistema de pagamentos eletrônico sem intermediação que se tem notícia (NAKAMOTO, 2008). Para Burgos e Alchieri (2021) problema do gasto duplo diz respeito à incapacidade de se garantir a transferência e a propriedade exclusiva de um artefato digital simultaneamente. O papel-moeda é uma representação física, ou *token* físico, de um determinado valor em uma determinada moeda. Quando é utilizado uma cédula para pagar por algum produto, ou serviço, o valor que ela representa é transferido juntamente com sua

posse para o vendedor. Para gastar o valor representado pela mesma cédula mais de uma vez, seria preciso copiá-la, o que é ilegal e passível de detecção devido às tecnologias utilizadas na produção da numeração física. Já a cópia de um artefato digital é indistinguível de seu original, permitindo assim, a circulação indetectável de um número potencialmente ilimitado de cópias do mesmo artefato.

O problema do gasto duplo é comentado por Lucas e Andrea (2019) onde é dito que ele também impossibilitaria a manutenção da moeda, pois o que garante valor ao dinheiro é sua escassez, e então, se todos pudessem multiplicar o dinheiro a seu bel prazer, o sistema monetário seria impraticável. Com isso não haveria mais necessidade em se discutir o valor e consequentemente a necessidade do dinheiro. As *criptomoedas*, desta forma, não teriam mais valor. Também segundo Lucas e Andrea (2019) as *criptomoedas* podem ser negociadas entre os usuários com a utilização da chave pública como espécie de "conta" em que serão retiradas ou recebidas as moedas, mas, podem também, e geralmente são, negociadas em corretoras de câmbio próprias: as *Exchanges*, ambiente no qual podem ser negociadas várias criptomoedas ao preço da moeda do país em que funcionam e são regulamentadas.

A Figura 6 representa o problema do gasto duplo, onde, por exemplo, o usuário malicioso faz dois pagamentos a pessoas diferentes utilizando um mesmo Bitcoin. Com isso, apenas uma dessas pessoas irá ter realmente sua transação confirmada, a outra terá a transação negada por saldo insuficiente.

Figura 6 – Gasto Duplo.



Fonte: o autor

2.2.3.2 Algoritmo Proof-of-Work

É um mecanismo de consenso em que o nó busca uma solução para um desafio matemático a fim de poder criar um novo bloco (ALIAGA; HENRIQUES, 2017). No caso específico do Bitcoin, a ideia consiste em encontrar o valor do *hash* do cabeçalho do bloco de tal forma a seguir os parâmetros definidos pelo grau de dificuldade.

Segundo Rolim e Freitas (2019) algoritmos de consenso PoW, ou Prova de Trabalho baseiam-se no fato de que um nó malicioso tem que executar muito trabalho do ponto de vista computacional para atacar a rede, e por isso, é menos provável que ele vá querer atacar. O trabalho realizado geralmente envolve fazer alguns cálculos até que uma solução seja encontrada, um processo que é comumente conhecido como mineração. No caso da *blockchain* do Bitcoin, a mineração consiste em encontrar um número aleatório, chamado de número *nonce* que fará o *hash* SHA256, um *hash* seguro de 256 bits, do cabeçalho do bloco ter no início certo número de zeros. Portanto, os mineradores têm que demonstrar que eles realizaram certa quantidade de trabalho para resolver o problema. Uma vez resolvido o problema, é realmente fácil para outros nós verificarem se a resposta obtida é válida.

Quando a taxa de mineração do PoW aproxima-se de zero, há cada vez menos incentivo para blocos serem minerados (CORREA, 2018). Sob este cenário, o consumo de energia na rede pode cair para níveis muito baixos, já que os mineradores desinteressados param de extrair a prova de trabalho dos blocos (PRIMECOIN, 2013).

2.2.3.3 Algoritmo Proof-of-Stake

Segundo Aliaga *et al.* (2019) o *Proof-of-Stake* é um mecanismo de consenso em que o sistema faz uma escolha do nó que poderá criar um novo bloco. A forma usual da escolha é um sorteio cuja chance de ganhar é proporcional à quantidade de moedas que o nó já possui. É como se um nó rico em moedas (ou em qualquer outro parâmetro) tivesse mais bilhetes da loteria para concorrer com mais chances de ganhar.

PoS ou Prova de Participação é um mecanismo de consenso que requer menos recursos computacionais e potência do que PoW (BITFURY, 2015), por isso consome menos energia. Em uma *blockchain* baseada em PoS, assume-se que as entidades com mais participação na rede são os menos interessados em atacá-la. Assim, os nós precisam provar periodicamente que eles possuem certa quantidade de participação na rede (por exemplo, moeda ou quantidade

de dados coletados a partir de sensores). Pode-se comparar o PoS a uma loteria, onde é realizado um sorteio e escolhido um nodo que irá dizer se o bloco que está sendo enviado pela rede é válido ou não. Por consequência, o nodo que tiver mais participação recebe mais "fichas" neste sorteio, e tem mais chances de validar o bloco. O nodo que realiza o sorteio pode ou não ser pré-definido. A Figura 7 mostra um comparativo entre as duas abordagens *Proof-of-Work* e *Proof-of-Stake* e relata um pouco sobre suas principais diferenças.

Figura 7 – Comparação *Proof of Work* vs *Proof of Stake*

Fonte: adaptado de (CORREA, 2018).

As principais variações do PoS seguem a estrutura do consenso do PoW, utilizando comunicação feita por troca de mensagens (ABREU, 2020). Existem as regras de validação de bloqueio, as regras de cadeia mais longa e finalidade probabilística. Ao contrário do PoW, um minerador do PoS pode tentar resolver o quebra-cabeça do *hash* apenas uma vez por ciclo de tentativas. Com isso, a dificuldade do quebra-cabeça diminui com o valor da participação do validador. O número de tentativas para resolver o problema do quebra-cabeça do *hash* pode ser significativamente reduzido se o valor da participação do minerador for alto. Portanto, o PoS evita a competição de força bruta que ocorreria se PoW fosse usado. Dessa forma é alcançando uma significativa redução do uso de energia. Os primeiros sistemas de blockchain baseados no

PoS foram Peercoin e Nxt (XIAO *et al.*, 2020).

2.2.4 Tipos de Blockchain e Plataformas

Os tipos de *blockchains* são classificados basicamente de acordo com a forma de acesso e proteção das transações armazenadas (MENDONÇA *et al.*, 2021). Os tipos encontrados são as públicas, privadas e de consórcio. As especificações de protocolo de consenso, proteção de acesso às informações e controle da forma de distribuição diferenciam os tipos de *blockchain*.

Em se tratando do ponto de vista arquitetural, segundo Moreira (2019), vale a pena observar que existem diferentes tipos de *blockchains* que diferem em termos de permissões de leitura ou gravação. *Blockchains* públicas (como a *blockchain* Bitcoin) são *blockchains* que podem ser lidas e potencialmente graváveis por todos. Já as *blockchains* privadas são aquelas que podem ser escritas apenas por membros da organização. As permissões de leitura podem ser públicas ou restritas a organização. Em *blockchains* de consórcio, um conjunto de nós selecionados pertencentes a diferentes instituições controla a validação, e a *blockchain* é usada para compartilhar informações entre as instituições participantes.

Em uma *blockchain* privada as respostas são mais rápidas e seguras, porém o controle é exercido por um proprietário específico e os nós precisam de permissão para ingressarem na rede (MENDONÇA *et al.*, 2021). Na *blockchain* pública, por sua vez, a rede é totalmente descentralizada e pode conter vários nós e qualquer nó pode ingressar na rede. Porém, apenas nós sincronizados são utilizados para consenso. Uma *blockchain* de consórcio é composta por nós de organizações específicas que se unem e controlam quem pode ter acesso à rede. A rede resultante do consórcio é parcialmente descentralizada (ROUHANI; DETERS, 2017) (WANG *et al.*, 2018).

Rifi *et al.* (2017) também relataram a existência de três tipos de *blockchain*:

- A *blockchain* pública sem permissão: é uma rede aberta que permite a participação de qualquer pessoa (exemplos incluem Bitcoin e Ethereum). Com esse tipo de *blockchain*, todos os usuários podem ler, escrever e verificar transações. Esse tipo de *blockchain* pode substituir o papel de um terceiro confiável. A confiança é construída entre pares na rede, porque todos eles têm que respeitar o estabelecido mecanismo de consenso. Os mais populares mecanismos de consenso são o PoW e o PoS;
- A *blockchain* pública permissionada: é uma rede fechada, em que apenas nós verificados e confiáveis podem participar (exemplos são Ripple, Multichain, Eris e Hyperledger Fabric).

Esse tipo também é chamado de "*blockchain* híbrida", porque todos os participantes podem visualizar os dados, mas apenas usuários autorizados podem validar as transações. Os usuários são autorizados através de um consenso de rede depois de fornecer a prova necessária de elegibilidade;

– A *blockchain* privada permissionada: é uma rede fechada que permite apenas usuários autorizados a ler, enviar e validar as transações (exemplos incluem Hyperledger Fabric e Corda). As transações são verificadas ou o consenso da *blockchain* é determinado dentro de uma organização. Geralmente é utilizado um protocolo de *Byzantine Fault Tolerance* (BFT), o qual requer uma certa porcentagem de nós previamente verificados para confirmar as transações.

Para iniciar o desenvolvimento de um projeto com *blockchain* em qualquer domínio da sociedade, outra etapa importante é selecionar a plataforma mais adequada (ABREU, 2020). As plataformas Bitcoin, Ethereum e Hyperledger Fabric são consideradas as mais conhecidas e utilizadas (XU *et al.*, 2019).

Ressalta-se que, na rede *blockchain* pública, a segurança é garantida a partir de algoritmos de consenso, em que os próprios participantes são responsáveis pela segurança, pela escrita e pela validação dos dados presentes (ARAUJO *et al.*, 2021). As transações podem ser rastreadas nas redes públicas através de chaves criptográficas públicas anônimas geradas por cada usuário, conhecida por endereço. Enquanto nas redes privadas a segurança é garantida pela aprovação prévia de participantes selecionados e a identidade desses participantes é conhecida.

A título de exemplo Araujo *et al.* (2021) comenta que, no Brasil, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) criou um programa piloto denominado "BNDESToken" que utiliza a rede Ethereum e que tem por objetivo rastrear a aplicação de recursos públicos em operações de crédito com entes públicos ou operações com recursos não reembolsáveis. O programa funciona da seguinte forma: cada unidade do BNDESToken atua como uma representação digital da moeda brasileira, no valor de um real, liberado pelo BNDES às pessoas jurídicas beneficiadas. É possível que essas pessoas jurídicas realizem aquisições de produtos e serviços e efetivem o pagamento de fornecedores a partir do BNDESToken, e estes poderão, por sua vez, resgatar posteriormente o token convertido em real junto ao BNDES. Importa ressaltar que, para que o fornecedor da entidade beneficiada receba o BNDESToken, é necessário que seja feito previamente um cadastro na plataforma utilizada, com o número do Cadastro Nacional de Pessoas Jurídicas (CNPJ). Desta forma, o referido banco também pode

rastrear pelo CNPJ e pelo BNDESToken as empresas que recebem algum tipo de aporte de capital através das diversas linhas de crédito da instituição, podendo ser verificado, consequentemente, se a entidade realmente está cumprindo os termos do contrato firmado no momento do dispêndio do capital.

Olhando também para o cenário internacional, a tecnologia *blockchain* já é utilizada em muitos dos registros de dados dos estados (ARAUJO *et al.*, 2021). A Estônia, por exemplo, implantou o sistema denominado "eEstonia", que conecta os sistemas nacionais de justiça, saúde, segurança, legislativo e comercial, armazenando-os de forma segura em relação à corrupção e uso indevido. No processo legislativo, o país utiliza o sistema e-Law, formalmente conhecido por *Eletronic Coordination System for Draft Legislation* (Sistema de Coordenação Eletrônica para Projetos de Legislação) que, através da rede blockchain, possibilita ao público o acesso a informações referentes a projetos de lei enviados desde 2003, podendo ser consultado pela sociedade o autor da legislação, bem como o status atual e alterações feitas ao longo do processo parlamentar.

O Hyperledger Fabric é um dos projetos de *blockchain* do Hyperledger (HYPERLEDGER, 2020). Como outras tecnologias *blockchain*, possui um livro-razão, usa contratos inteligentes e é um sistema pelo qual os participantes gerenciam suas transações. Onde o Hyperledger Fabric se diferencia de alguns outros sistemas *blockchain* é que ele é privado e autorizado. Em vez de um sistema aberto sem permissão que permite que identidades desconhecidas participem da rede (exigindo protocolos como "prova de trabalho" para validar transações e proteger a rede), os membros de uma rede Hyperledger Fabric se inscrevem por meio de um provedor de serviços de associação *Membership Service Provider* (MSP) confiável.

O Hyperledger Fabric é uma plataforma de tecnologia de código aberto modular e configurável, projetada para o ambiente empresarial, com o foco na construção de aplicações em cadeia de blocos privados e permissionados (BURLE, 2019). A plataforma opera baseada na premissa de contratos inteligentes (*chaincode*), em uma rede *blockchain* privada. A escolha dessa plataforma se deve a sua natureza permissiva, à programação em linguagens de uso geral e ao processamento em tempo real (HYPERLEDGER, 2020).

Bem parecido com o Hyperledger Fabric, existe a plataforma Corda que possui um livro de registros compartilhados apenas entre grupos definidos de participantes da rede (ABREU, 2020). Isso visa melhorar a privacidade e escalabilidade, reduzindo a replicação de dados na rede. Também existe a plataforma Ripple, que é considerada um sistema de liquidação e câmbio

em tempo real entre instituições financeiras. A Ripple usa um livro de registros comum que é gerenciado por uma rede de servidores de validação independente que comparam constantemente registros de transações, no qual esses servidores de validação podem pertencer a indivíduos ou bancos.

Várias técnicas foram propostas para preservar a privacidade na *blockchain* (ABREU, 2020). Por exemplo, a plataforma Zcash criptografa informações de transações de pagamento e usa um método criptográfico para permitir que qualquer nó verifique a validade das transações criptografadas, permitindo que a rede *blockchain* tenha um livro de registros que possibilite pagamentos privados sem a divulgação das partes ou valores envolvidos. A plataforma Monero também dá ênfase a privacidade, em que usa outras ferramentas criptográficas para proteger endereços de envio e recebimento de valores das transações (XU *et al.*, 2019). Existem várias outras plataformas para desenvolvimento com *blockchain*, em que grande parte tem propósitos e definições semelhantes aos apresentados, sendo necessário uma análise da infraestrutura e detalhes de implementação para escolher a plataforma mais adequada para determinado projeto.

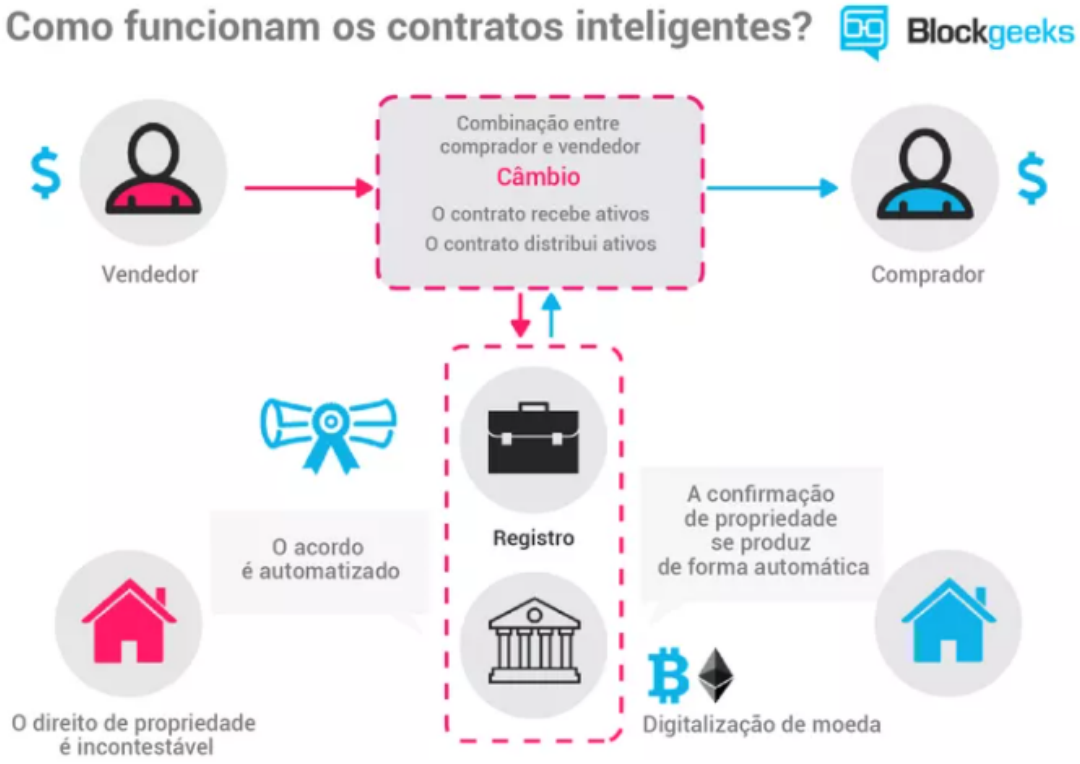
2.3 Contratos Inteligentes

O conceito de contrato inteligente foi introduzido por Szabo (1994), definido como um protocolo de transação computadorizado que executa os termos de um contrato. Szabo sugeriu traduzir cláusulas contratuais (e.g., garantias e títulos) em código e incorporá-las em propriedades (*hardware* ou *software*) que possam se autoaplicar, de modo a minimizar a necessidade de intermediários confiáveis entre as partes envolvidas na transação, e a ocorrência de exceções maliciosas ou acidentais. Como se pode verificar, os ativos e os termos do contrato são codificados e colocados no bloco de uma rede *blockchain* (CARDOSO, 2018). Este contrato é distribuído e copiado várias vezes entre os nós da plataforma. Após o desencadeamento do processo, o contrato é executado de acordo com os termos nele contidos. O programa verifica a implementação dos compromissos automaticamente (CARDOSO, 2018). A Figura 8 apresenta o funcionamento de um contrato inteligente dentro da rede *blockchain*.

Ainda segundo Cardoso (2018) os contratos inteligentes podem ter diversas utilidades:

- Funcionar como contas “multi-assinaturas”, de modo que os fundos são gastos apenas quando uma porcentagem exigida de pessoas concordam;
- Gerenciar acordos entre usuários, por exemplo, alguém compra um artefato, seja digital ou

Figura 8 – Como funcionam os contratos inteligentes.



Fonte: adaptado de (CARDOSO, 2018).

físico, diretamente de outro usuário;

– Fornecer utilidade para outros contratos (semelhante ao funcionamento de uma biblioteca de software);
– Armazenar informações sobre um aplicativo, como informações de registro de domínio ou registros de associação.

Um contrato inteligente (*Smart Contract*) se assemelha a um contrato legal tradicional, regulamentando a interação entre partes interessadas no objeto comum do contrato (MASCARENHAS *et al.*, 2018). Entretanto, o conceito de contrato inteligente define que as cláusulas de um contrato são codificadas e podem ser incorporadas a um *hardware* ou *software* com auto-execução (CHRISTIDIS; DEVETSIKIOTIS, 2016). Assim, sistemas de contratos inteligentes podem mover recursos digitais de acordo com regras e comandos pré-estabelecidos na sua criação. A partir desse conceito básico, contratos inteligentes podem ser usados em uma grande variedade de aplicações, tais como liquidação de transações e testamentos inteligentes criptografados (BUTERIN *et al.*, 2014).

A Figura 9 exibe um exemplo de contrato inteligente simples “Caixa de Mensagem” contendo somente duas funções, uma construtora que recebe a mensagem inicial - Inbox() e

outra que atualiza a mensagem com a nova mensagem enviada - setMessage().

Figura 9 – Contrato Caixa de Mensagem.

```
1   pragma solidity ^0.4.17;
2
3   contract Inbox {
4       string public message;
5
6       function Inbox(string initialMessage) public {
7           messsage = initialMessage;
8       }
9
10      function setMessage(string newMessage) public {
11          message = newMessage;
12      }
13  }
```

Fonte: o autor.

Segundo Braga *et al.* (2017), *blockchain* passou por uma grande evolução com o uso de contratos inteligentes. Em aplicações baseadas em *blockchain*, contratos inteligentes são *scripts* inseridos nas transações que executam ações baseadas nas regras do contrato. O programa do contrato inteligente é executado por todos os nós da rede do *blockchain*, sendo sua execução correta e consistente garantida pelo mecanismo de consenso distribuído (BRAGA *et al.*, 2017). Em aplicações de *criptomoedas* construídas em contratos inteligentes, primeiro as entradas das transações são verificadas pelas assinaturas digitais. Em seguida, verifica-se se o saldo dos endereços de saída coincide com os de entrada. Por fim, aplica-se a mudança de estado, ou seja, os recursos são efetivamente transferidos. Em aplicações de *criptomoedas*, tal como Ethereum, usuários podem criar transações de acionamento (*call*) e criação (*create*) de contratos inteligentes (WOOD *et al.*, 2014).

Um contrato inteligente é uma aplicação autônoma com entradas e saídas pré-definidas que podem ser executadas por um minerador de maneira determinística (ABREU, 2020). Qualquer usuário pode invocar um contrato inteligente, cujo resultado é registrado como uma transação no livro de registro distribuído (WOOD, 2019).

Os contratos inteligentes funcionam como *scripts* armazenados (ABREU, 2020). Como residem na cadeia, eles possuem um endereço exclusivo. Pode-se acionar um contrato

inteligente endereçando uma transação para ele, onde em seguida, ele executa de forma independente da forma que foi escrito, em qualquer nó da rede, de acordo com os dados que foram incluídos no acionamento da transação (CHRISTIDIS; DEVETSIKIOTIS, 2016).

Contratos inteligentes são criados sobre uma plataforma de *criptomoeda* (e.g. *Ethereum*) (COUTINHO *et al.*, 2020). Uma *criptomoeda* é um sistema descentralizado para interagir com dinheiro virtual em um livro compartilhado de forma global. Os usuários transferem dinheiro e interagem com contratos por meio da publicação de dados assinados, denominados de transações da rede de *criptomoedas*. A rede consiste em nós chamados mineradores que propagam informações, armazenam dados e atualizam os dados aplicando transações.

2.4 Ethereum

A *blockchain* da rede Ethereum, fundada por Vitalik Buterin em 2014. É uma *blockchain* de propósito geral, o que significa que é programável para realizar as mais diversas tarefas. Diferentemente da *blockchain* do Bitcoin, cujo único propósito é movimentar sua *criptomoeda*, a moeda da Ethereum, chamada de Ether (ETH), é utilizada como dinheiro para pagar a execução de código na sua *blockchain* (BEGINNERS, 2021).

Ethereum pode ser vista como uma máquina de estados baseada em transações (WOOD *et al.*, 2014). A partir de um estado inicial, a cada transação, o estado se modifica até se transformar em estado final. Estados podem incluir informações como balanço de contas, reputação, arranjos confiáveis, ou qualquer informação que possa ser representada por um computador (WOOD *et al.*, 2014).

Na rede da Ethereum, os endereços de carteira pertencentes a usuários podem ser associados a nós de uma rede, onde os usuários trocam informações através desses nós (MASCARENHAS *et al.*, 2018). A comunicação é feita com o objetivo de transferir informações entre carteiras, sejam valores, ou parâmetros de um contrato (WOOD *et al.*, 2014). Essas informações são inseridas dentro de transações, que podem ser representadas por arestas interconectando os nós da rede Ethereum envolvidos em cada transação. Usuários da plataforma Ethereum podem ser classificados como mineradores, usuários ou pertencer as duas categorias. O usuário comum apenas realiza transações, enquanto o minerador valida os blocos dentro da rede.

2.4.1 Conceitos Elementares

Na rede Ethereum é muito utilizado o termo “gas”, uma unidade de medida do poder computacional, e o “ether”, utilizado para a medição e pagamento pelo custo computacional no Ethereum (COUTINHO *et al.*, 2020). O ether é o combustível da Ethereum cuja finalidade é pagar pelo custo da computação realizada.

Por definição, em seu *white paper*, a Ethereum é uma maquina virtual descentralizada capaz de executar os *bytecodes* dos programas escritos em Solidity após compilação (ASSIS, 2021). Todo contrato possui uma capacidade de armazenamento e funções externas que podem ser invocadas por usuários ou contratos. Do mesmo modo, usuários e contratos podem possuir a *criptomoeda* chamada ether ou ETH, assim como são capazes de receber/enviar ether para/de outros usuários ou contratos. Usuários podem enviar transações para rede da Ethereum com três objetivos diferentes: (i) Criar um novo contrato; (ii) Invocar funções de um contrato; (iii) Transferir ether para contratos ou outros usuários (alterar balanço do contrato). A Figura 10 mostra algumas das unidades utilizadas na Ethereum.

Figura 10 – Unidades da Ethereum.

Unidade	Contexto/Conceito
GAS	Uma taxa cobrada em cada transação na blockchain da Ethereum.
WEI	Um wei está para o ether como um satoshi está para o bitcoin – ambas as unidades são a menor unidade a partir da qual um usuário pode fazer uma transação.
ETHER	Cada ETH equivale a 1.000.000.000.000.000.000 (um quintilhão) de Weis.
GWEI	É a unidade de ether mais comumente usada porque os preços do "gas" são facilmente especificados em gwei. Por exemplo, em vez de dizer que o gas custa 0,000000001 ether, pode-se afirmar que custa 1 gwei.

Fonte: o autor.

2.4.1.1 Gas e Ether

Gas é a taxa que um usuário paga para processar uma transação na *blockchain* Ethereum. Os preços do gas são contabilizados em “gwei”, que é uma denominação da moeda

nativa do Ethereum, ether. 1 gwei, também conhecido como nanoether, é igual a 0,000000001 ether (PEASTER, 2020). Quando o usuário paga gas para enviar uma transação, está pagando pela energia computacional necessária para alimentar a validação dessa transação na Ethereum. Como a rede Ethereum 1.0 é um sistema de prova de trabalho, essa computação atualmente é cortesia de "mineradores", que usam hardware especial para competir por pedidos e processamento de blocos Ethereum cheios de transações. Em troca de seu serviço, os mineradores podem ganhar recompensas de bloco ether e taxas de transação por meio de pagamentos de gas.

Um componente chave do sistema de cobrança de gas na rede Ethereum é o limite de gas (PEASTER, 2020). No contexto das transações, o limite de gas é a quantidade máxima de unidades de gas que o usuário está disposto a gastar em uma transação. Esse teto é usado para garantir que as transações sejam executadas e, como nem sempre será pago o valor máximo, qualquer ether não utilizado é devolvido à sua carteira.

Para Albert *et al.* (2020) existem três justificativas para medição de gas no ambiente da Ethereum: (i) pagar pelo gas no momento de propor a transação evita que o emissor desperdice o poder computacional dos mineradores por exigir que realizem trabalho intensivo sem valor; (ii) taxas de gas desincentivam os usuários a consumir muito do armazenamento replicado, que é um recurso valioso em um sistema de consenso baseado em *blockchain*; e (iii) limita o número de cálculos que uma transação precisa para ser executada, quanto maior o tempo para executar a transação maior o valor a ser pago em gas, portanto, evita ataques *Denial of Service* (DoS) baseados em execuções sem término.

2.4.1.2 Transações

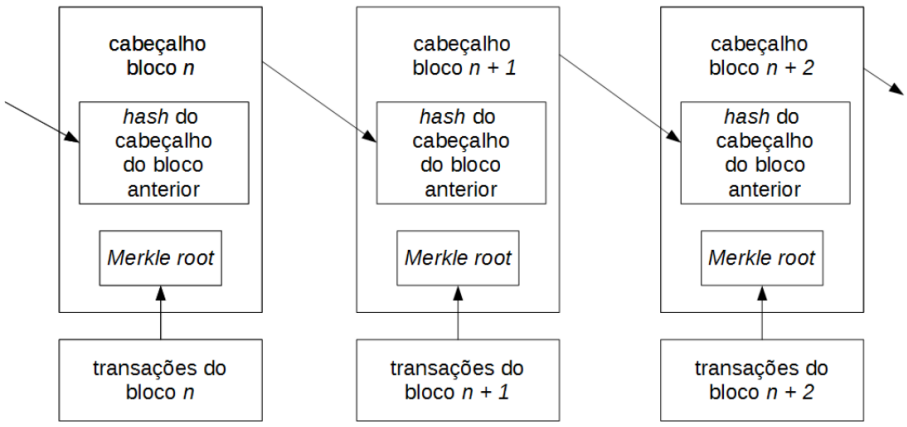
Todas as transações são armazenadas em uma lista encadeada de tal forma a permitir que qualquer membro da rede acesse o registro das transações e não seja necessário um agente centralizador para gerenciar, mediar e controlar as transações realizadas entre os membros desta rede (FIDELIS, 2022). Assim, percebe-se que a *blockchain* surgiu para ser uma espécie de livro-razão distribuído, disponível a todos os usuários de uma rede, com o histórico de todas as transações já realizadas (PEREIRA, 2018).

As transações são uma estrutura de dados atômica, indivisível, de uma *blockchain* (ABREU, 2020). Normalmente, uma transação é criada por um conjunto de usuários ou objetos autônomos (contratos inteligentes) para indicar a transferência de *tokens* dos remetentes para os destinatários especificados. Uma transação especifica uma lista de entradas associadas aos

valores de *token* com as identidades (endereços) das entidades de envio (WANG *et al.*, 2019).

A Figura 11 criada por Lucena e Henriques (2016) ilustra a estrutura e composição de cada bloco inserido na *blockchain* do Bitcoin. Em um bloco são reunidas uma ou mais transações e estas transações são organizadas como se fossem uma árvore (*Merkle tree*). Uma primeira transação tem seu valor *hash* calculado; em seguida, a próxima transação em conjunto com o *hash* da transação anterior também têm seu valor *hash* calculado e este processo continua até a última transação. O valor *hash* obtido ao final de todo processo é denominado *Merkle root*. Desta forma, é praticamente inviável alterar qualquer transação sem que se quebre toda esta cadeia, pois seus elementos estão fortemente ligados por meio de seus valores *hash*. Por fim, é calculado o valor *hash* do resultado final da operação entre as transações, *Merkle root*, com o valor *hash* do cabeçalho do bloco anterior da *blockchain*. Desta forma, qualquer alteração em uma transação ou em um bloco anterior é facilmente detectada por qualquer *peer* da rede *blockchain*.

Figura 11 – Modelo simplificado do *blockchain* do Bitcoin.



Fonte: adaptado de (LUCENA; HENRIQUES, 2016)

Em relação a criptografia assimétrica, cada nó na rede *blockchain* gera um par de chaves privada e pública (ABREU, 2020). A chave privada está associada a uma função de assinatura digital, que produz uma *string* de assinatura de comprimento fixo para qualquer comprimento arbitrário da mensagem de entrada. A chave pública está associada a uma função de verificação, que tem como entrada a mesma mensagem e a assinatura reconhecida para essa mensagem. A função de verificação só retorna verdadeiro quando a assinatura é gerada pela função de assinatura com a chave privada correspondente e a mensagem de entrada.

Os nós da rede identificam suas chaves públicas, ou seja, o código *hash* de suas chaves públicas, como seus endereços permanentes (também conhecidas como suas pseudo-

identidades) na *blockchain* (ABREU, 2020). Cada tupla de entrada em uma transação é assinada pela conta de envio. Dessa forma, a rede é capaz de validar publicamente a autenticidade da entrada por meio da verificação da assinatura com base no endereço público do remetente (WANG *et al.*, 2019).

2.4.2 Mineração

Segundo os desenvolvedores do Bitcoin.org (2022), a mineração é o processo de usar capacidade de processamento para processar transações, garantir a segurança da rede, e manter todos participantes do sistema sincronizados. Pode ser considerado como o *datacenter* do Bitcoin, exceto que foi projetado para ser totalmente descentralizado, com mineradores em todos os países e nenhum em particular tendo controle sobre a rede. Este processo é chamado de "mineração" em uma analogia à mineração de ouro porque é um mecanismo temporário utilizado na emissão de novos bitcoins. Porém diferentemente da mineração de ouro, a mineração de Bitcoin provê uma recompensa em troca dos serviços essenciais para operar uma rede segura de pagamentos. Mineração ainda será necessária depois que o último Bitcoin for emitido.

A mineração na *blockchain* é um processo de resolução de um quebra-cabeça criptográfico com poder de computação, em que os mineradores podem encontrar um novo bloco para *blockchain* (ABREU, 2020). Eles podem obter uma recompensa pelo bloco encontrado como forma de retribuir pelo seu poder de computação utilizado no processo de mineração (QIN *et al.*, 2018).

As atividades de mineração têm se tornado mais atrativas (MGHAZLI *et al.*, 2017). Porém, igual ocorre em uma mina de ouro, cada vez mais surgirá um maior número de interessados procurando ouro naquele lugar. O mesmo ocorre na mineração de dados e com isso a dificuldade na obtenção da moeda aumenta. Outro problema é que algumas moedas digitais apresentam volatilidade elevada. Por exemplo, no dia 15 de Janeiro de 2016 de acordo com a Exchange Poloniex, bolsa de valores digital, o Bitcoin abriu ao valor de 428 dólares e fechou a 362 dólares. No dia 29 de Maio de 2016 abriu a 491 dólares e fechou 551 dólares.

2.5 Arquiteturas para *Blockchain*

Executando uma busca sobre arquiteturas para *blockchain* é possível encontrar muitas propostas. Algumas dessas propostas fazem divisões em camadas na representação dos elementos

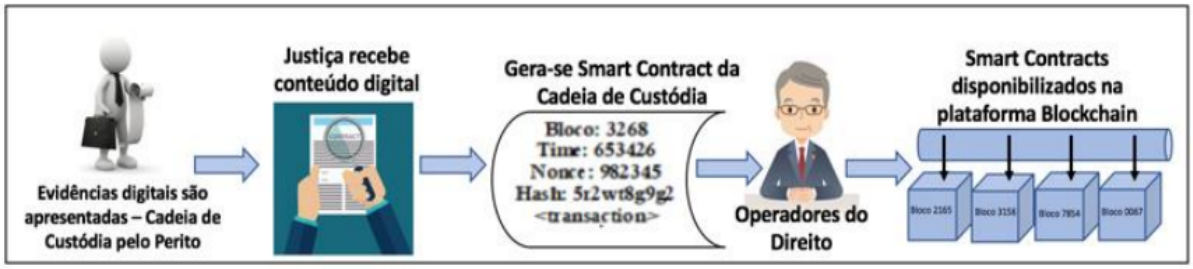
da arquitetura incluindo uma infraestrutura de *blockchain*. Como exemplos dessas arquiteturas existem os trabalhos de Petroni e Franco (2018), Gregório *et al.* (2021) e Mendonça *et al.* (2020).

Levando em consideração que toda evidência digital gerada, armazenada e coletada deve ser preservada de maneira completa, formando assim uma cadeia de custódia, antes da fase de análise para posterior confecção de um laudo pericial (PETRONI; FRANCO, 2018). Um *Smart Contract* baseado em *blockchain* apresenta um potencial considerável para garantir que as evidências – transformadas em objetos na cadeia de custódia possuam integridade e segurança para além do trabalho do perito, bem como o seu devido armazenamento.

A Figura 12 mostra uma arquitetura para disponibilizar a cadeia de custódia de provas em processos judiciais dividida por Petroni e Franco (2018), em cinco partes. Sendo a primeira etapa a apresentação das evidências digitais pela justiça, o perito apresenta a justiça as evidências digitais coletadas, podendo estas serem oriundas de mídias, redes de computadores, *dumps* de memória, etc.

A etapa seguinte é onde os componentes desta cadeia de custódia devidamente aprovados serão transformados em objetos – integrados através de *Smart Contract*. Próxima etapa é da criação efetiva do *Smart Contract*, ou seja, a sua preparação para posterior disponibilidade na plataforma *blockchain*. Após a criação do *Smart Contract*, cabe aos operadores do direito disponibilizá-lo na plataforma *blockchain*. Uma vez disponibilizados pelos operadores do direito, todos os *Smart Contracts* contendo os objetos da cadeia de custódia com as evidências digitais, poderão a qualquer tempo e lugar serem consultados.

Figura 12 – Proposta de arquitetura para disponibilizar a cadeia de custódia

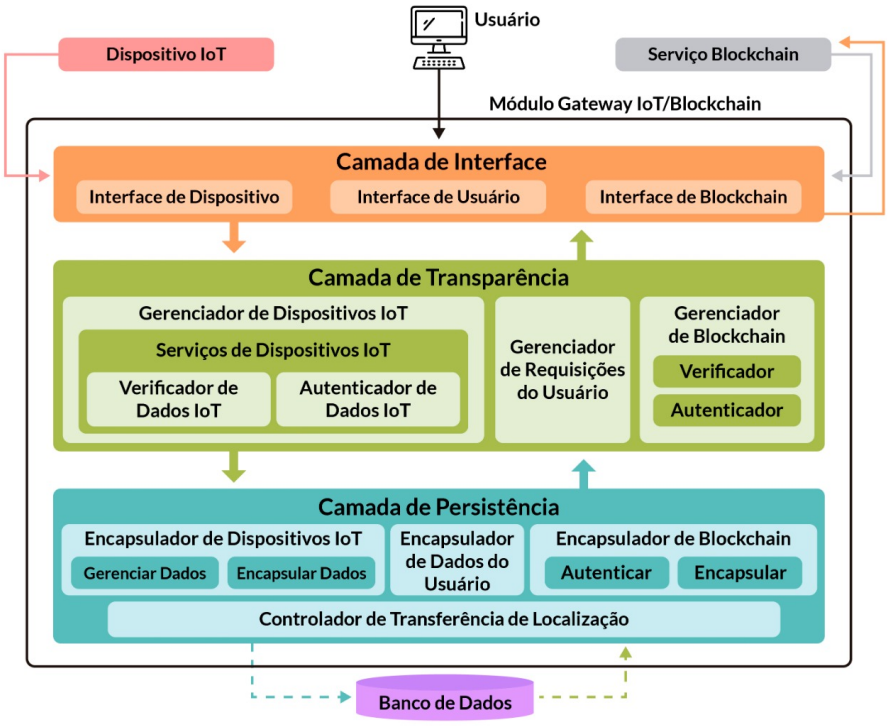


Fonte: adaptado de (PETRONI; FRANCO, 2018).

A Figura 13 mostra uma arquitetura de referência dividida por Gregório *et al.* (2021), em três camadas. A camada de Interface tem por objetivo a interação com o usuário, exibindo as informações requisitadas. Nesta camada estão os clientes (usuários, dispositivos e *blockchain*) ou aplicações que utilizarão os dados coletados através dos dispositivos *Internet of Things* (IoT). Esses usuários podem ser páginas *web* ou qualquer outro serviço habilitado com conexão à

internet. A camada de Transparência é responsável por gerenciar as funcionalidades necessárias para conexões dos dispositivos IoT com os serviços de *blockchain*, de forma que o usuário não tenha a percepção da complexidade e da estrutura dos métodos aplicados dentro desta camada, resultando em uma transparência para o usuário final. A camada de Persistência é responsável por gerenciar a manipulação dos dados dentro do sistema através da linguagem de manipulação de dados (ou *Data Manipulation Language* (DML)). A DML é um conjunto de comandos dentro da linguagem de consulta estruturada ou *Structure Query Language* (SQL), utilizado para recuperar, incluir, remover e modificar informações em bancos de dados (ALI; SHIBGHATULLAH, 2016).

Figura 13 – Arquitetura Proposta por Gregório *et al.* (2021)



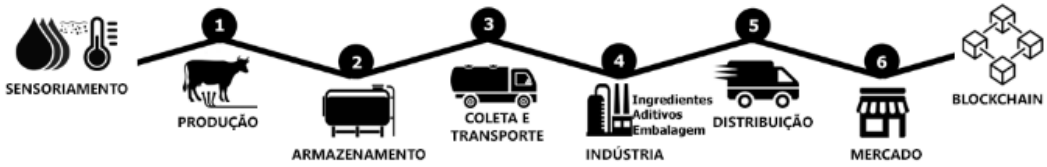
Fonte: adaptado de (GREGÓRIO *et al.*, 2021).

A arquitetura proposta no trabalho de Mendonça *et al.* (2020) foi baseada nos processos da cadeia de suprimentos do leite, foi definido um modelo de arquitetura para atender a rastreabilidade em relação ao funcionamento da captação, armazenamento e transporte da produção leiteira. A arquitetura visa interligar os diversos componentes em um sistema de gerenciamento da cadeia de suprimentos para garantir que os usuários tenham confiabilidade nos dados coletados durante o processo de produção. A arquitetura é composta por três módulos principais, sendo que o módulo rastreabilidade e o módulo cliente comunicam diretamente com a *blockchain*. Já o módulo sensores provê suporte à comunicação dos sensores externos ao sistema.

A Figura 14 apresenta a cadeia produtiva do leite com relação ao sensoriamento e

ao armazenamento dos dados coletados para análise e rastreabilidade em todos os pontos de controle (MENDONÇA *et al.*, 2020). A *blockchain* foi utilizada como um banco de dados distribuído e também para a validação de acessos. Os contratos inteligentes foram utilizados para organizar o processo de manipulação dos dados. O módulo rastreabilidade é responsável por toda interoperabilidade entre a captação dos dados coletados no decorrer da cadeia de suprimentos e a sua disponibilização na *blockchain*. O módulo cliente fica encarregado em prover acesso público aos dados registrados pelo módulo rastreabilidade. Por meio dele, o consumidor final ou qualquer outro interessado na rastreabilidade do produto, poderá solicitar a visualização dos dados coletados.

Figura 14 – Cadeia produtiva do leite



Fonte: adaptado de (SHINGH *et al.*, 2020).

2.6 Principais Aplicações da *Blockchain*

A primeira aplicação da *blockchain* que ganhou destaque foi o desenvolvimento da moeda digital denominada Bitcoin. Não obstante, são inúmeras as possibilidades de aplicação da *blockchain*, entre as quais: (i) contratos digitais autoexecutáveis (*Smart Contracts*); (ii) ativos inteligentes que podem ser controlados via *blockchain* por meio de contratos automatizados (*Smart Property*); (iii) desenvolvimento de novos sistemas de governança com maior participação democrática, tais como sistemas de votação; e (iv) organizações descentralizadas autônomas que podem operar sem qualquer interferência externa (PORTO *et al.*, 2019).

O potencial dessa tecnologia é imenso, sendo que aplicações estão surgindo em inúmeros setores além da própria computação (protocolos de redes, nuvem e IoT), como por exemplo, nas áreas de finanças, saúde, artes e governo (GREVE *et al.*, 2018). Investimentos em desenvolvimento ou monitoramento de aplicações que se baseiam em *blockchain* por parte de empresas vem ganhando força. Como exemplo, existem os seguintes projetos:

– Rastreabilidade de Alimentos: A PariPassu, em 2007, lançou a primeira versão do Sistema Rastreador PariPassu, uma tecnologia capaz de registrar a origem, caminho percorrido

e destino de um produto. Hoje, a solução é referência em rastreabilidade e *recall* de alimentos e pode ser utilizada por todos os elos da cadeia de suprimentos. Por meio do Rastreador PariPassu, todos os participantes da cadeia produtiva podem consultar a origem, destino e trajetória de um alimento (LIMA, 2018);

– *Blockchain* na Agroindústria: Um projeto está sendo conduzido no âmbito do acordo de cooperação técnica firmado entre a Empresa Brasileira de Pesquisa Agropecuária (Embrapa) e o Grupo Granelli Ltda – unidade agroindustrial Usina Granelli e registrado no Sistema de Acompanhamento de Instrumentos Contratuais (SAIC) sob o número 23800.20/0028-1. É um exemplo de *blockchain* privada que está sendo implementada no projeto-piloto intitulado "Sistema de rastreabilidade utilizando tecnologia blockchain para produtos e processos agroindustriais da cadeia produtiva sucroalcooleira". Este projeto-piloto é um desdobramento de uma solução de inovação intitulada "Software de rastreamento e compartilhamento de dados dentro da cadeia produtiva da cana-de-açúcar via tecnologia *blockchain*" (USINA GRANELLI, 2022);
– Governo: o órgão de Serviço Federal de Processamento de Dados (Serpro) do governo brasileiro anunciou em 2019 uma solução que utiliza a tecnologia *blockchain* para garantir a autenticidade das informações compartilhadas entre o Brasil e países do Mercosul. Essa solução permite o compartilhamento de informações cadastrais das empresas certificadas pela Receita Federal para facilitação dos procedimentos aduaneiros, tanto no Brasil quanto no exterior (SERPRO, 2019);
– Financiamento coletivo: O impactMarket, plataforma de financiamento coletivo em *blockchain*, focada na erradicação da pobreza e na renda mínima garantida para populações vulneráveis, ultrapassou a marca de 350 mil dólares (mais de 2 milhões de reais) distribuídos no Brasil. Lançado em setembro de 2020, o projeto utiliza o *Celo Dollar* (cUSD), uma *criptomoeda* de valor equivalente ao dólar, para realizar as transações. Funciona assim: instituições e associações cadastram seus projetos sociais ou comunidades no impactMarket. A plataforma lista os projetos aprovados em seu aplicativo e doadores do mundo todo, sejam pessoas físicas ou jurídicas, podem fazer suas contribuições. As doações são encaminhadas através da Bitfy ou outra carteira com suporte ao cUSD, onde os beneficiários podem utilizar o valor da forma que acharem mais conveniente (RUBINSTEINN, 2021).

Existem outras aplicações possíveis, como votação eletrônica, pagamento de hipoteca, gerenciamento de direito digital, seguro de automóvel, armazenamento de arquivos

distribuídos, gerenciamento de identidades e cadeia de suprimentos (ALHARBY; MOORSEL, 2017). Está surgindo uma infinidade de aplicações com a utilização dos contratos inteligentes na *blockchain*. Essas aplicações são desenvolvidas por organizações da indústria e acadêmicas, buscando benefícios dessa tecnologia em diversas áreas da sociedade.

2.7 Analisando Adoção da Tecnologia *Blockchain*

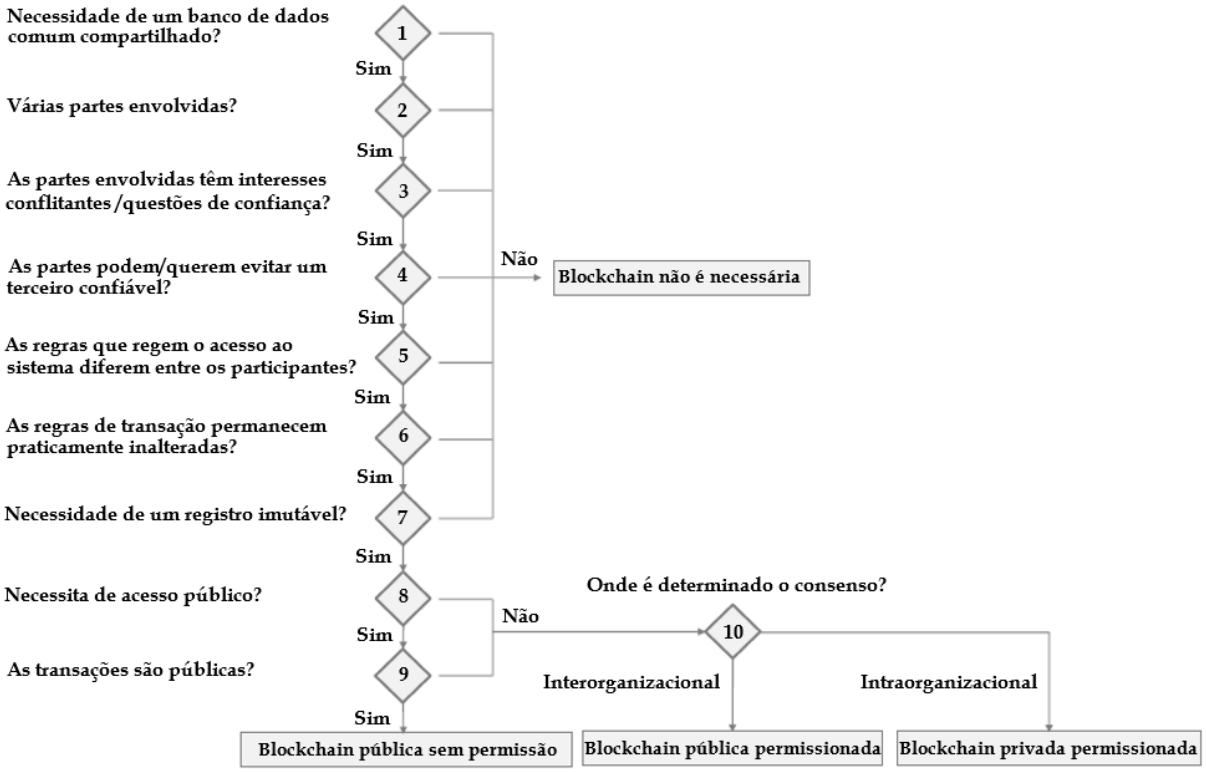
Um grande desafio encontrado por arquitetos de sistemas na utilização de tecnologia *blockchain*, é o fato dela poder adicionar muita complexidade a qualquer área da indústria ou acadêmica. Com isso é importante considerar-se atributos de qualidade e buscar justificativas que apoiem decisões sobre o uso de uma *blockchain* ou um sistema convencional. O trabalho de Rifi *et al.* (2017) descreve uma simplificação na escolha da tecnologia *blockchain*, fazendo algumas perguntas cruciais em dez etapas (Figura 15), buscando justificar o uso da *blockchain*. A ideia central do trabalho recomenda que uma *blockchain* é viável caso tenha pelo menos cinco das sete primeiras pergunta respondidas com "Sim". Mesmo com essa ajuda, os interessados devem ponderar de maneira cuidadosa diversos requisitos para cada caso de aplicação de forma individualizada.

As perguntas devem ser discutidas com usuários que tenham experiência na lógica de negócio do ambiente a ser analisado, permitindo uma interação mais adequada com os profissionais com experiência em *blockchain* que atuariam na avaliação do emprego dessa tecnologia. Dentre as questões, as sete primeiras se mostram mais específicas sobre o uso da tecnologia *blockchain*, buscando a viabilização da aplicação da solução. Já as três últimas questões buscam auxiliar na escolha de qual tipo de *blockchain* seria mais adequado para uma aplicação específica.

O passo a passo seguindo as perguntas, corresponde a um caminho de decisão que pode ser usado pelos interessados para identificar se existe um caso onde a adoção de uma solução *blockchain* seja válido. Uma sequência de perguntas simples com respostas compostas apenas de sim ou não poderá auxiliar os profissionais na decisão de quando usar uma *blockchain* além de também indicar o tipo mais adequado. Mesmo assim, o projeto da solução requer mais que decisões binárias, precisa levar em conta as regras de negócio mais amplas, requisitos e restrições (RIFI *et al.*, 2017).

Analisando no contexto do *crowdfunding*, com a utilização dos contratos inteligentes em uma rede *blockchain*, possibilitará aos usuários investidores uma auditoria a respeito do

Figura 15 – Visão geral do caminho de decisão da *blockchain*



Fonte: adaptado de (RIFI *et al.*, 2017).

dinheiro aplicado em um projeto. Isso agrega mais confiança na hora de investir e segurança pelo fato da imutabilidade atrelada aos blocos na cadeia, além de mais transparência aos usuários. A partir do momento em que um número suficiente de computadores – geralmente 51% – aceita a gravação de um bloco novo no banco de dados, tal bloco passa a ser imutável dentro da *blockchain* – é o que se chama de confirmação. A imutabilidade é decorrente não apenas do número crescente de confirmações, mas também – e principalmente – pelo fato de que como cada bloco tem seu próprio *hash* que depende do conteúdo ali armazenado, eventuais tentativas de alteração do conteúdo do bloco gerariam um novo *hash*, conflitando com o *hash* original. Verifica-se, portanto, que a decisão de gravar ou não um novo bloco na *blockchain* depende do consenso entre os usuários e não apenas da "vontade" da entidade controladora da rede (SILVA, 2018).

3 TRABALHOS RELACIONADOS

Este capítulo descreve a metodologia utilizada para encontrar trabalhos relacionados a esta dissertação. Uma visão geral do assunto é mostrada com a finalidade de situá-lo perante a literatura encontrada, além de uma breve descrição de cada trabalho. Em seguida, alguns critérios levados em consideração em termos de comparação entre a proposta da dissertação e os trabalhos relacionados também são apresentados.

3.1 Planejamento da Busca por Trabalhos Relacionados

Blockchain é uma tecnologia que tem ganhado muito destaque nos últimos anos, fato que acaba chamando atenção tanto para o meio acadêmico quanto para o meio industrial. A tecnologia vem sendo aplicada nas mais variadas áreas e chegando cada dia mais próximo de todos. Na área de financiamento coletivo, o chamado *crowdfuding*, a *blockchain* vem sendo utilizada para diversos fins, em muitos casos explorando suas características de imutabilidade e rastreabilidade.

O objetivo principal deste trabalho é propor uma solução para *crowdfunding* de forma integrada com uma rede *blockchain* buscando melhorias no processo de investimentos em projetos com colaboração coletiva. Desta forma esta revisão da literatura servirá de base para fundamentação teórica e estudos de trabalhos que se relacionam com o tema definido pelo objetivo. Para obter uma melhor organização da busca por trabalhos relacionados foi utilizada a ferramenta Parsifal [1]. Nela há a possibilidade de importar os trabalhos de acordo com suas respectivas base de dados, também possibilita a inclusão de questões de qualidade a serem respondidas de acordo com cada trabalho individualmente. Além disso é possível gerar uma análise dos dados inseridos, a respeito dos trabalhos, a partir dela.

Levando em consideração observações dos trabalhos encontrados na revisão da literatura, algumas questões são levantadas a fim de entender em que momento o campo de pesquisa se encontra atualmente. O questionamento principal a ser respondido é “Qual o estado da arte de arquiteturas de sistemas de *crowdfunding* com *blockchain*?”. Em um segundo momento é importante observar de que modo está sendo feito o estudo, e quais as vantagens do uso da *blockchain* em relação aos bancos de dados tradicionalmente utilizados, assim faz-se o questionamento “Quais as maiores vantagens de utilização da tecnologia *blockchain* nas

[1] https://parsif.al/ Acesso em: 08 ago. 2022

arquiteturas e quais as diferenças em relação às tecnologias tradicionais do ponto de vista de *crowdfunding*?".

Observa-se também o desempenho das plataformas de *blockchain*, a fim de entender qual a melhor a ser utilizada na solução que se quer propor neste trabalho, dessa forma registra-se o questionamento "Em trabalhos comparativos, utilizando arquiteturas de *blockchain* para sistemas de *crowdfunding*, quais plataformas de *blockchain* mais utilizadas e quais apresentam melhor desempenho neste tipo de sistema?". Neste trabalho, considerando que visa-se a aplicação da solução em um ambiente real, também se tenta identificar informações acerca do custo de uso das plataformas, assim levanta-se o questionamento "Existem estudos que tratem o custo de utilização da tecnologia *blockchain* nas arquiteturas de sistemas de *crowdfunding*? Qual o impacto deste custo?". Ao fim da revisão sistemática espera-se ter respondido estes questionamentos para se ter embasamento suficiente que justifique a proposição da solução aqui descrita.

Esta revisão foi inspirada pela seguinte questão "Quais trabalhos científicos fazem uso do *blockchain* para desenvolver *crowdfunding*?". Com esta questão em mente e após testes com algumas palavras chave, foi definido a seguinte *string* de busca: "*allintitle*: ("*Crowdfunding*" *OR* "Financiamento Colaborativo") *AND* ("*Blockchain*")". Logo em seguida a busca foi refeita sem o termo em português "Financiamento Colaborativo" e acabou gerando o mesmo resultado, com isso a *string* de busca final para o trabalho foi: "*allintitle*: ("*Crowdfunding*") *AND* ("*Blockchain*")".

Ao buscar utilizando apenas os termos "("*Crowdfunding*") *AND* ("*Blockchain*")" sem a utilização da palavra *allintitle*, que significa que os termos da pesquisa devem estar presente no título dos trabalhos, os resultados obtidos da busca chegam a números expressivos no valor de 14.200 resultados. Qualquer outra combinação buscada geravam diversos trabalhos. Assim foi o processo para a definição da *string* de busca.

Para a busca, foram utilizados bibliotecas digitais através da funcionalidade de busca avançada, bibliotecas como: ACM Digital Library [2], IEEE Xplore Digital Library [3], Science Direct [4] e Springer Link [5]. Foi percebido que em sua grande maioria não era retornado nenhum trabalho ou apenas 1 ou 2. Diante disso, a busca foi direcionada ao Google Acadêmico [6].

[2] https://dl.acm.org/ Acesso em: 08 ago. 2022
[3] https://ieeexplore.ieee.org/Xplore/home.jsp Acesso em: 08 ago. 2022
[4] https://www.sciencedirect.com/ Acesso em: 08 ago. 2022
[5] https://link.springer.com/ Acesso em: 08 ago. 2022
[6] https://scholar.google.com.br/ Acesso em: 08 ago. 2022

Como critério de inclusão foram considerados apenas artigos científicos sem limite para data de sua publicação, que fossem escritos no idioma inglês ou português, que estivessem disponíveis para livre acesso via Internet, que apresentassem uma arquitetura proposta ou utilizada, que apresentassem sistema *crowdfunding* e que utilizassem a tecnologia *blockchain*. Como critério de exclusão, caso o artigo apenas cite os termos da busca e não tenha aprofundamento do tema, tenha menos de 4 páginas, possua os termos apenas no título ou é um trabalho meramente informativo ou uma notícia, procedeu-se ao descarte da pesquisa.

Alguns crítérios de qualidade foram aplicados na seleção dos trabalhos. Foi observado se a motivação do estudo está bem justificada, se do ponto de vista de metodologia o trabalho está bem organizado/estruturado, se a arquitetura proposta e/ou utilizada no trabalho é apresentada de modo claro e detalhado. Também foi observado se existe um esboço gráfico ou imagem da arquitetura proposta ou utilizada no trabalho, se houve testes em ambiente realístico do trabalho proposto e também se foi realizado um estudo sobre os custos de utilização da tecnologia *blockchain*.

O processo de busca pelos trabalhos relacionados seguiu os seguintes passos: (i) definição da *string* de busca refinada; (ii) na seleção dos estudos inicial, é feita a leitura dos resumos, títulos, verificado as estruturas, logo após aplicado os critérios de inclusão e exclusão; e (iii) os trabalhos que passaram da etapa anterior são lidos por completo e aplica-se novamente os critérios de inclusão e exclusão.

3.2 Visão Geral

O processo de busca por trabalhos relacionados ocorreu em abril de 2022. Foram encontrados 21 trabalhos ao todo. A Tabela 1 exibe as fontes e também o quantitativo encontrado em cada uma delas.

Os 21 documentos selecionados foram provenientes de 18 fontes distintas. Após serem aplicados os critérios de inclusão e exclusão, resultou-se em 10 artigos e a única base de dados que teve mais de um artigo selecionado foi a IEEEXplore. A Tabela 2 lista as fontes e as quantidades de trabalhos selecionados em cada uma delas.

Todos os 10 trabalhos identificados na etapa final foram lidos por completo e descritos brevemente na Seção 3.3. Diversos aspectos foram coletados, dispostos e analisados após a coleta das informações contidas nos trabalhos. Informações como: ano de sua publicação, palavras chaves do trabalho, país da instituição dos autores, se o trabalho foi aplicado no mundo real, se

Tabela 1 – Fontes dos Trabalhos Relacionados Encontrados

Fonte	Quantidade de Trabalhos
ACM Digital Library	1
Applied Information Technology and Computer Science (AITCS)	1
Biblioteca Virtual em Saúde (BVS)	1
Darmabakti Cendekia: Journal of Community Service and Engagements	1
Emerald Publishing	1
FirstMonday	1
IEEEXplore	2
Innovation and Global Issues Congress IV	1
MIT Libraries	1
Munich Personal RePEc Archive	1
Prorequest	1
Research Platform Alexandria	1
ResearchGate	1
SSRN	2
Springer Link	2
Universitat Autónoma de Barcelona	1
Wiley Online Library	1
eLIBRARY.RU	1
Total	**21**

Fonte: o autor.

Tabela 2 – Fontes dos Trabalhos Relacionados Selecionados

Fonte	Quantidade de Trabalhos
ACM Digital Library	1
Applied Information Technology and Computer Science (AITCS)	1
Biblioteca Virtual em Saúde (BVS)	1
FirstMonday	1
IEEEXplore	2
Munich Personal RePEc Archive	1
Research Platform Alexandria	1
SSRN	1
Springer Link	1
Total	**10**

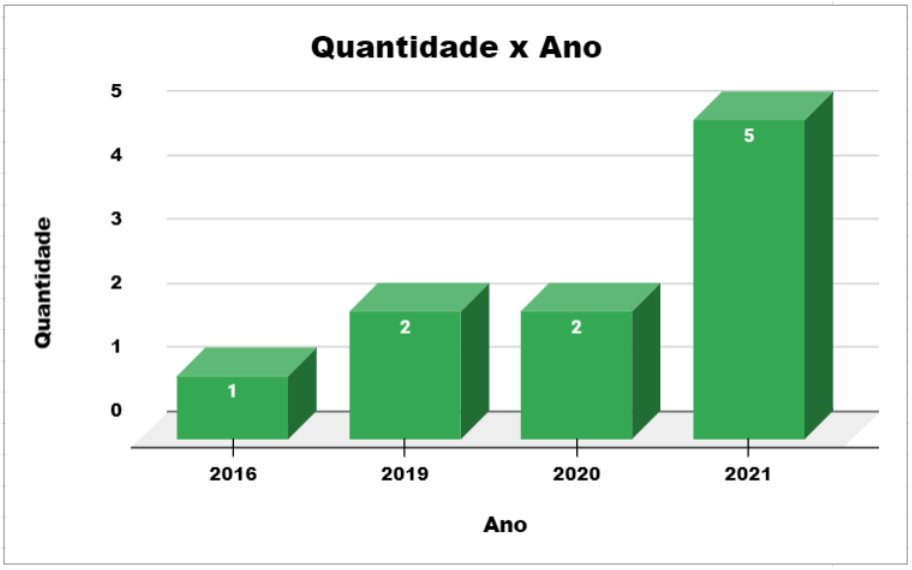
Fonte: o autor.

propôs arquitetura, se uma aplicação/aplicativo/site foi construído(a) com base na proposta e se realizou alguma análise de desempenho, caso tenha realizado, quais foram as métricas utilizadas. Também foram analisadas ferramentas que se relacionam com o desenvolvimento utilizando *blockchain* presentes nos trabalhos. Esses dados foram utilizados para confecção da revisão sistemática realizada por este trabalho.

A Figura 16 apresenta a quantidade de trabalhos identificados e catalogados de acordo com o ano de publicação por ano. Como é observado, os trabalhos relacionados à tecnologia *blockchain* ligado ao *crowdfunding* vem aumentando ao longo dos anos, saindo de 1 trabalho em 2019 para 5 em 2021. Como a área está começando a evoluir, também espera-se

cada vez mais publicações futuras.

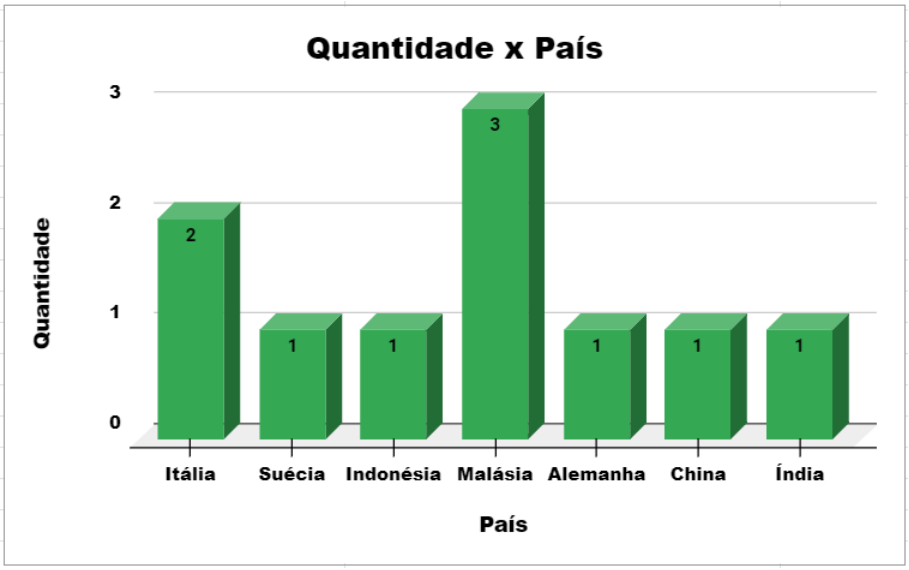
Figura 16 – Quantidade de trabalhos por ano



Fonte: o autor.

A Figura 17 apresenta a quantidade de trabalhos identificados de acordo com o país da instituição dos autores. Entre os 10 trabalhos, existem 3 que são provenientes do mesmo país, a Malásia. Fato este que mostra avanços nas pesquisas envolvendo *blockchain* no continente asiático. Com destaque também para a Itália com seus 2 trabalhos sendo um da cidade de Turim e outro da cidade de Pisa. Todos os demais foram de países diferentes totalizando 7 países distintos.

Figura 17 – Quantidade de trabalhos por país



Fonte: o autor.

A Figura 18 foi construída utilizando uma ferramenta online gratuita Wordclouds [7] onde é possível descrever todas as palavras chaves definidas nos trabalhos e escolher o formato em que elas devem aparecer de forma aleatória e automática. Com destaque para *blockchain*, *crowdfunding* e *smart contract*, que por serem recorrentes nos trabalhos acabam aparecendo mais vezes na figura. Elementos e características da tecnologia *blockchain* também foram mencionados.

Figura 18 – Nuvem de palavras construída pelas palavras chave dos trabalhos

Fonte: o autor.

O Quadro 1 lista os veículos de publicação utilizados pelos trabalhos identificados. Todos os trabalhos foram publicados em eventos e revistas diferentes.

Respondendo ao questionamento sobre o estado da arte de arquiteturas de sistemas *crowdfunding* com o uso de *blockchain* foi percebido que existe um crescente número de estudos sendo realizados, principalmente no continente europeu e asiático. Muitas empresas já buscam sistemas que utilizam *blockchain* para uso de *crowdfunding*.

A respeito das vantagens elencadas nos trabalhos encontrados, se destacam a confiabilidade, imutabilidade e rastreabilidade das transações realizadas em uma rede *blockchain*. O *crowdfunding* tem sido beneficiado pelo uso desta tecnologia, aumentando a confiança dos participantes do processo.

[7] https://www.wordclouds.com/ Acesso em: 08 ago. 2022

Quadro 1 – Lista de veículos de publicação identificados na pesquisa

International Conference on Computer Technology Applications (ICCTA)
IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT
Applied Information Technology And Computer Science
International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)
Pre-ICIS SIGBPS 2019 Workshop on Blockchain and Smart Contract
International Journal of Advanced Trends in Computer Science and Engineering
International Conference on Computer Technology Applications (ICCTA)
Munich Personal RePEc Archive (MPRA)
Available at SSRN
First Monday

Fonte: o autor.

Em relação à questão das plataformas *blockchain* que aparecem nos trabalhos encontrados, foi observado que em sua grande maioria é utilizado a rede Ethereum. Nos trabalhos onde foram desenvolvidos aplicações ou apenas arquitetado o desenvolvimento de uma, a rede escolhida foi a Ethereum com destaque para seus contratos inteligentes.

Um detalhe que chama atenção nos trabalhos, é o fato de não mencionarem a questão dos custos sobre transações. Ao trabalhar com a tecnologia *blockchain* deve-se sempre lembrar que existe um custo sobre as transações que são enviadas para a rede. Com isso, não foi levado em consideração os impactos inerentes aos custos devido a utilização da tecnologia *blockchain*.

3.3 Descrição dos Trabalhos Relacionados e Comparação

O estudo desenvolvido por Zhu e Zhou (2016) examina os problemas atuais na prática de *crowdfunding* de capital na China. Com base na análise das características da tecnologia *blockchain*, explora suas aplicações práticas em *crowdfunding* de ações. Para eles, no que diz respeito ao registro e confirmação de acionistas de uma empresa de *crowdfunding*, documentos em papel, como listas de acionistas, são uma espécie de meio de armazenamento de informações centralizado. As listas de acionistas baseadas na tecnologia *blockchain* podem ser usadas como uma alternativa melhor aos documentos tradicionais em papel. Os recursos da *blockchain* de gerenciamento de dados descentralizado, armazenamento de contabilidade distribuído, anti-adulteração e anti-falsificação garantem que ela seja mais segura do que os documentos em papel tradicionais.

Acreditam Zhu e Zhou (2016) que, com a maturidade e amplo uso da tecnologia *blockchain*, uma plataforma unificada de registro, transação e transferência de ações de *crowdfunding* pode ser estabelecida com base na tecnologia *blockchain*. Com base na revisão de literatura, análise de funcionalidades do *blockchain* e casos de aplicações de *blockchain*, eles acreditam

que a tecnologia *blockchain* tem alto valor e boas perspectivas na resolução dos problemas de *equity crowdfunding* e na otimização do seu processo.

Como objetivo principal, Martino *et al.* (2019) investigam as potenciais vantagens e desafios da tecnologia *blockchain* e *Initial Coin Offerings* (ICOs), e como eles afetarão o ambiente empreendedor. Em particular, além de fornecer uma primeira visão geral sobre *blockchain* e ICOs no contexto das finanças empresariais, o trabalho também visa fornecer contribuições práticas para reguladores, empresários e investidores interessados nessas novas inovações financeiras.

Blockchain e ICOs possibilitam que as empresas atraiam investimentos de uma variedade de investidores em todo o mundo, graças à natureza transfronteiriça e descentralizada da *blockchain*. Além disso, a aplicação da tecnologia *blockchain* proporciona maior segurança aos investidores, pois os pagamentos dos investidores são registrados em um livro público de forma transparente e imutável. Eles também apresentam uma visão geral sobre o potencial das ofertas iniciais de moedas e as tecnologia *blockchain* no contexto de finanças empresariais. Apontam Martino *et al.* (2019) que as ICOs e as tecnologia *blockchain* permitem que novos empreendimentos coletem um grande número de contribuições financeiras de um número significativo de investidores em todo o mundo, de forma rápida, de baixo custo e flexível em comparação com outro mecanismo de financiamento tradicional, como a *crowdfunding*.

O papel da *blockchain* no armazenamento de informações na rede Ethereum é apresentado por Lee e Rahim (2021). Também existe uma proposta de uma aplicação web *blockchain* descentralizada, FundDapp, que visa projetar uma aplicação *web* de *crowdfunding* descentralizada que forneça transferências *peer-to-peer*, desenvolver um site *blockchain* para fins de *crowdfunding* e testar a aplicação na rede Ethereum. Foi adotada Análise e Design Orientados a Objeto (OOAD) como metodologia para o desenvolvimento do projeto. Essa metodologia e seu fluxo são separados em análise de requisitos orientada a objetos, *design* orientado a objetos, implementação e testes orientados a objetos.

O trabalho de Lee e Rahim (2021) também visa utilizar extensivamente a tecnologia *blockchain* para proteger as informações importantes, como os registros transacionais de doação. A solução *blockchain* resolve e preserva a integridade das informações e resolve o problema de modificação não autorizada. A solução também permite que o público rastreie os registros de doações da plataforma de *crowdfunding* e se beneficie da garantia de transações em tempo real. Por fim, a solução elimina a necessidade de intermediários. Assim, organizações de caridade podem agilizar os processos e reduzir custos.

Para Ashari *et al.* (2020), muitas organizações sem fins lucrativos desempenham um papel como arrecadadores de fundos, especialmente na condição da pandemia do Covid-19. A confiança é seu desafio para atrair doadores para doar seu dinheiro para a organização. Portanto, a partir disso, concluiu-se que, além da confiança, que é o principal fator para obter o máximo de recursos possível, a tecnologia também desempenha um grande papel nisso. Com base nisso Ashari *et al.* (2020) fazem uma análise dos processos que geralmente estão contidos nestas organizações de captação de recursos, aplicando a tecnologia *blockchain* que pode ser uma solução alternativa para aumentar a confiança dos financiadores o que certamente afetará o quanto de fundos será obtido pela captação de recursos.

A aplicação da tecnologia *blockchain* não apenas aumenta a confiança nas organizações de captação de recursos, mas também pode ser usada como validação dos financiadores para garantir que os fundos sejam obtidos de fontes confiáveis e também para validar os destinatários dos fundos, sejam eles confiáveis ou não. A revisão bibliográfica realizada por Ashari *et al.* (2020) utiliza o método de pesquisa em biblioteca, que conta com fontes de periódicos que foram publicados internacionalmente e nacionalmente, juntamente com outros artigos relevantes para que possam ser usados como referência.

Foram descritos por Ashari *et al.* (2020) três esquemas dominantes de processo de *crowdfunding*:

- **Tudo ou Nada (AoN):** É um esquema de processo de *crowdfunding* que emprega a estratégia que caso a angariação de fundos não atinja a meta, os fundos serão devolvidos aos financiadores;
- **Mantenha o Tudo (KIA):** Não muito diferente do esquema AoN, é um esquema de processo de *crowdfunding* que implementa se a angariação de fundos não atingir a meta, os fundos serão devolvidos aos financiadores;
- **Esquema de Metas Esticadas (SGS):** Há um desenvolvimento da meta de captação de recursos que é ampliada e vinculada pela declaração onde se pode agregar alguns valores adicionais pré-determinados para produtos e serviços. Caso a meta de captação de recursos seja alcançada, então o arrecadador poderá realizar todas as ações necessárias para agregar esse valor.

Também segundo Ashari *et al.* (2020) existem alguns processos que podem ser otimizados usando contrato inteligente e tecnologia *blockchain*. Exemplo de onde poderiam ser aplicados é no processo de verificação de dados de requerentes e financiadores, eliminando a

dependência com terceiros (bancos) e encurtando o envio e desembolso de fundos.

Uma discussão é levantada por Creta e Tenca (2021) a respeito de como os administradores de plataformas, que operam dentro do ecossistema de *crowdfunding* imobiliário, podem implementar inovações tecnológicas como *blockchains* ou o uso de *tokens* digitais, e também são listados os benefícios que podem ser obtidos pelo setor imobiliário. É apresentada uma análise exploratória de estudos de casos múltiplos, constituídos por doze empresas que gerem plataformas de *crowdfunding* imobiliário. As informações coletadas por meio de entrevistas dão uma ideia de como as opiniões compartilhadas dos profissionais do trade são identificadas com fatores e variáveis que afetam a abertura desse segmento financeiro alternativo. Em termos de implicações, acreditam que o seu trabalho é um dos primeiros estudos a explorar a adoção de tecnologias inovadoras por plataformas de *crowdfunding* imobiliário e é o primeiro a analisar o impacto da *tokenização*.

Na opinião de Creta e Tenca (2021), poucas pesquisas empíricas foram realizadas sobre a possível interação entre *crowdfunding* e *blockchain* no setor imobiliário. Uma abordagem inicial de pesquisa exploratória e qualitativa, portanto, pareceu ser o meio mais recomendado para estudar esse novo fenômeno. Em seu trabalho, as entrevistas tiveram como objetivo alcançar uma visão do estado da arte atual sobre uma possível interação e conexão entre *crowdfunding* e *blockchain* dentro de plataformas de *crowdfunding* especializadas em imóveis. Opiniões sobre os rumos futuros dos empreendimentos do setor e sobre o possível uso da tecnologia *blockchain* foram buscadas, as vantagens que adviriam de seu uso também, discutindo os assuntos em questão e levando em consideração a literatura.

Especificamente, a entrevista realizada por Creta e Tenca (2021) consistiu em sete questões abertas que abrangeram três aspectos principais: (1) o possível uso da tecnologia *blockchain* em plataformas de *crowdfunding* imobiliário; (2) a possível utilização de *tokens* digitais em plataformas de *crowdfunding* imobiliário; e, (3) as possíveis vantagens e desvantagens, com base nas regulamentações atuais, que podem derivar da aplicação da tecnologia *blockchain*. Partindo de ideias fornecidas pela literatura, foram alcançadas várias áreas, deixando aos entrevistados uma ampla liberdade para suas respostas.

A principal consideração feita por Creta e Tenca (2021), que surgiu das respostas fornecidas pelos entrevistados, é o pensamento compartilhado de que o uso da tecnologia *blockchain* só pode ser benéfico dentro de um setor – imobiliário – que é estático, pouco inovador e que possui fortes barreiras à inovações. No que diz respeito a primeira questão levantada (Quais

são os efeitos das alternativas de financiamento no setor imobiliário?) o uso da *blockchain* no setor imobiliário permite maior transparência, imutabilidade das transações, redução de tempo e custos, e melhora a eficiência do processo de informação. Em termos da segunda questão (O uso de *tokens* digitais dentro do ecossistema de *crowdfunding* imobiliário pode contribuir para melhorar a eficiência dos investimentos?) a criação e utilização de *tokens*, principalmente *security tokens* oferecidos por meio de *Security Token Offering* (STO), trariam benefícios para um setor em termos de liquidez, ou seja, a eficiência dos investimentos, contribuindo para a implantação do chamado mercado secundário de negociação de títulos em um imóvel.

Com o objetivo de avaliar a interação entre *crowdfunding*, tecnologias *blockchain*, *criptomoedas* e ICOs, Bogusz *et al.* (2020) desenvolveram um trabalho que utiliza uma abordagem metodológica emergente chamada Social Media Analítica (SMA), que permite rastrear discussões públicas sobre *crowdfunding*, *blockchain*, criptomoedas e ICOs no cenário de mídia social. Com base em um total de 197.770 conteúdos gerados por usuários capturados em três rodadas de coleta de dados, foi avaliado a interação entre *crowdfunding*, *blockchain*, criptomoedas e ICOs e além disso é oferecido uma exploração sistemática das principais características dessa interação.

Em seu trabalho, Bogusz *et al.* (2020) utiliza a palavra-chave "*crowdfunding*" para coletar conteúdo gerado pelos usuários e publicado publicamente durante três períodos de tempo.

- **Primeiro período:** Entre 6 e 12 de maio de 2017, produzindo um conjunto de dados de 74.678 conteúdos gerados por usuários do Twitter, Instagram, Facebook, blogs, fóruns e YouTube que incluíam a palavra-chave (durante o surgimento das ICOs);
- **Segundo período:** Entre 12 e 18 de outubro de 2017, produzindo um conjunto de dados de 67.076 postagens de mídia social extraídas das mesmas plataformas de mídia social, (durante o auge do investimento em ICOs);
- **Terceiro período:** Entre 26 de setembro e 2 de outubro de 2018, gerou um conjunto de dados de 56.016 postagens de mídia social também extraídas das mesmas plataformas de mídia social (logo após a deflação do mercado de ICOs).

Assim, os dados permitiram analisar se e como as ICOs, *criptomoedas* e *blockchain* se integraram no contexto das discussões de *crowdfunding* nas mídias sociais durante esses três períodos.

Na coleta dos dados Bogusz *et al.* (2020) utilizaram um serviço chamado notificado. O serviço captura conteúdo gerado pelo usuário publicado em um conjunto diversificado de

plataformas de mídia social. Ao usar o serviço, o pesquisador primeiro insere um conjunto de palavras-chave junto com o idioma ou conjunto de idiomas para coleta de dados. Todo o conteúdo gerado pelos usuários e postado publicamente no Twitter, Instagram, Facebook, blogs, fóruns e YouTube é coletado em um banco de dados em tempo real. A ferramenta, portanto, permite que os pesquisadores coletem dados de maneira estruturada de um conjunto relativamente amplo de aplicativos de mídia social.

Foi indicado por Bogusz *et al.* (2020) que o fenômeno estabelecido de *crowdfunding*, conforme percebido pelos usuários de mídias sociais e explicado em postagens de mídia social, torna-se associado à tecnologia emergente de *blockchain*, *criptomoedas* e ICOs. A princípio, a *blockchain* era vista como algo interessante em si (Período 1), mas à medida que as ICOs arrecadavam cada vez mais dinheiro, ela passa a ser vista como uma potencial substituta para o *crowdfunding* (Período 2), antes de ser percebida como fenômeno altamente integrado (Período 3).

Uma revisão da literatura com diferentes periódicos que variam de 1994 a 2016 foi conduzida por Ullah (2021) a respeito do empreendedorismo global, inovação e sustentabilidade - teoria e prática, microempreendedorismo – ideia/projeto de empresa e reflexão crítica de teorias, conceitos e técnicas empreendedoras. As discussões foram divididas em três partes. A parte 1 declara empreendedorismo global, inovação e sustentabilidade - teoria e prática. O trabalho contém uma pesquisa a respeito do financiamento coletivo, *tradeoff* (troca) entre risco e retorno relacionado ao *crowdfunding*, *criptomoeda* e *blockchain*, impacto da *blockchain* e *criptomoeda*, desafios e questões de planejamento de negócios. A parte 2 vincula microempreendedorismo – ideia/projeto da empresa. A última parte inclui a reflexão crítica de teorias, conceitos e técnicas empresariais. Com isso, a segunda e terceira parte são mais voltadas para o viés empresarial, o foco de Ullah (2021) ficou voltado para a primeira parte.

Com base na revisão feita por Ullah (2021), o financiamento coletivo e a *criptomoeda* são a nova inovação no mundo dos negócios e usada para transações financeiras. A ideia inovadora deve ser baseada em demanda emergencial e urgente, como o uso de máscara e Equipamento de Proteção Pessoal (EPI) em todo o mundo.

Ao optar pelo *crowdfunding*, algumas aplicações podem acumular benefícios. Por exemplo, uma das recompensas creditadas ao *crowdfunding* é sua capacidade de atrair fundos potencialmente volumosos (MOLLICK, 2014). Um benefício adicional associado à opção pelo *crowdfunding* é a facilidade de acesso aos fundos que ele oferece às empresas. Tradicionalmente,

as empresas enfrentavam dificuldades para obter capital, o que atrasava as operações da empresa dependentes dos fundos. Por meio do *crowdfunding* de empréstimos de mercado, as empresas acessam fundos de opções alternativas melhores que os bancos. Uma opção alternativa é o *crowdfunding* baseado em recompensas, que premia os primeiros investidores com seus produtos ou serviços.

Com o objetivo de fornecer uma solução transparente, Khatter *et al.* (2021) pensaram em uma maneira para que as as pessoas que arrecadam fundos possam ver como sua doação está sendo utilizada e também ter uma opinião por meio do mecanismo de votação se o proprietário do projeto tem permissão para usar os fundos para uma solicitação específica. Apresentaram uma ideia de aplicação *web* baseada em *blockchain* na qual *startups*/empreendedores, serviços sociais podem expor sua ideia e buscar financiamento da massa. As pessoas que estão dispostas a arrecadar fundos podem doar através deste aplicativo. Com o modelo de aprovação de pedidos seria desenvolvido um sistema transparente em que os angariadores podem monitorizar a utilização dos fundos, garantindo assim confiança. Os fundos são mantidos pelo contrato inteligente.

O *crowdfunding* tradicional tem seus próprios desafios e limitações que precisam de atenção (AHMAD; RAHMAN, 2021). Entre as ameaças visíveis à plataforma de *crowdfunding* está a assimetria de informação (GEBERT, 2017) (NORDIN *et al.*,) onde as partes interessadas recebem informações desiguais ou uma parte recebe mais informações que a outra. Por conta da assimetria de informação, o público enfrenta vários problemas, como a dificuldade em obter informações sobre o modo que os captadores de recursos usam os fundos arrecadados. Diante disso, Ahmad e Rahman (2021) buscaram encontrar uma solução para tais problemas integrando os *Smart Contracts* da Ethereum à plataforma de *crowdfunding*. Ao aplicar o contrato inteligente, todas as transações feitas em *blockchain* serão registradas. Além disso, todos os dados que foram inseridos na rede *blockchain* estão protegidos de qualquer modificação. Portanto, esta solução permitirá que os contribuintes invistam com confiança no sistema, livre de fraudes e informações assimétricas.

Foi desenvolvida por Ahmad e Rahman (2021) uma aplicação chamada “Bantu”, construída como sistema independente e autocontido, onde sua arquitetura focou na separação de funcionalidades entre cada módulo. As principais funções do sistema exigem que o usuário tenha uma carteira externa que permita realizar transações Ethereum. Para cada transação ocorrida, a *blockchain* Ethereum registrará a transação, se ela falhou ou foi bem-sucedida. O banco de

dados é usado para armazenar as informações do usuário e as informações da campanha. Além disso, o banco de dados também é usado para fins de consulta.

Também foi realizada por Ahmad e Rahman (2021) uma comparação entre uma aplicação convencional (sem *blockchain*) e uma que utiliza a rede *blockchain*, buscando comparar alguns atributos. A Figura 19 mostra um comparativos entre o sistema de *crowdfunding* com implementação de *blockchain* e o sistema de *crowdfunding* tradicional. Os resultados foram comparados em termos de transparência das transações, imutabilidade dos dados, operações *Create - Read - Update - Delete* (CRUD), velocidade das transações e grau de simetria das informações. No geral, a implementação do *blockchain* no sistema de *crowdfunding* fornece maior transparência, o que pode reduzir a assimetria de informações e aumentar a confiança das partes interessadas em contribuir e arrecadar dinheiro por meio da plataforma de *crowdfunding*.

Figura 19 – Resultado da implementação de *blockchain* na plataforma de *crowdfunding* em termos de transparência, velocidade e simetria de informações.

Características	**Sistema de crowdfunding baseado em blockchain**	**Sistema de crowdfunding tradicional (sem implementação de blockchain)**
Transparência das transações	**Maior** porque cada transação é registrada na rede Ethereum e uma vez que os dados são inseridos, não podem ser alterados.	Embora cada transação possa ser registrada em banco de dados, não há garantia de que os dados não sejam alterados.
Operações CRUD	**Suporta somente** operações de criação e leitura .	Suporte para criar, ler, atualizar e excluir dados.
Velocidade das transações	**Mais lento** (15 a 30 segundos por operação de inserção).	Mais rápido (até 100.000 registros de inserção em 100 segundos)
Simetria da informação	**Maior** porque os dados no blockchain não podem ser facilmente adulterados.	Menor porque os dados no banco de dados podem ser alterados pelo administrador do banco de dados ou hacker.

Fonte: Adaptado de Ahmad e Rahman (2021).

Contribuindo com a literatura, Billert (2019) elencou requisitos orientados ao *design*, mostra implicações práticas ao construir um conceito de plataforma baseado em *blockchain* buscando facilitar um processo combinado de *crowdfunding* e *crowdworking* mais eficiente, reduzindo as transações. Para o desenvolvimento do conceito de plataforma, foram utilizados os três ciclos de pesquisa em ciência do *design*. Portanto, a primeira iteração foi realizada combinando os componentes mais importantes do sistema de *crowdfunding* e *crowdworking* com o uso de contratos inteligentes baseados em *blockchain*. Primeiramente, as informações necessárias sobre o ciclo de rigor, ou ciclo de conhecimento para o desenvolvimento do conceito

através do ciclo de *design* foram transferidas da base de conhecimento. A base de conhecimento contém conhecimento sobre *crowdfunding*, *crowdsourcing* e contém também informações sobre os contratos inteligentes baseados em *blockchain*. Após a primeira iteração, a base de conhecimento foi estendida pela adaptação do processo combinado de *crowdfunding* e *crowdworking*. O conhecimento especializado do ecossistema de *crowdsourcing* e exemplos de aplicativos de contratos inteligentes baseados em *blockchain* foram retirados do ambiente e repassados por meio do ciclo de relevância para a coleta dos requisitos.

O trabalho de Billert (2019) visou reduzir a transação em um processo combinado de *crowdfunding* e *crowdworking* usando os novos contratos inteligentes baseados em *blockchain*, construindo e avaliando uma plataforma futura em vários ciclos. No processo atual, um *crowdsourcer* usa uma plataforma de *crowdfunding* para buscar potenciais investidores para apoiar o projeto iniciado. Em seguida, o *crowdsourcer* submete a tarefa a uma plataforma de *crowdworking* com ou sem a influência dos investidores. No novo processo futuro, a busca por investidores e *crowdworkers* é combinada e as respectivas condições são definidas em um contrato inteligente. Isso minimiza o número de interações entre as partes interessadas individuais e, ao mesmo tempo, reduz os custos das transações. Além disso, terceiros não estão mais envolvidos e são desnecessários. A Figura 20 mostra um esboço dos processos atuais e futuro.

Figura 20 – Processo de *crowdfunding* e *crowdworking* combinados atual (esquerda) e futuro (direita).

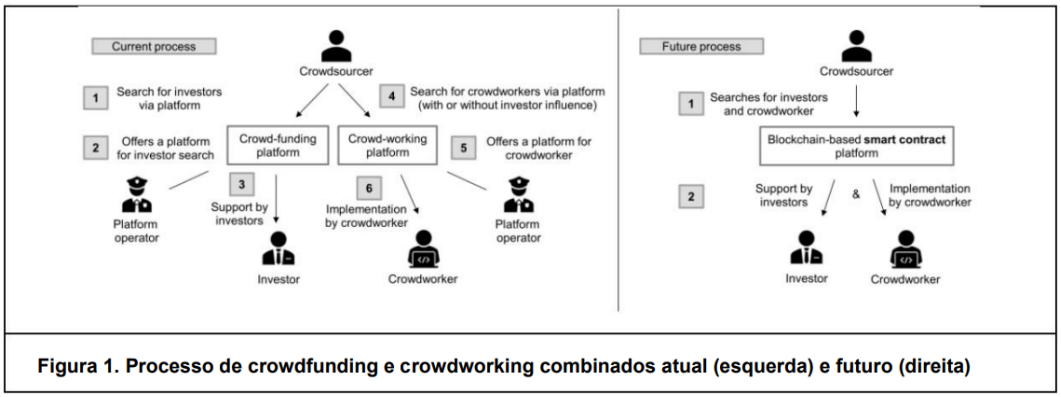


Figura 1. Processo de crowdfunding e crowdworking combinados atual (esquerda) e futuro (direita)

Fonte: Adaptado de Billert (2019).

As Tabelas 3 e 4 exibem um sumário dos critérios de comparação entre os trabalhos relacionados e a proposta. Os critérios foram: (i) Desenvolveu uma aplicação?; (ii) Modelou a aplicação?; (iii) Apresentou vantagens da *blockchain* com *crowdfunding*?; (iv) Propôs arquitetura?; (v) Que ferramenta de *blockchain* foi utilizada?; e (vi) Executou alguma análise de custos?;

Quanto à criação/desenvolvimento de uma aplicação que utilize recursos da *blockchain* para utilização de *crowdfunding*, 2 trabalhos desenvolveram aplicações e 8 não. Outro aspecto é se modelou a aplicação, apenas em 3 trabalhos se constatou o uso de modelagem. Em um deles não não se sabe ao certo se foi desenvolvida a aplicação, mas foi feito uma modelagem completa da aplicação, elencando tecnologias a serem utilizadas no seu desenvolvimento. Todos os trabalhos fazem menções e defendem as vantagens que a tecnologia *blockchain* pode proporcionar ao se unir com o *crowdfunding*.

A proposição da arquitetura é importante, com ela é possível demonstrar certo nível de maturidade na solução e tecnologia. Quatro trabalhos propuseram em níveis variados, sendo que em alguns descrevendo apenas com texto. A maioria dos trabalhos utiliza a rede Ethereum como *blockchain* com ênfase em seus contratos inteligentes. Houve também menções ao Bitcoin, mas apenas citando-o. Em relação a execução de análise de custos feitos nas aplicações desenvolvidas utilizando *blockchain*, nenhum dos trabalhos realizou. Em 2 trabalhos foram efetuados testes, onde foram levados em consideração características como tempo de resposta do sistema que usa *blockchain* em relação a outro sistema tradicional de *crowdfunding*. Teste de auditoria de transações também foi foco em um dos trabalhos.

Tabela 3 – Comparação entre trabalhos relacionados

Artigo	**Criou aplicação**	**Modelou aplicação**	**Apresenta vantagens entre *blockchain/crowdfunding***
Zhu e Zhou (2016)	Não	Não	Sim
Martino *et al.* (2019)	Não	Não	Sim
Lee e Rahim (2021)	Sim	Sim	Sim
Ashari *et al.* (2020)	Não	Não	Sim
Creta e Tenca (2021)	Não	Não	Sim
Bogusz *et al.* (2020)	Não	Não	Sim
Ullah (2021)	Não	Não	Sim
Ahmad e Rahman (2021)	Sim	Sim	Sim
Billert (2019)	Não	Sim	Sim
Khatter *et al.* (2021)	Não	Sim	Sim
Este Trabalho	**Sim**	**Sim**	**Sim**

Fonte: o autor.

Os trabalhos fazem menções a algumas ideias para construção de trabalhos futuros, mas com particularidades para seus próprios contextos. Por exemplo, Do ponto de vista de funcionalidades, implementar uma barra de pesquisa para ajudar na busca de projetos, projetar uma interface melhor e fazer com que os comentários sejam editáveis (LEE; RAHIM, 2021). Do ponto de vista de tecnologia, implementar a proposta criada no trabalho visando fornecer

Tabela 4 – Comparação entre trabalhos relacionados

Artigo	Propôs arquitetura	Ferramenta	Análise de Custos
Zhu e Zhou (2016)	Não	Não informado	Não
Martino *et al.* (2019)	Não	Não informado	Não
Lee e Rahim (2021)	Sim	Ethereum	Não
Ashari *et al.* (2020)	Não	Não informado	Não
Creta e Tenca (2021)	Não	Não informado	Não
Bogusz *et al.* (2020)	Não	Não informado	Não
Ullah (2021)	Não	Não informado	Não
Ahmad e Rahman (2021)	Sim	Ethereum	Não
Billert (2019)	Sim	Não informado	Não
Khatter *et al.* (2021)	Sim	Não informado	Não
Este Trabalho	**Sim**	**Ethereum**	**Sim**

Fonte: o autor.

um ambiente que facilite o financiamento coletivo (KHATTER *et al.*, 2021). Do ponto de vista de pesquisa, o trabalho pode ser estendido olhando para o estado da arte em outros países além da Itália (CRETA; TENCA, 2021). Por fim, do ponto de vista das possibilidades, estudos futuros podem envolver a introdução de outra tecnologia que pode ser usada em *blockchain* para consultar dados e realizar mais pesquisas para melhorar a experiência geral do usuário sobre como as transferências de Ethereum podem ser aceleradas (AHMAD; RAHMAN, 2021).

Portanto, a proposta desta dissertação é implementar todos os critérios dispostos nas Tabelas 3 e 4, e também fazer uso da tecnologia *blockchain* da rede Ethereum. Uma arquitetura junto com aplicação será desenvolvida buscando atender às necessidades do domínio do *crowdfunding*. Foi realizado o planejamento de um projeto de experimentos, com métricas de tempo e valores financeiros.

Em relação às diferentes arquiteturas apresentadas na Seção 2.5, diferencia-se a arquitetura proposta neste trabalho das demais pelo fato de haver uma união de camadas de forma simples e adequada. A ideia é propor uma arquitetura mais enxuta e com flexibilidade para se implementar. Foi escolhido não utilizar a camada de banco de dados convencional, mas entende-se que ela pode ser composta por qualquer tipo de banco de dados de maneira externa à *blockchain*. O protótipo da aplicação seguirá essa nova arquitetura em seu desenvolvimento.

4 ARQUITETURA E APLICAÇÃO CROWDCOIN

Este capítulo trata de apresentar a arquitetura proposta para um sistema *crowdfunding* que utiliza a tecnologia *blockchain*. A Seção 4.1 apresenta a arquitetura proposta neste trabalho. Na Seção 4.2, são apresentados os requisitos encontrados em aplicações tradicionais de financiamento coletivo.

4.1 Arquitetura

Observar a *blockchain* como um componente de software ajuda no entendimento dos impactos arquitetônicos importantes para o desempenho e na qualidade de atributos como segurança, privacidade, rastreabilidade e escalabilidade (ABREU, 2020). Como um componente, *blockchain* tem propriedades e limitações únicas, sendo complexo, ter componentes de software baseados em rede que podem fornecer dados, serviços de armazenamento, computação e comunicação (XU *et al.*, 2019).

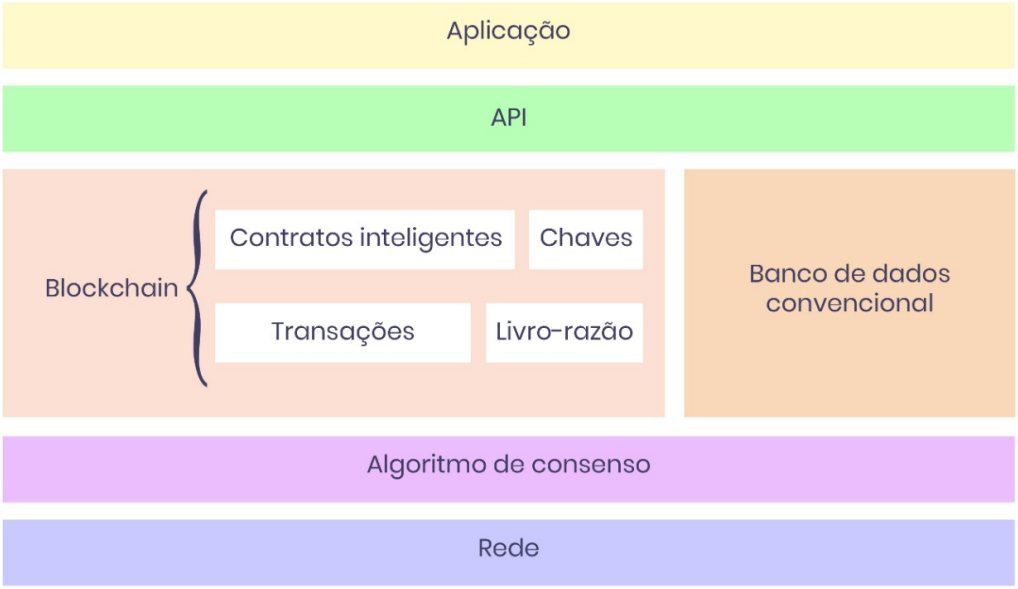
Seguindo a arquitetura encontrada no trabalho de Abreu *et al.* (2020) na Figura 21 são mostradas todas as camadas exploradas por este trabalho. Observa-se também a divisão de camadas e componentes da aplicação. Os dados a serem armazenados foram todos guardados nos blocos da *blockchain*. A listagem a seguir descreve seus elementos:

- **Aplicação:** nesta camada são encontradas as aplicações que utilizam-se de recursos da *blockchain*. Essas aplicações facilitam a interação com os usuários por possuírem interface gráfica, podendo também incluir lógica de negócios e dados;
- ***Application Programming Interface* (API):** auxilia a *blockchain* a trocar informações com elementos de fora da rede. A comunicação é feita através de APIs seja para consultar ou escrever dados;
- ***Blockchain*:** a camada de *blockchain* fica responsável por armazenar e compartilhar dados nos blocos, assim como também executar contratos inteligentes. Está subdividida nos seguintes componentes:
  - **Contratos Inteligentes:** um contrato inteligente se assemelha a um contrato físico acordado em cartório em forma de programa criado pelo usuário, que é implantado e executado na *blockchain* assim podendo conter as regras do negócio. Podendo ser desenvolvidos também como parte de uma transação;
  - **Transações:** este componente possui a capacidade de gerar e validar blocos em sua

ordem correta;

  - **Chaves:** o gerenciamento de chaves permite aos utilizadores da *blockchain* assinatura de forma digital de suas transações com o uso de suas chaves privadas;
  - **Livro-razão:** componente que representa a *blockchain* distribuída livro-razão;
- **Algoritmos de consenso:** esta camada ajuda a resolver o problema de confiança com implementações para gerar a ordem da cadeia de blocos e validações pelos nós da rede; e
- **Rede:** camada responsável pela comunicação entre os nós, incluindo descoberta, propagação de transações e blocos.

Figura 21 – Arquitetura de Referência.



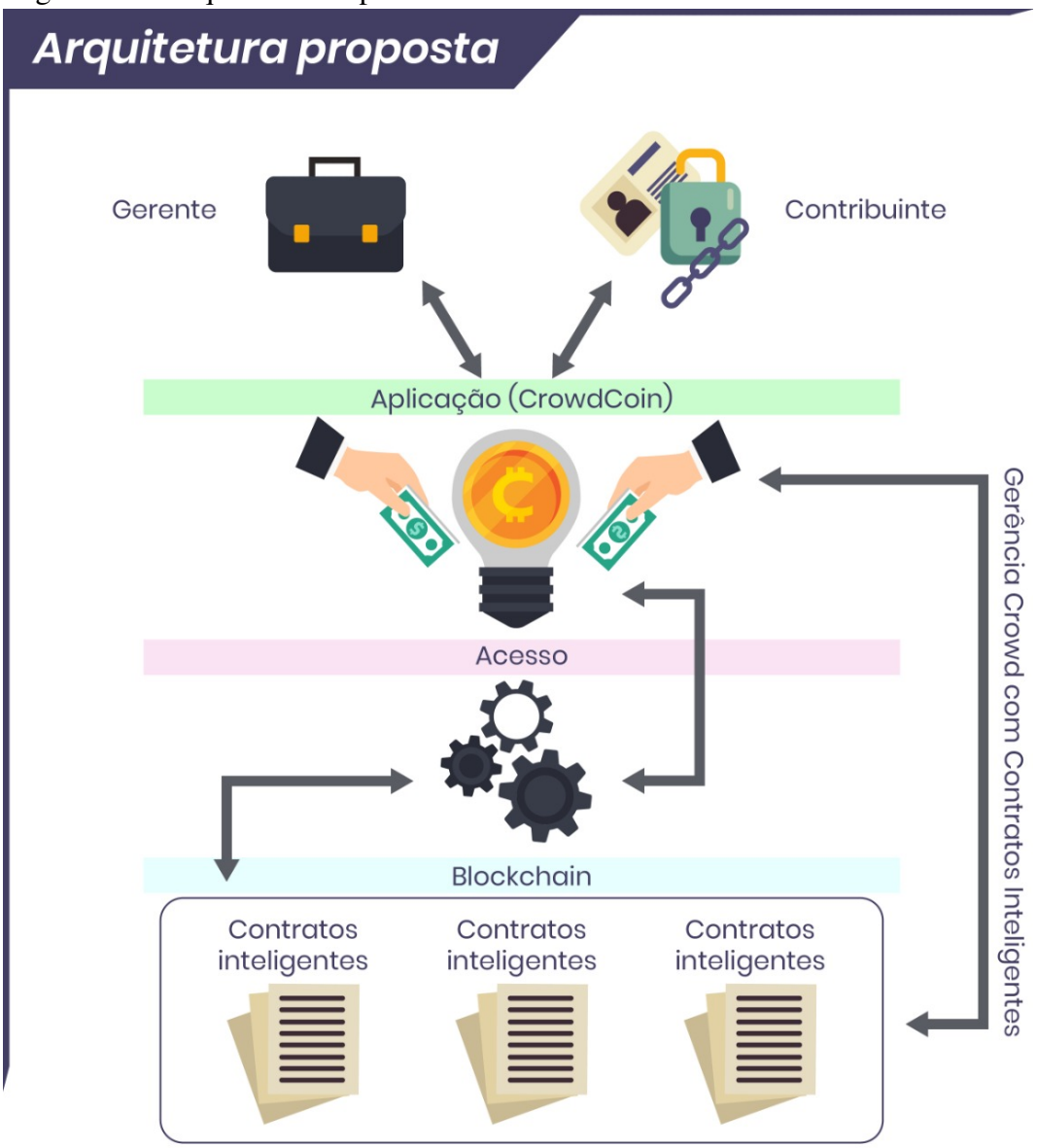
Fonte: Adaptado de (ABREU *et al.*, 2020)

A arquitetura de *blockchain* proposta por este trabalho utiliza uma interface *web* para fazer a comunicação entre os participantes de um dito projeto, com a utilização de contratos inteligentes. Um contrato geral é criado de início e nele contém as informações de quantos projetos existem, quantas pessoas fizeram doações para tal projeto. Cada projeto se torna um contrato inteligente. A aplicação executa as transações utilizando um *plugin* Metamask chegando até a rede *blockchain* que utiliza o processo de consenso em uma rede com vários nós, garantindo a integridade, rastreabilidade das informações armazenadas na *blockchain*.

Ao construir a abordagem baseada em *blockchain*, foi observado que existem vários componentes específicos da área de *blockchain*. A partir disso, se fez necessário propor e usar um novo modelo arquitetônico como uma referência.

A Figura 22 mostra a arquitetura dividida em três camadas:

Figura 22 – Arquitetura Proposta.



Fonte: o autor.

- **Camada de aplicação:** encontra-se a aplicação, no caso deste trabalho chamada CrowdCoin, onde é possível a interação com usuários fora do sistema;
- **Camada Acesso:** composta pelas tecnologias necessárias para criar acesso à *blockchain*; e
- **Camada *Blockchain*:** onde residem os contratos inteligentes, com os dados de projetos com seus financiadores.

A primeira camada é composta pela aplicação CrowdCoin, responsável pela comunicação direta com os criadores de projetos e também os financiadores, os principais *stakeholders* definidos neste trabalho. Um contrato "fábrica" é o contrato principal da aplicação, ele faz a criação dos novos contratos de acordo com os dados cadastrados para uma nova campanha e mantém uma lista contendo todos os endereços *hash* dos contratos criados. Qualquer usuário

pode criar o seu próprio projeto no contrato principal, inserindo assim dados na *blockchain*. Para cada projeto, existe um contrato diferente. O custo pela criação de novos contratos fica por conta do mentor desse novo projeto.

Os financiadores podem entrar em cada um dos contratos e ver informações como: quantidade de financiadores que já contribuíram, quantidade de dinheiro arrecadado no contrato, a identificação de quem é o gerente do projeto, quantidade de requisições de compra tem no contrato e valor mínimo para se fazer parte do projeto. Ao participar, os financiadores ganham o poder de votar nas requisições feitas pelo gerente a fim de usar parte ou o total do dinheiro acumulado. Esse voto foi definido, neste trabalho, como igualitário para todos que investiram em determinada campanha, cada voto tem o mesmo peso independente do valor investido. Para que uma requisição seja atendida, será preciso que ela consiga a aprovação de mais de 50% dos investidores.

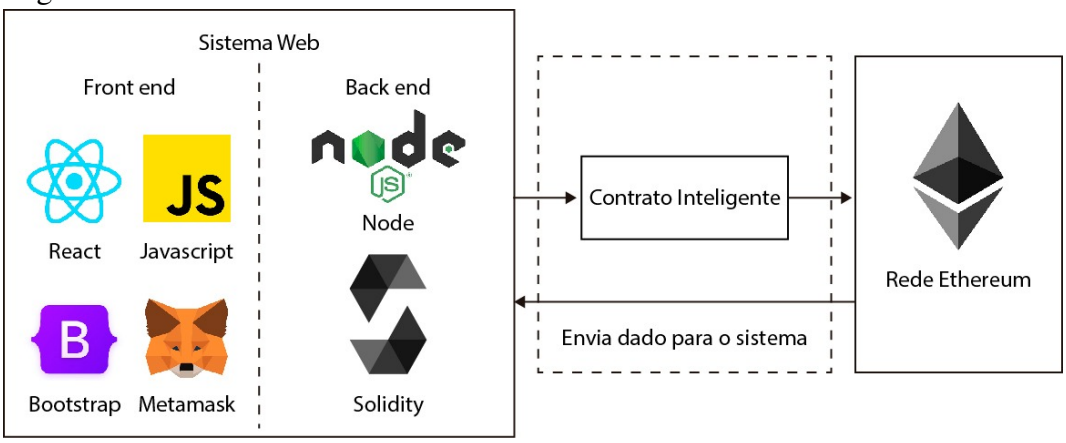
Na segunda camada existem algumas tecnologias utilizadas para interação do *front-end* da aplicação com a camada de *blockchain*. Ao criar uma aplicação que se comunique com *blockchain* é necessário utilizar configurações específicas no *front-end*. Esta camada tem correspondência com a camada API da arquitetura de referência, dispondo de tecnologias que auxiliam os desenvolvedores a acessarem recursos necessários na interação da aplicação com a *blockchain*.

A terceira camada do ambiente é formada pela *blockchain* que armazena os dados dos projetos, que serão usados na visualização dos possíveis financiadores. Esta camada armazena os contratos inteligentes, que definem as regras de como um usuário pode fazer parte do projeto, como o dinheiro será gasto. Estas regras de contratos inteligentes são informadas dentro do aplicativo CrowdCoin.

Esta abordagem funciona como um novo modelo de negócios para o *crowdfuding*, oferecendo uma melhor percepção por parte dos financiadores, de como o dinheiro investido foi ou está sendo utilizado. Qualquer usuário pode ver a lista de requisições feitas pelo gerente. Nesta lista é exibida a quantidade de pessoas que as aprovaram e também a sua situação, que pode ser em aprovação ou finalizada. Uma requisição finalizada significa que a quantidade de ether nela descrita foi enviada para o fornecedor também descrito.

A Figura 23 representa as tecnologias utilizadas na arquitetura proposta de sistema *web*. No capítulo seguinte essas tecnologias são descritas. Existe uma divisão entres as tecnologias em três partes:

Figura 23 – Contexto do Sistema.



Fonte: adaptado de (AHMAD; RAHMAN, 2021).

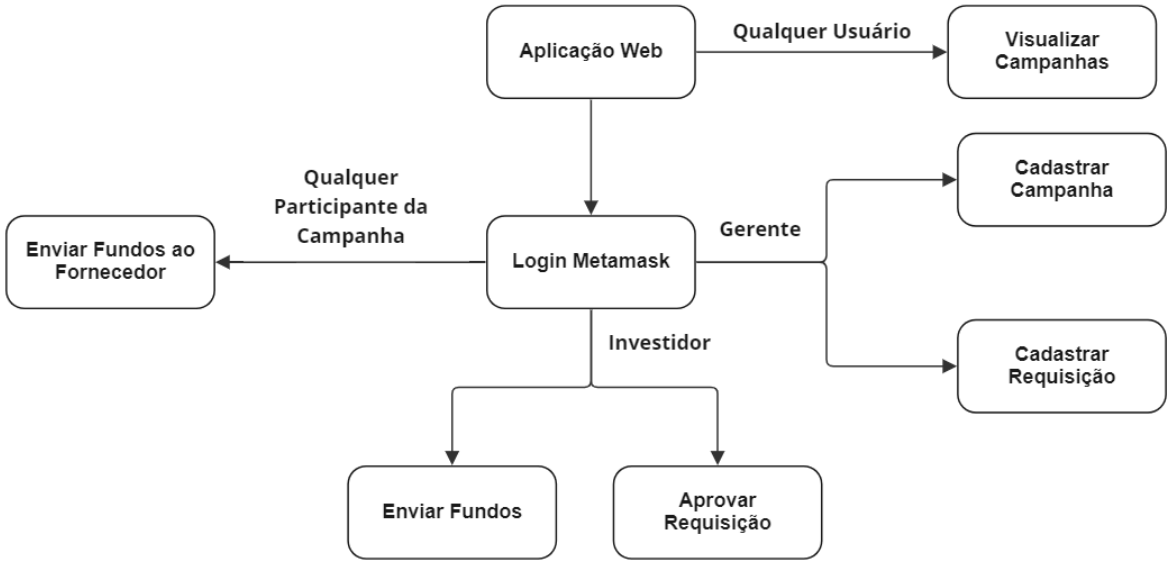
- ***Front-end*:** React que é a biblioteca mais popular do JavaScript e é usada para construir uma interface de usuário; Bootstrap é um framework CSS utilizado no front-end de aplicações web, estiliza as páginas e adiciona funcionalidades tornando-se mais do que um visual do site; Metamask entra como carteira digital e faz as interações da aplicação com a rede *blockchain*.
- ***Back-end*:** Node que é um ambiente de execução JavaScript permitindo executar aplicações desenvolvidas com a linguagem de forma autônoma, sem depender de um navegador; Solidity é a linguagem de programação de alto nível, com a sua utilização é possível criar aplicações com contratos inteligentes na Ethereum.
- **Rede *blockchain***: A rede Ethereum armazena os contratos inteligentes e os dados das campanhas além de receber as interações dos usuários.

O fluxo da aplicação proposta está representado no diagrama da Figura 24 melhorando o entendimento dos recursos da aplicação.

Esse fluxo mostra uma visão geral da aplicação sem a dependência das tecnologias utilizadas. Os detalhes de cada etapa estão descritos a seguir:

- **Aplicação Web:** Inicialmente é preciso acessar a aplicação *web*, a partir desta é possível fazer uso das funcionalidades do ambiente proposto;
- ***Login* Metamask:** Para poder fazer interações com o sistema é necessário que o usuário realize o *login* no Metamask;
- **Visualizar Campanhas:** Todo e qualquer usuário pode ver a lista de campanhas disponíveis, assim como os detalhes de cada uma de forma individual;
- **Cadastrar Campanha:** Após login no Metamask qualquer usuário pode criar campanhas novas e ao fazer isso torna-se o gerente das mesmas;

Figura 24 – Visão geral do fluxo da aplicação proposta



Fonte: o autor.

- **Cadastrar Requisição:** Com a campanha criada e com fundos suficientes para início do projeto, apenas o gerente da campanha pode gerar requisições para compra de materiais, por exemplo, a serem utilizados em seu projeto;
- **Enviar Fundos ao Fornecedor:** Após votação feita pelos investidores da campanha, sendo aprovada a requisição, qualquer usuário pertencente a campanha pode finalizar a requisição e assim enviar o valor nela definido para a carteira especificada;
- **Enviar Fundos:** Usuários interessados em investir em uma campanha tornam-se investidor da mesma ao enviar fundos de sua carteira para o contrato inteligente da campanha; e
- **Aprovar Requisição:** Apenas usuários que enviaram fundos para determinada campanha podem participar da votação para aprovação de requisições feitas no intuito de utilizar os fundos arrecadados e que ficam "presos" no contrato inteligente.

Os papeis desempenhados e suas possíveis ações dentro da aplicação são divididos em três:

- **Administrador do Sistema:** esse usuário é o que inicia a aplicação, ele quem faz a criação do contrato "fábrica" e o disponibiliza na rede;
- **Usuário - Gerente de Projeto:** o gerente de projetos é o idealizador de uma campanha e é ele quem faz o cadastro do seu próprio projeto; e
- **Usuário - Investidor:** usuário que faz visualiza as informações das campanhas no intuito de ingressar em uma ou em mais campanhas

4.2 Requisitos da Aplicação

Para o levantamento de requisitos da aplicação proposta foi tomado como base sites de *crowdfunding* como o Kickstarter[1], que é um dos sites mais famosos encontrado em uma pesquisa rápida. O CrowdCoin é uma simulação de uma possível solução para que qualquer pessoa possa investir em campanhas de financiamento coletivo com um pouco mais de controle sobre o projeto. A ideia desse trabalho é oferecer um pouco mais de segurança para quem quer investir, deixando mais claro o uso do dinheiro arrecadado. Os Requisitos Funcionais (RF) da aplicação estão apresentados a seguir:

- **RF1 - Cadastro de usuário:** A aplicação deve receber dados do usuário em forma de formulário e mantê-los em um banco de dados para futuras utilizações;
- **RF2 - Editar usuário:** Recuperar dados do usuário possibilitar alterações necessárias após a sua criação em atributos como email, telefone de contato;
- **RF3 - Cadastro da campanha:** O cadastro de um novo projeto "campanha" deve receber dados como descrição, video explicativo, meta de arrecadação, contribuição mínima, local geográfico da execução do projeto, etc. Guardá-las em um banco de dados;
- **RF4 - Visualizar dados da campanha:** Exibir todas as informações da campanha recuperadas do banco de dados, para visualização dos usuários da aplicação;
- **RF5 - Editar dados da campanha:** Recuperar dados da campanha possibilitar alterações necessárias após a sua criação em atributos como atualização de meta de arrecadação, valor da contribuição mínima;
- **RF6 - Enviar fundos:** Usuário que mostrou interesse em entrar na campanha pode enviar a contribuição mínima exigida para poder fazer parte do projeto;
- **RF7 - Receber comentários:** Usuário podem fazer comentários a respeito de campanhas específicas dentro das mesmas, informando sua experiência com o projeto ou qualquer outro tipo de informação em forma de texto;
- **RF8 - Receber perguntas:** Usuário podem fazer perguntas ao gerente "dono" da campanha seja buscando esclarecimento ou sanando dúvidas, em formato texto.

Os Requisitos Não Funcionais (RNF) da aplicação estão descritos a seguir:

- **RNF1:** A aplicação deve ter compatibilidade com os navegadores que suportem a instalação da extensão MetaMask (Chrome, Firefox, Opera e Brave);
- **RNF2:** A aplicação deve se adaptar ao tamanho de tela que está sendo acessada de maneira

[1] https://www.kickstarter.com/ Acesso em: 08 ago. 2022

responsiva;

- **RNF3:** Os dados da aplicação devem ser mantidos em segurança, podendo serem acessados por meio de senhas de autorização;
- **RNF4:** A aplicação deve fornecer um fluxo de fácil compreensão para facilitar a aprendizagem e memorização;
- **RNF5:** A aplicação deve conter opção para alterar o idioma para português ou inglês;
- **RNF6:** O ambiente da aplicação deve ser dividido em blocos de funcionalidades para facilitar a manutenção;
- **RNF7:** A aplicação deve carregar as informações na tela de maneira rápida e eficiente fornecendo uma fluidez ao usuário;
- **RNF8:** A aplicação deve ficar disponível a todo momento 24 horas por dia, em caso de uma queda do servidor um novo deve ser instanciado de imediato;
- **RNF9:** Devem ser feitos backups semanais e mensais dos dados a fim de resguardar os dados;
- **RNF10:** Respeitar as regras exigidas pela LGPD - Lei Geral de Proteção de Dados.

5 DESENVOLVIMENTO E AVALIAÇÃO DE DESEMPENHO DO PROTÓTIPO DA ARQUITETURA PROPOSTA UTILIZANDO CONTRATOS INTELIGENTES

Neste capítulo é apresentada uma implementação que utiliza contratos inteligentes baseados na plataforma Ethereum gerando um protótipo do ambiente da arquitetura proposta. A Seção 5.1 comenta os detalhes da implementação e também das tecnologias utilizadas no protótipo. A Seção 5.2 apresenta o contexto da aplicação e cenários de uso. As Seções 5.3 e 5.4 exibem os resultados alcançados com a solução proposta. A Seção 5.5 apresenta um modelo analítico desenvolvido sobre os resultados obtidos. Por fim, a Seção 5.6 faz uma análise e discute pontos gerais sobre os resultados obtidos.

5.1 Implementação da Solução Proposta

Para desenvolver uma solução baseada em *blockchain*, foram feitas algumas análises em tecnologias e plataformas passíveis de uso. Contudo, a plataforma selecionada para este trabalho foi a Ethereum. Nessa plataforma existe o conceito de contrato inteligente tornando-se uma *blockchain* mais generalista, expandindo as transações para operações computacionais que podem ser programadas para executar determinadas regras (CHRISTIDIS; DEVETSIKIOTIS, 2016).

5.1.1 Infraestrutura

No mercado atual existem uma variedade de redes *blockchain* que possibilitam o uso de contratos inteligentes. Redes como: Hyperledger [1] - que é um sistema *open source* que foi desenvolvido pela Linux Foundation, Counterparty [2] - nesta plataforma existe a inclusão de dados às transações de Bitcoin e Polkadot [3] - conta com um protocolo *blockchain* alternativo, ficou famoso pela sua capacidade para hospedar *blockchains* paralelas, que com isso possibilitam realizar mais transações que o padrão. Outros exemplos são Tron [4], NEO [5], Stellar [6], Ripple [7]. A Ethereum foi selecionada para esse trabalho devido a indicação de utilização para execução de contrato inteligente no contexto da *blockchain* (KORPELA *et al.*, 2017). Ela possui a *Ethereum*

[1] https://www.hyperledger.org/ Acesso em: 08 ago. 2022
[2] https://counterparty.io/ Acesso em: 08 ago. 2022
[3] https://polkadot.network/ Acesso em: 08 ago. 2022
[4] https://tron.network/ Acesso em: 08 ago. 2022
[5] https://neo.org/ Acesso em: 08 ago. 2022
[6] https://www.stellar.org/ Acesso em: 08 ago. 2022
[7] https://ripple.com/ Acesso em: 08 ago. 2022

Virtual Machine (EVM) (WOOD, 2019), onde foi criada uma aplicação (contrato inteligente), que funciona exatamente como programado sem qualquer possibilidade de censura ou fraude, pois o contrato é imutável. Outro fato importante na escolha, foi existir uma variedade materiais disponibilizados na Internet a respeito do desenvolvimento dos contratos inteligentes.

As tecnologias associadas a Ethereum e utilizadas neste trabalhos foram escolhidas por critério de familiaridade ou facilidade de uso. Elas são elencadas em forma de lista a seguir:

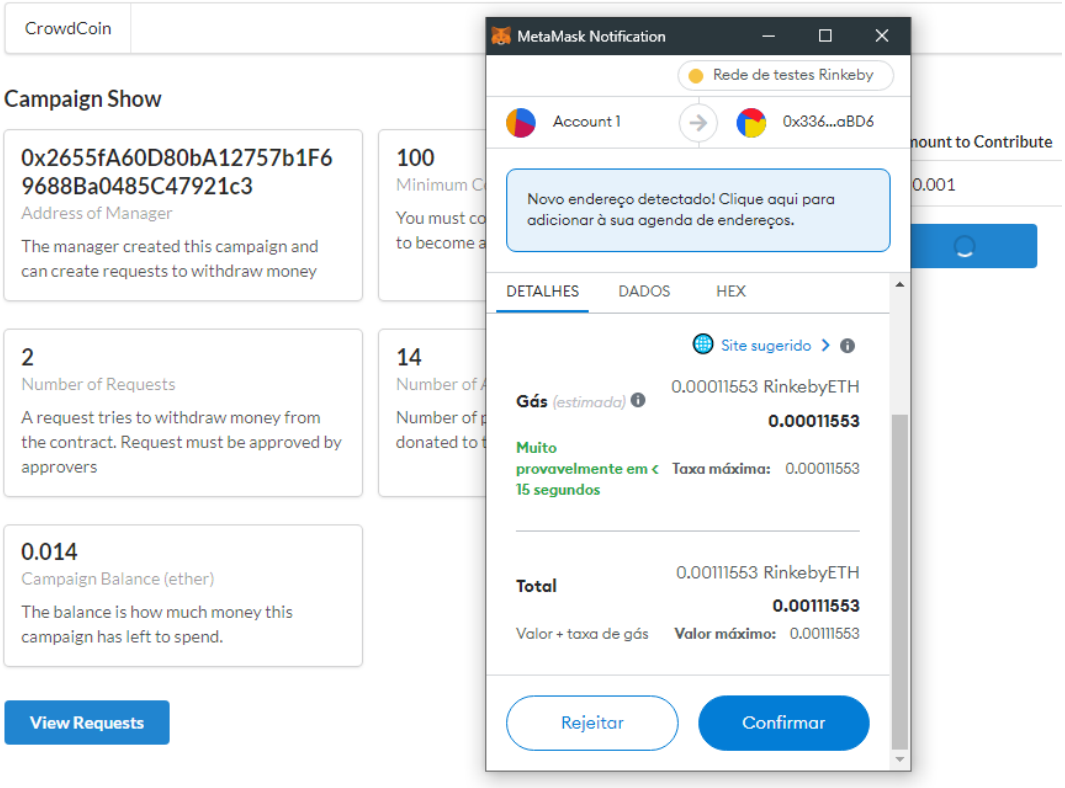
- **Solidity:** linguagem utilizada pela rede Ethereum no desenvolvimento e construção de contratos inteligentes;
- **IDE Remix:** IDE *online* que auxilia o desenvolvimento de contratos inteligentes, com a possibilidade de fazer testes e validações de contratos inteligentes;
- **Rinkeby:** uma rede pública da Ethereum usada para testes e validação de aplicações. Nela é feito o uso da *criptomoeda* ether "falso", sem valor financeiro, ajudando na viabilização de testes em um ambiente mais próximo do real;
- **Infura:** é um serviço de infraestrutura disponível na *blockchain* da Ethereum que possibilita a interação com o contrato inteligente criado, pois para que haja interação é preciso uma conexão inicial com um nó da rede Ethereum. O Infura provê uma camada de abstração para diversos nós na rede da *blockchain* Ethereum;
- **API Web3.js:** documentação da Web3 JavaScript Dapp API é usada para desenvolver aplicações que são descentralizadas assim como a rede *blockchain*;
- **Visual Studio Code:** um editor de código-fonte bastante utilizado no desenvolvimento da interface *web* de aplicações;
- **HTML5/CSS3/Bootstrap:** tecnologias usadas no desenvolvimento do *front-end* da aplicação;
- **Metamask:** *plugin* disponível para navegadores (Chrome, Firefox, Opera e Brave) que possibilita o acesso às plataformas *blockchain* como a Ethereum. Funciona como uma carteira virtual que recebe ether e interage com a rede sem a necessidade de ter uma cópia da *blockchain* instalada no ambiente local;
- **Etherscan:** uma ferramenta que possibilita explorar uma *blockchain*, permitindo uma análise de transações na plataforma Ethereum. Mostra informações dos blocos de transações feitas na rede.

A utilização do Metamask [8] se fez obrigatória neste trabalho, devido a maneira que a

[8] https://metamask.io/ Acesso em: 08 ago. 2022

aplicação foi implementada. Ele é usado para fazer as validações a respeito das transações, se o usuário aceita ou não enviar aquela transação para a rede. Um resumo do que será gasto com a transação prestes a ser enviada é exibido. Junto aos detalhes dos custos da transação também é exibido e são mostrados dois botões, um "Confirmar" e outro "Rejeitar" usados pelos usuários ao decidirem se vão ou não dar continuidade a tal transação. A Figura 25 exibe um exemplo para a aprovação de transação pelo Metamask.

Figura 25 – Metamask - Operação de Contribuição em uma Campanha



Fonte: o autor.

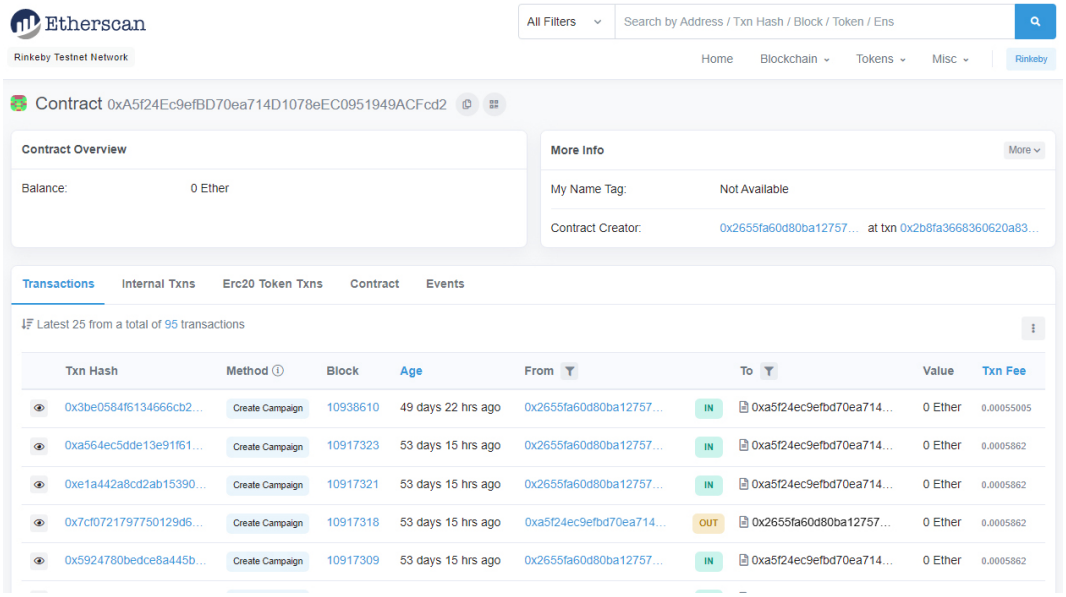
A utilização do Etherscan [9] auxilia na obtenção da transparência oferecida pela *blockchain*. Com essa ferramenta é possível saber todas as transações que aconteceram durante toda a vida do contrato inteligente ou de alguma carteira. A Figura 26 mostra a visualização oferecida pela ferramenta a qualquer usuário que deseja fazer tal verificação. Para fazer a busca é necessário digitar o código *hash* do contrato ou da carteira que se deseja verificar. As informações obtidas são exibidas em forma de tabela com linhas e colunas. Destacando-se as principais colunas obtém-se:

- ***Txn Hash*:** exibe o link com *hash* da transação, ao clicar o usuário é direcionado para os detalhes da transação;

[9] https://rinkeby.etherscan.io/ Acesso em: 08 ago. 2022

- ***From*:** exibe o *hash* da carteira ou contrato de onde o ether foi enviado, também é mostrado um indicador "*IN*" significando que houve entrada de ether ou "*OUT*" representando a saída do ether;
- ***To*:** exibe o *hash* da carteira ou contrato de onde o ether foi recebido; e
- ***Value*:** mostra o valor em ether enviado ou recebido pela transação.

Figura 26 – Etherscan

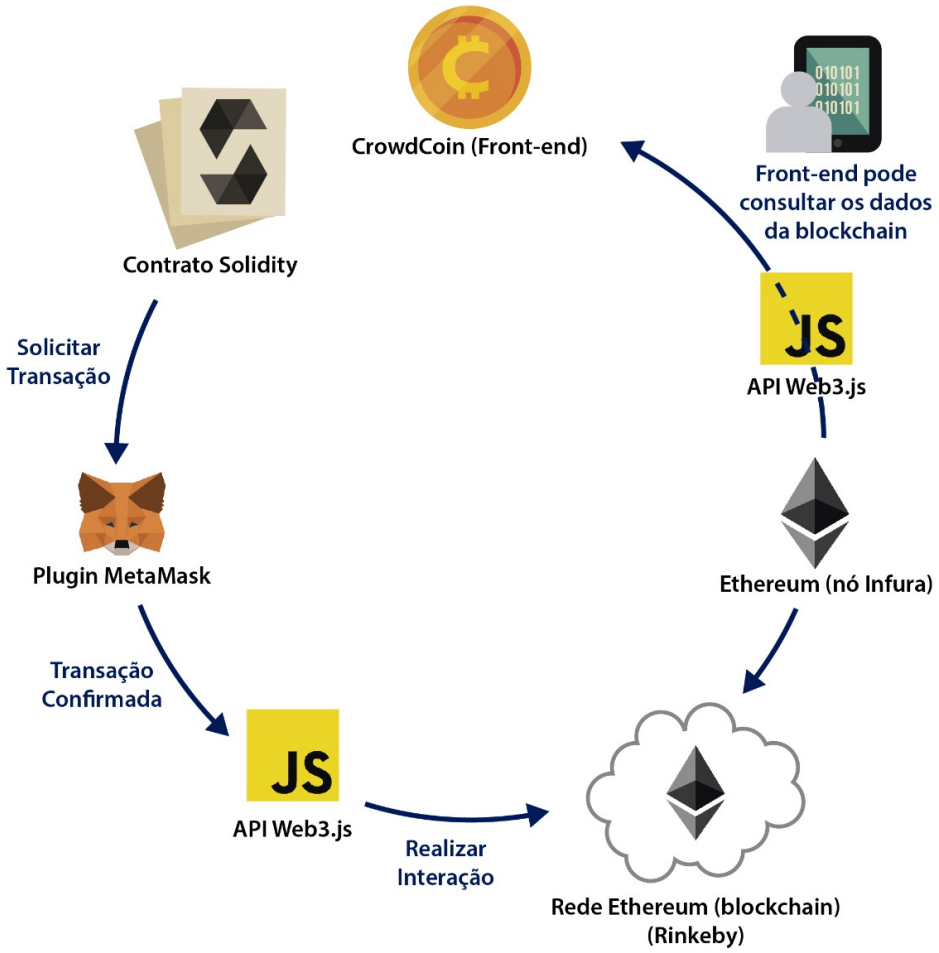


Fonte: o autor.

A Figura 27 possibilita obter uma visão completa do fluxo de execução das tecnologias utilizadas ao executar as transações dentro do protótipo que foi desenvolvido. Na aplicação, qualquer usuário pode usar a *blockchain* para enviar dados e também recuperá-los.

O objetivo principal do *front-end* é a interação com o usuário, possibilitando a interação direta com o contrato inteligente criado. Também são realizadas no *front-end* as configurações necessárias para intereagir com a rede Ethereum, assim como também a maneira de interagir com o contrato inteligente e seus métodos. Para que exista esse funcionamento, o código em JSON que corresponde ao código compilado do Solidity e a especificação da *Apliccation Binary Interface* (ABI) do contrato devem ser informados no *front-end*. Quando uma transação é iniciada na aplicação, ela será executada apenas depois da confirmação da transação feita pelo *plugin* MetaMask. Caso a resposta recebida seja positiva, a API Web3.js interpreta o código em Solidity que está no formato JSON e inicia a comunicação com a rede Rinkeby da Ethereum. Essa rede possui o processo de consenso PoW e o realiza com a participação dos nós da *blockchain* a fim de minerar um novo bloco para serem armazenados todos dos dados

Figura 27 – Fluxo de execução das tecnologias utilizadas



Fonte: o autor.

relacionados à transação solicitada. Logo depois de todo esse processo é possível recuperar os dados para consulta sem nenhuma restrição de acesso na *blockchain* utilizando o endereço do nó Infura informado no *front-end*. A utilização do *plugin* MetaMask é dispensada para fins de consulta de dados existentes na *blockchain*. Após as informações serem inseridas na *blockchain*, qualquer usuário pode consultar sem a obrigação de realizar qualquer tipo de cadastro ou instalação como pré-requisito para acessar os dados.

5.1.2 Contratos Inteligentes

Para o protótipo foi desenvolvido um contrato inteligente que funciona como uma fábrica de contratos inteligentes, onde cada campanha criada se torna um contrato inteligente independente dentro da *blockchain*. O Código 1 exibe a parte principal do código-fonte, na linguagem Solidity, do contrato inteligente utilizado na aplicação proposta por este trabalho. O

código completo do contrato encontra-se disponível em um repositório[10].

```
pragma solidity ^0.4.25;
contract CampaignFactory {
    address [] public deployedCampaigns;
    function createCampaign(uint minimum) public {
        address newCapaign = new Campaign(minimum, msg.sender);
        deployedCampaigns.push(newCapaign);
    }
    function getDeployedCampaigns() public view returns (address[]) {
        return deployedCampaigns;
    }
}
contract Campaign {
    ...
    }
    function Campaign(uint minimum, address creator) public {
        manager = creator;
        minimunContribuition = minimum;
    }
    function contribute() public payable {
        require(msg.value > minimunContribuition);
        approvers[msg.sender] = true;
        approversCount++;
    }
   ...
    function approveRequest(uint index) public {

        Request storage request = requests[index];
        require(approvers[msg.sender]);
        require(!request.approvals[msg.sender]);
        request.approvals[msg.sender] = true;
        request.approvalCount++;
    }
    function finalizeRequest(uint index) public restricted {
        Request storage request = requests[index];
        require(request.approvalCount > (approversCount / 2));
        require(!request.complete);
        request.recipient.transfer(request.value);
        request.complete = true;
    }
    ...
    }
}
```

Código-fonte 1 – Código Solidity do contrato inteligente.

[10] https://github.com/delanoholanda/kickstart Acesso em: 08 ago. 2022

O contrato inteligente apresentado possui três validações de controle que são elencadas a seguir:

- Valida dados da nova campanha que está sendo criada - a nova campanha só é criada se existir um valor mínimo de contribuição nos parâmetros de criação;
- Verifica quem é o gerente/criador da campanha - o gerente da campanha fica impedido de executar algumas funções, caso venha a tentar, será negada a ação;
- Verifica o resultado das requisições de compra - caso ela tenha atingido sua meta de mais 50% de aprovação, o método que envia ether acumulado no contrato pode seguir.

Na implantação do contrato inteligente o *plugin* MetaMask foi utilizado e funciona como um intermediador na realização das transações na rede *blockchain*. Nesse protótipo a rede utilizada foi a Rinkeby, uma rede de testes da Ethereum, que trabalha com ethers fictícios em seus pagamentos de operações, possibilitando diversos testes de funcionalidades antes mesmo de publicar contratos na rede principal (*mainnet*). O usuário para interagir com o contrato deve utilizar uma conta nesse *plugin* autorizando ou não as transações na *blockchain*, com a possibilidade ainda de gerenciar as transações por meio dessa conta.

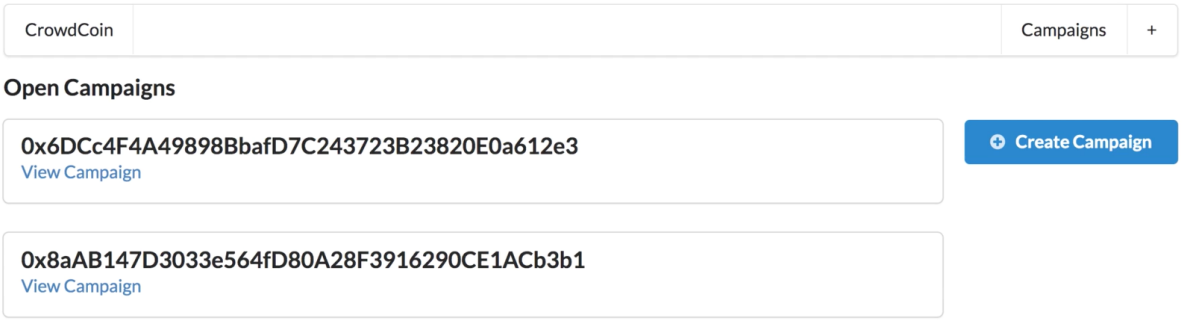
5.1.3 Aplicação Web

A aplicação criada utilizando a linguagem React e seus componentes foi a CrowdCoin. Foi criado um *front-end* onde os usuários podem ter acesso às campanhas já existentes assim como também a criação de novas campanhas. A Figura 28 mostra a tela inicial onde são exibidas as campanhas existentes. No caso da imagem existem duas campanhas criadas, representadas pelos seus números *hash*, que exibe o *hash* do contrato da campanha, ou seja cada campanha é um contrato inteligente na rede Ethereum. Logo ao lado existe o botão para criação de novas campanhas (novos contratos).

Para uma melhor visualização da campanha com suas características, descrições e situação, existe uma tela de gerenciamento. Na Figura 29 a tela da aplicação CrowdCoin exibe o resumo de uma campanha, mostrando o endereço (*hash*) da conta do gerente/criador; quantidade de requisições existentes, sejam elas pendentes ou finalizadas; o valor arrecadado pelo contrato inteligente da campanha; a quantidade de pessoas que investiram; e o valor da contribuição mínima em wei. Ao lado mostra uma caixa de texto onde é possível contribuir para fazer parte da campanha de um jeito simples e rápido.

Estas informações são exibidas em blocos bem definidos para uma melhor visua-

Figura 28 – Tela Inicial - CrowdCoin

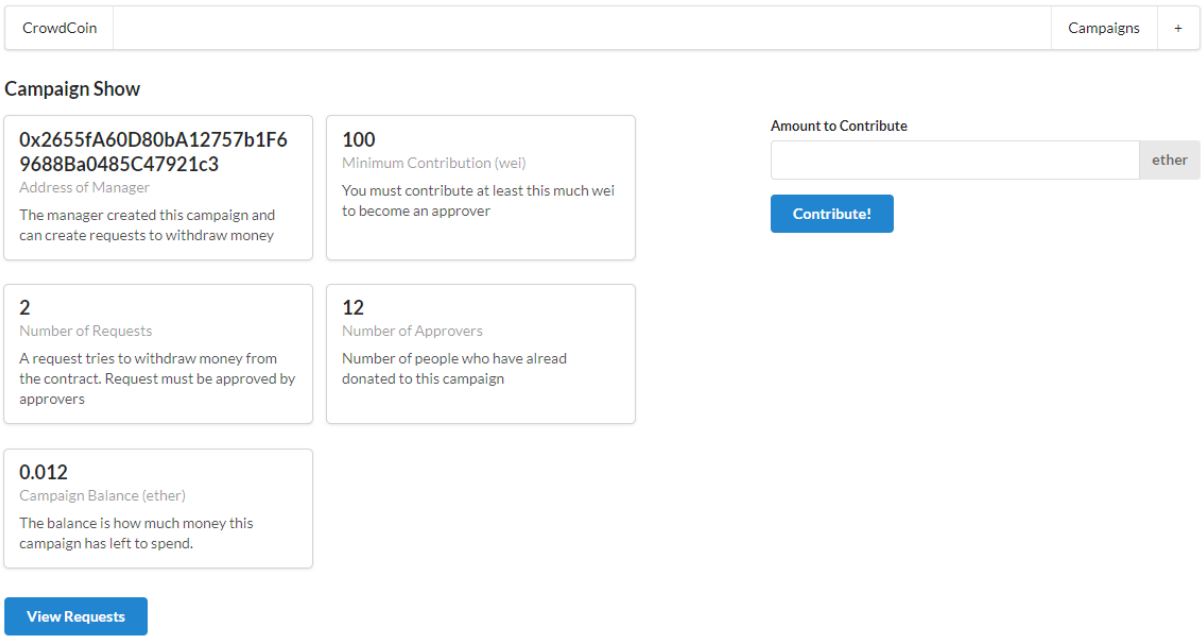


Fonte: o autor.

lização. Também é mostrado um botão que oferece acesso as requisições da campanha, que nada mais é do que os pedidos de compra feitos pelo gerente do projeto no intuito de comprar matéria-prima ou serviços voltados à confecção do projeto.

Ao preencher um valor igual ou acima da contribuição mínima e confirmar o envio de ether para o contrato, o usuário em questão passa a compor o time dos investidores, fazendo parte do projeto de fato e ganhando direito à votação das requisições. Caso o valor não tenha atingido o mínimo é exibido um erro de processamento.

Figura 29 – Tela Resumo da Campanha - CrowdCoin

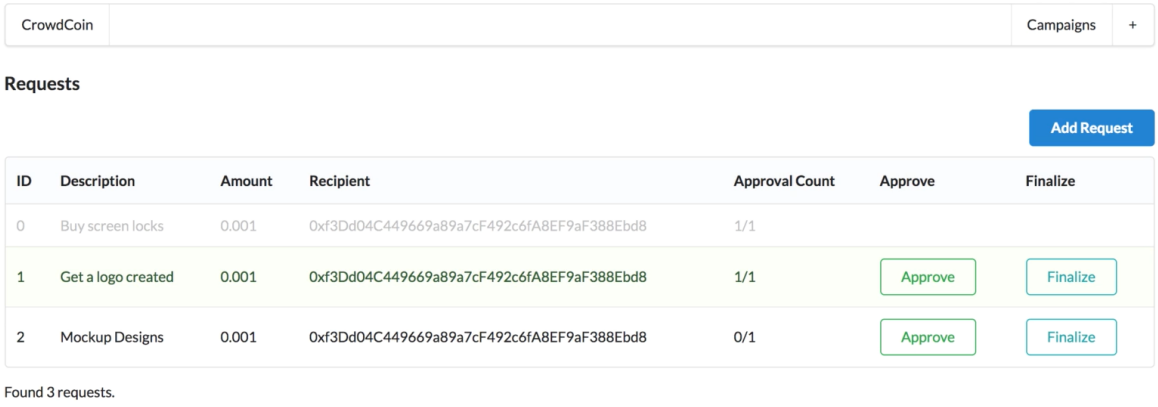


Fonte: o autor.

A Figura 30 exibe a tela de visualização das requisições. É exibida uma lista com o valor a ser enviado e o *hash* da conta que receberá assim como uma descrição do que trata

o pedido de compra. Na listagem é possível visualizar quais as requisições estão em processo de "votação" e as finalizadas. As que aparecem em cinza claro são as que já foram aprovadas e o dinheiro já foi enviado ao destinatário. As que aparecem na cor verde, são requisições que já foram votadas o suficiente para serem finalizadas, ou seja, mais de 50% dos investidores aprovaram o pedido.

Figura 30 – Tela de Requisições - CrowdCoin



Fonte: o autor.

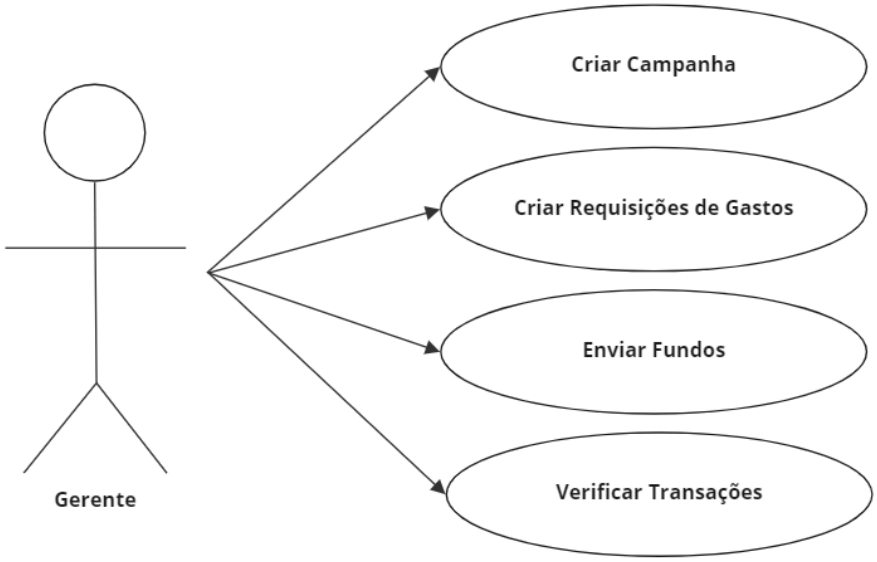
5.1.4 Análise e Projeto do Sistema

A Figura 31 mostra o diagrama de caso de uso dos gerentes de projetos ou criadores das campanhas. Ele descreve quais as funções principais que podem ser executadas por usuários no sistema proposto. Os gerentes podem executar as seguintes ações: criação de novas campanhas, criar requisições de gastos para utilizar o dinheiro arrecadado, enviar fundos de requisições já aprovadas e também podem verificar as transações na *blockchain*.

A Figura 32 mostra o diagrama de caso de uso dos usuários que fazem os investimentos nos projetos. As principais funções que eles podem executar na aplicação são: escolher uma campanha para participar, enviar fundos para tal campanha escolhida, verificar as requisições feitas pelo gerente do projeto de gastos, aprová-las ou rejeitá-las e verificar as transações na rede *blockchain*.

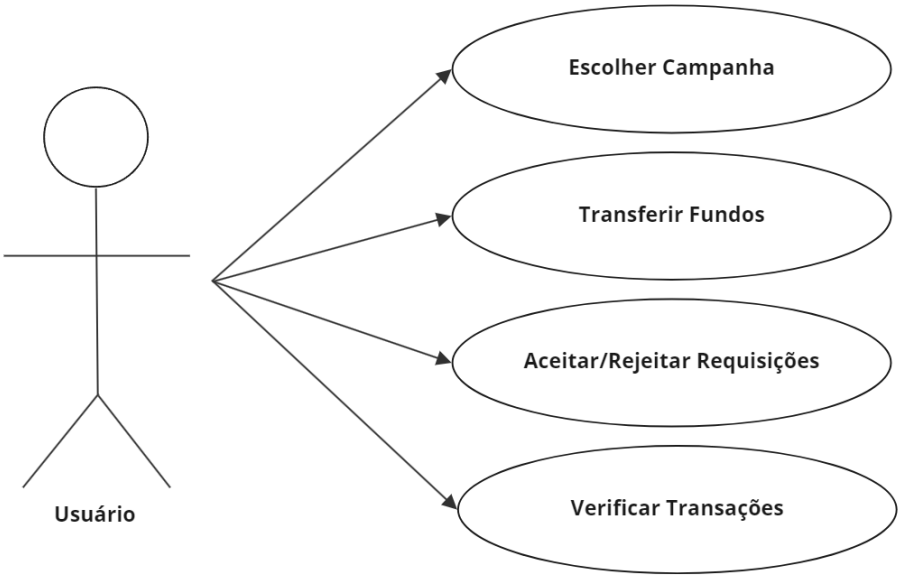
A Figura 33 mostra o fluxo da atividade desempenhada pelo gerente de campanha, desde o momento da criação até a obtenção dos fundos arrecadados. As caixas amarelas representam funções a serem desempenhadas pelo mesmo. Ele quem cria a campanha definindo sua descrição e estabelecendo uma contribuição mínima. Passa por uma primeira validação na

Figura 31 – Diagrama de Caso de Uso do Gerente de Campanha



Fonte: o autor.

Figura 32 – Diagrama de Caso de Uso do Usuário Investidor



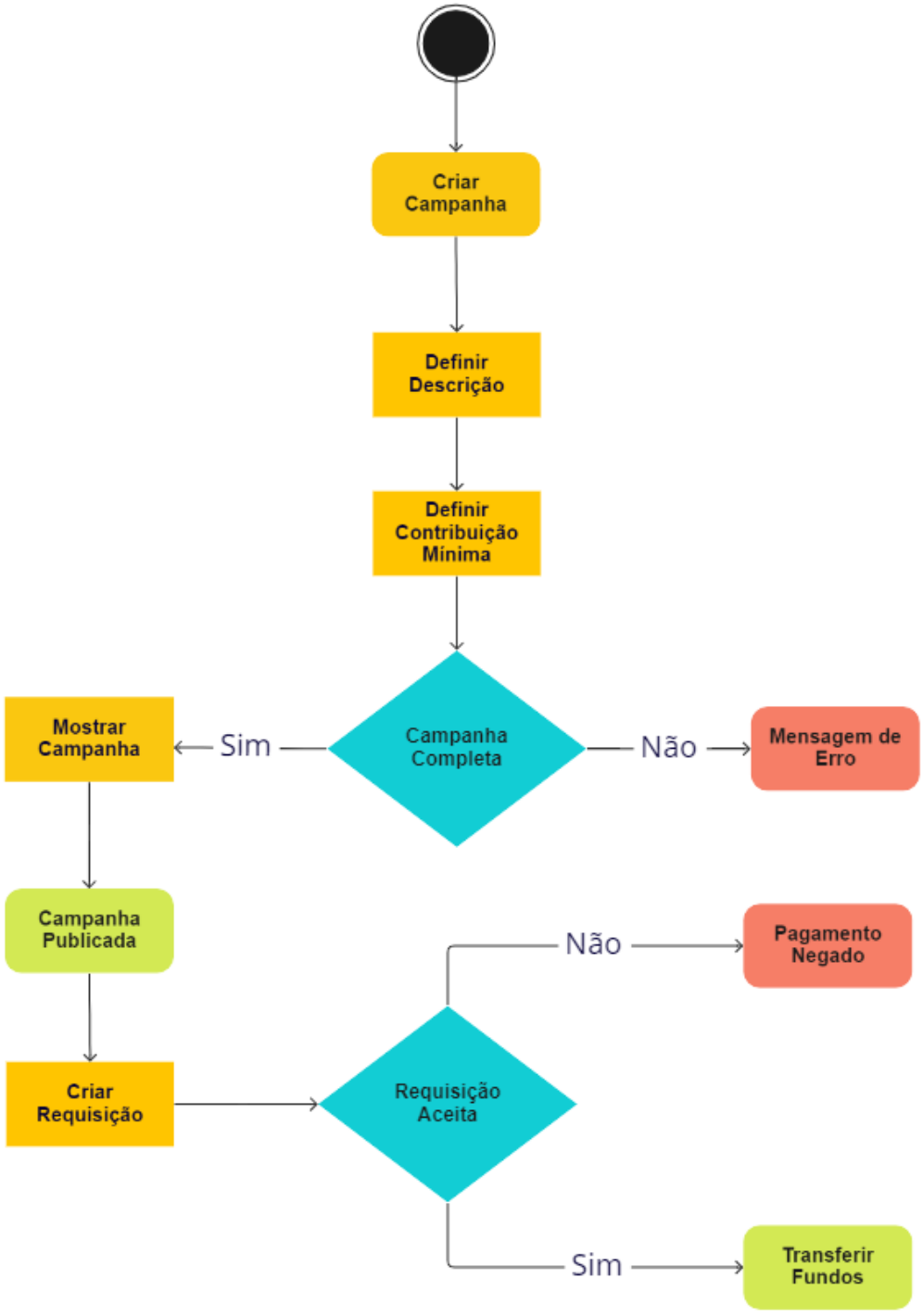
Fonte: o autor.

cor verde (losango), caso esteja tudo correto novo contrato com a nova campanha é adicionado na rede *blockchain*, caso contrário o sistema exibe mensagem de erro.

Outra funcionalidade é a criação de requisição para utilizar os fundos arrecadados, que passa por outra validação feita dessa vez por votação dos investidores. Resultado positivo os fundos solicitados são transferidos para a carteira previamente definida no ato de criação da requisição.

A Figura 34 mostra o fluxo da atividade desempenhada pelos usuários investidores, desde o momento da escolha por uma campanha específica até o momento de fazer de fato parte

Figura 33 – Diagrama de Atividade para o Usuário como Gerente de Campanha



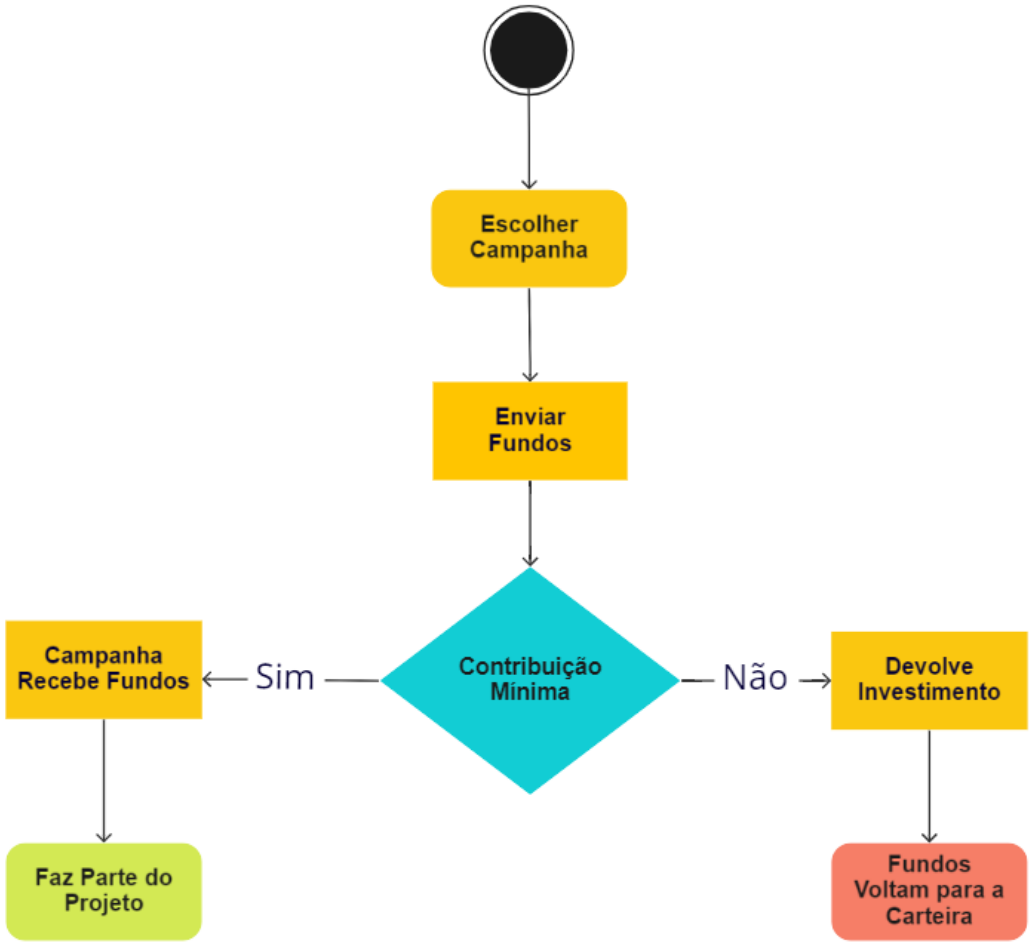
Fonte: o autor.

do projeto. As caixas amarelas representam funções a serem desempenhadas pelos mesmos.

Ao escolher uma campanha o usuário é cobrado para que envie a quantidade mínima estabelecida pelo criador do projeto e já passa pela validação, caso o valor seja igual ou superior ao definido na campanha, o contrato da campanha recebe o valor enviado e a partir desse momento este usuário passa a fazer parte do projeto. Caso não tenha sido enviado quantidade suficiente, a transação é revertida e os fundos retornam para a carteira do usuário que tentou

ingressar na campanha.

Figura 34 – Diagrama de Atividade para o Usuário como Investidor



Fonte: o autor.

5.1.5 Requisitos

Em uma aplicação de *crowdfunding* diversos requisitos podem surgir. Alguns requisitos explorados por este trabalho são: (i) Apenas o gerente pode criar requisições de compra - quando o usuário faz a chamada para criação de requisição temos uma função que verifica se quem chamou é o gerente da campanha, caso seja, o evento acontece normalmente; (ii) Percentual de aprovação - apenas requisições com a aprovação superior a 50% dos financiadores podem ser finalizadas, o dinheiro é de fato enviado para o fornecedor; e (iii) Quantas vezes é possível aprovar - cada financiador pode votar apenas uma vez, seu endereço é guardado em uma lista dentro do próprio contrato evitando assim violação das aprovações.

No capítulo anterior foram identificados requisitos gerais de um sistema convencional

crowdfunding. Neste capítulo foi definido quais os requisitos explorados, para obtenção de uma versão de aplicação proposta utilizando a rede *blockchain*. A Tabela 5 exibe a lista de RF - requisitos funcionais implementados.

Tabela 5 – Requisitos Funcionais (RF) Explorados.

Código	Requisito	Descrição
RF1	Criação de campanha	Qualquer usuário pode criar uma nova campanha e os custos da criação são responsabilidade do mesmo.
RF2	Permitir a criação de requisição	Apenas o criador da campanha pode criar
RF3	Criação de requisição	O criador da campanha pode criar quantas requisições quiser
RF4	Listar requisições	Deve ser exibido uma lista de requisições da campanha
RF5	Mostrar quantas pessoas aprovaram a requisição	Mostrar a quantidade de pessoas que já aprovaram e quantas pessoas tem na campanha como financiador
RF6	Habilitar para finalizar requisição	Ao atingir mais de 50% de aprovação dos financiadores o botão para finalizar deve ativar
RF7	Permitir finalização da requisição	Qualquer pessoa pode finalizar a requisição se o botão estiver habilitado
RF8	Finalizar requisição	Ao apertar no botão o dinheiro é enviado para o fornecedor indicado na requisição
RF9	Mostrar para onde o dinheiro foi enviado	Mostrar na lista de requisições o endereço *hash* do fornecedor que recebeu o dinheiro
RF10	Mostrar o valor arrecadado	Mostrar na campanha o valor arrecadado pelos financiadores

Fonte: o autor.

5.1.6 Testes

A realização de testes na utilização de contratos inteligentes é de suma importância. Uma vez o contrato implantado na rede, para fazer alterações do mesmo torna-se uma tarefa quase impossível diante da imutabilidade dos contratos inteligentes. Alguns métodos de alterações podem ser implementadas durante a confecção do contrato, por exemplo, alterações no valor de uma variável. Um vez o contrato implantado, caso não exista métodos de alteração implementado, o melhor a se fazer é implementar novo contrato e executar uma nova implantação na rede, mas com isso existiria um novo custo devido à nova transação.

Neste trabalho foram desenvolvidos testes unitários simples, mostrando assim a possibilidade de implantar um contrato mais maduro e que tenha sido submetido a pelo menos

alguns testes. A Figura 35 exibe um dos testes feitos durante o desenvolvimento do contrato utilizado neste trabalho que valida a obrigatoriedade de um valor mínimo para um usuário enviar à campanha e assim se tornar membro dela.

Figura 35 – Testando se a contribuição mínima é respeitada.

```
it('requires a minumum contribution', async () => {
    try {
        await campaign.methods.contribute().send({
            value: '5',
            from: accounts[1]
        });
        assert(false);
    } catch (err) {
        assert(err);
    }
});
```

Fonte: o autor.

5.2 Contexto da Aplicação

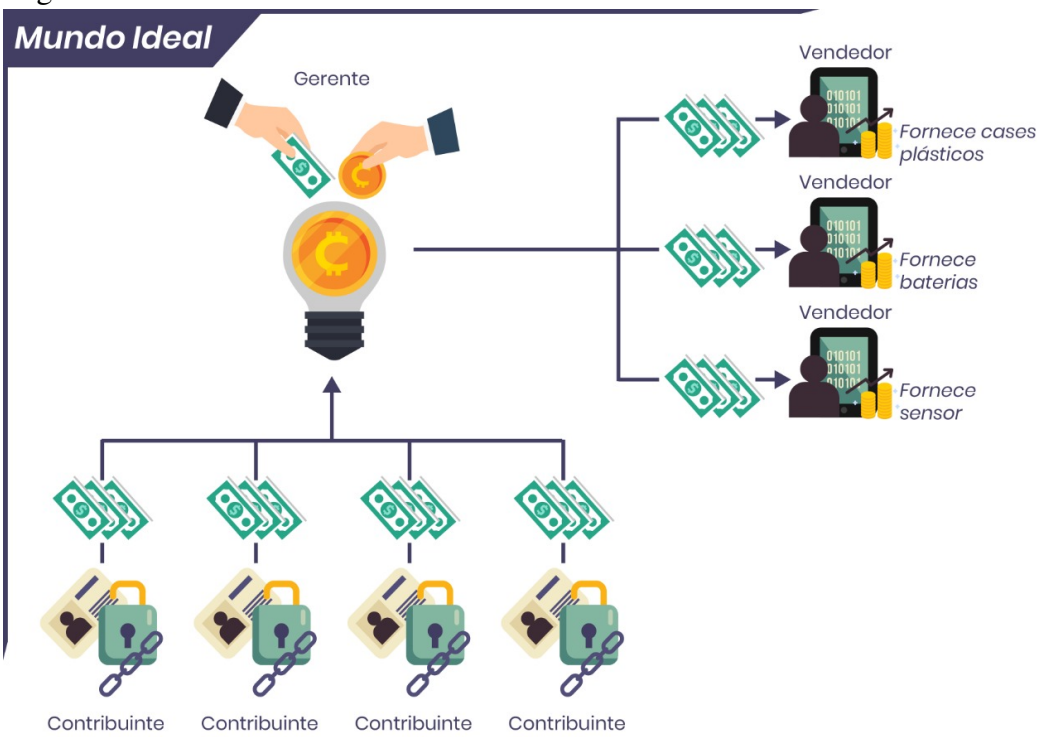
Em um cenário de inovações, onde muitas pessoas têm ideias para produção de um produto ou software, mas muitas vezes encontram impedimento financeiro para custear a sua produção e por conta disso, a ideia não é levada adiante, são ideias que muitas vezes poderiam contribuir com a sociedade seja ajudando ou facilitando a vida das pessoas. Exemplo disso é a ideia de um produto que automatiza tarefas, um robô que limpa a casa ou um sistema que acompanha o nível corporal de massa do corpo humano. O impedimento financeiro acaba gerando assim a desistência dos idealizadores e a ideia por vezes acaba indo para o esquecimento.

Pensando nisso, existem diversos sites onde pessoas podem criar uma campanha, onde é descrito o projeto de maneira a se ter o melhor entendimento do que se pretende fazer ou criar. De posse desse entendimento, sites como esses possibilitam aos usuários tornarem-se um investidor/colaborador do projeto. Existem muitas formas de recompensa para tal investimento, um exemplar do produto a ser criado ou confeccionado é uma delas. Esse processo é chamado de *crowdfunding* que seria uma espécie de financiamento colaborativo, onde várias pessoas se juntam para financiar um projeto ou ideia.

A Figura 36 mostra uma situação ideal em que o *crowdfunding* aconteceria, onde a

parte que teve a ideia e criou o projeto é honesta e realmente utiliza o dinheiro investido pelos colaboradores para o desenvolvimento do que foi prometido. Nesse caso o dinheiro é enviado para fornecedores de componentes por exemplo a fim de colocar o projeto em prática.

Figura 36 – Cenário ideal.

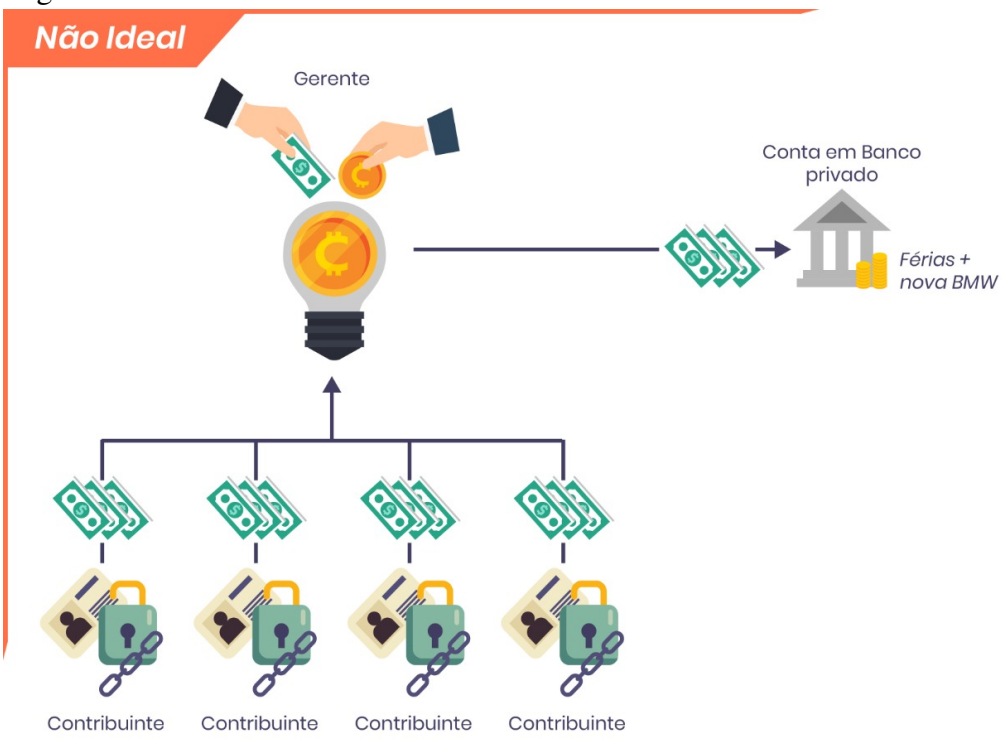


Fonte: o autor.

Entretanto, muitas vezes acontece que os criadores dessas campanhas acabam recebendo o dinheiro dos seus financiadores e por fim acabam por não dar seguimento ao projeto como previsto e simplesmente desaparece com todo o dinheiro arrecadado como está ilustrado na Figura 37.

Em uma aplicação onde para obter o envio de dinheiro arrecadado até o momento, seja necessário a aprovação de mais de 50% dos financiadores, ficariam um pouco mais difícil para aqueles que pretendem apenas lesar os financiadores. Dessa forma, o idealizador do projeto apenas cria uma solicitação de compra de um componente, por exemplo, indicando o valor e o *hash* da carteira digital do fornecedor. Com isso feito, os envolvidos fazem a aprovação ou não de tal demanda. Com acesso ao histórico de requisições criadas desse tipo, os investidores conseguem assim ter mais transparência e auxílio na rastreabilidade do dinheiro arrecadado. A Figura 38 mostra como passa a ser o caminho entre o dinheiro sair do contrato de arrecadação para a carteira de algum fornecedor.

Figura 37 – Cenário não ideal.



Fonte: o autor.

Figura 38 – Aprovação de Requisição (Compra).

Fonte: o autor.

5.2.1 Projeto do Experimento

Como projeto de experimento, é feita uma análise dos custos relacionados às transações efetuadas na rede Ethereum interagindo com os contratos inteligentes. Também é desenvolvida uma análise do tempo necessário para a execução das transações.

O contexto utilizado é o de criação de novas campanhas (projetos), em seguida o envio de ether para as campanhas e com isso passando a fazer parte da campanha. Dando continuidade é feito a criação de requisições feitas pelo gerente da campanha que com elas almeja o uso do dinheiro arrecadado. Por fim aprovações realizadas pelos investidores, a respeito das requisições criadas na campanha.

A análise de tempo se deu procedendo a coleta dos tempos de duração entre o envio de uma nova transação para a rede Ethereum e sua resposta. Isso já com o novo bloco validado e devidamente adicionado na *blockchain*.

Para análise de custo de uma transação, verifica-se o valor a ser pago por ela. Também é feito um detalhamento da quantidade de *gas* utilizado nos diferentes tipos de ações: criação de uma nova campanha; envio de ether para uma determinada campanha que diz respeito a transações de investimento, ou seja, de entrada no projeto; criação de requisições paro o uso do dinheiro arrecadado e aprovação das requisições.

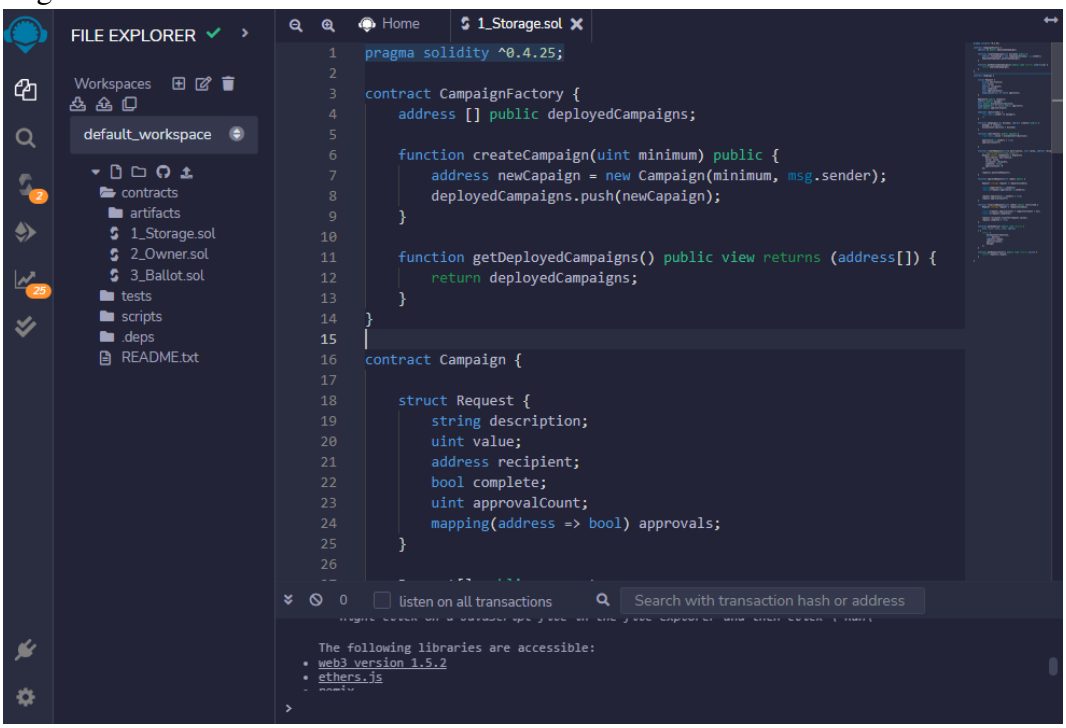
Com isso, as métricas observadas neste trabalho foram três. O tempo em segundos que uma transação leva para ser minerada e adicionada à rede Ethereum, valor gasto em gas por cada transação e o valor médio da transação em si por completo em dólar americano e em real brasileiro.

5.2.2 Especificações das Simulações

Para o projeto de simulação foi escolhida a rede Ethereum que possibilita a utilização de contratos inteligentes em sua rede. Em sua concepção foi utilizada a ferramenta online Remix IDE[11] para confeccionar o contrato e realizar testes iniciais de funcionalidades. A Figura 39 exibe o visual da ferramenta Remix IDE, ferramenta que possibilita diversos testes utilizando contratos inteligentes na rede *blockchain*, permite desenvolver, implantar e administrar contratos inteligentes para Ethereum com *blockchains*. Foi utilizada a linguagem Solidity que é a linguagem de programação criada pela Ethereum no desenvolvimento de contratos inteligentes.

[11] https://remix.ethereum.org/ Acesso em: 08 ago. 2022

Figura 39 – Ferramenta Online Remix.



Fonte: o autor.

Na confecção da aplicação *web* foram empregadas a tecnologia React do JavaScript juntamente com API Web3. Um *plugin* Metamask que serve como carteira digital onde guarda-se o ether também foi usado para autorizar o uso de ether em cada transação. A rede escolhida foi a Rinkeby, uma rede de teste da própria Ethereum que possibilita desenvolvedores que utilizem a rede executem testes simulando as transações na rede principal, mas com o benefício de não gastar dinheiro de fato, utilizando ether falso.

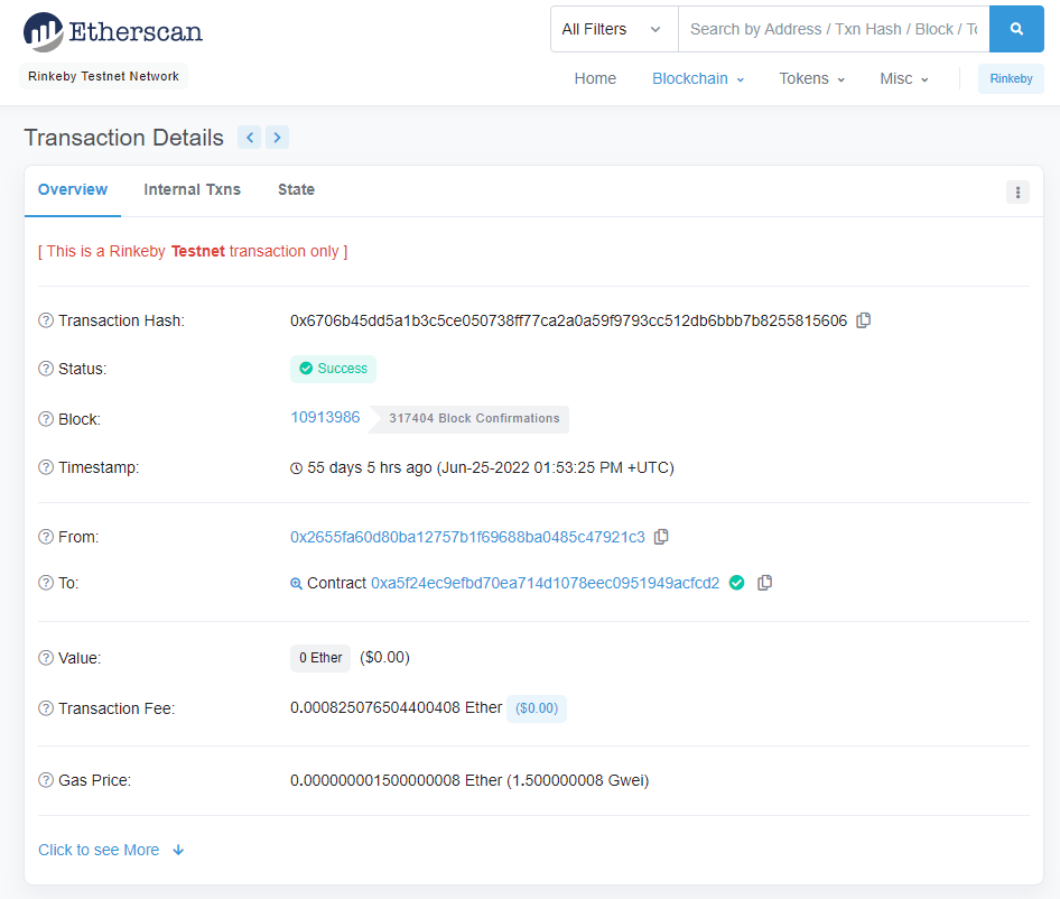
Ao pensar nas principais ações a serem abordadas na proposta deste trabalho, foram definidos quatro cenários de simulações. As execuções desses cenários foram definidas da seguinte forma: cada cenário deveria ser repetido trinta vezes em três períodos distintos durante o dia, com intervalo de dois minutos entre uma transação e outra, totalizando assim noventa repetições para cada cenário. Isso pelo fato do valor do dólar assim como o do ether ter variações durante o dia e dessa forma possibilitar a obtenção de uma amostragem mais completa dos valores. Ao final de todas as simulações foram obtidos quatro cenários repetidos noventa vezes cada, totalizando em trezentos e sessenta simulações realizadas neste trabalho.

Os testes deste trabalho foram todos realizados em um *notebook* Intel(R) Core(TM) i5-826U CPU @ 1.60GHz 1.80 GHz com 8.00 GB de memória RAM, sistema operacional Windows 11 Pro. Essas configurações impactam na aplicação da seguinte forma: quanto mais poder de processamento a estação de teste possuir, mais rapidamente as páginas da aplicação

serão renderizadas na tela do *browser*, já para a rede *blockchain* são indiferentes, pois dependem da própria rede.

Os testes utilizam a aplicação desenvolvida para interagir com a rede Ethereum juntamente com o Metamask. Os tempos foram coletados via código e exibidos na tela da aplicação. Os valores das transações foram coletados no EtherScan depois da confirmação de cada transação. A Figura 40 exibe os detalhes de uma transação de criação de uma nova campanha. Nela é possível verificar o *hash* da transação, o seu *status*, hora exata em que a transação foi confirmada na rede, dentre outras informações.

Figura 40 – Ferramenta Online Etherscan.



Fonte: o autor.

5.2.3 Cenários de Avaliação

Para obter uma experiência de *crowdfunding* visando as principais funcionalidades desempenhadas em aplicações convencionais, neste trabalho foram escolhidos quatro cenários definidos como essenciais. Representando assim, ações a serem realizadas em um site que realiza processos de *crowdfunding*. Dessas quatro ações, duas dizem respeito ao idealizador do projeto

que está buscando financiamento para sua campanha e duas são realizadas pelos usuários que pretendem investir em determinadas campanhas.

Em todos os cenários, para que exista a possibilidade de interação entre o usuário e a aplicação existem dois requisitos a serem cumpridos: o usuário deve ter o plugin do MetaMask instalado e habilitado em seu navegador; e uma carteira digital conectada. Cumprindo os dois requisitos, a aplicação ficará habilitada para a interação.

O primeiro cenário foi definido como criação de campanha. Nele, qualquer usuário pode interagir com a aplicação criando uma nova campanha. Para criar uma nova campanha é preciso definir apenas o campo que se refere ao valor mínimo de contribuição. Esse passará a ser o valor esperado pelo novo contrato criado, caso algum usuário envie valor inferior, a transação será rejeitada a transação. Este cenário é voltado para qualquer gerente de projeto.

O segundo cenário é o segundo momento da campanha, depois de sua criação ela espera receber investimento dos usuários. Com isso, este cenário representa o investimento feito à campanha. Qualquer usuário pode realizar esta ação. Ao enviar um valor que seja superior ao valor mínimo, este usuário passará a fazer parte da campanha escolhida e também automaticamente do time que possui o poder de votação, a ser realizada no último cenário, sobre as requisições de uso do dinheiro arrecadado. Este cenário é voltado qualquer investidor.

O terceiro cenário representa uma campanha que já possui determinada quantidade de ether, quantidade esta que já pode dar início ao projeto de desenvolvimento da ideia. Mas como a abordagem deste trabalho conta com um passo fundamental na utilização do dinheiro arrecadado, o criador do projeto, gerente, deve criar na campanha uma nova requisição. A requisição é a forma projetada para “sacar” ether do contrato inteligente que se encontra na campanha. Este cenário é destinado aos gerentes de projeto, apenas eles podem realizar esta ação.

O quarto e ultimo cenário diz respeito ao poder de voto que é fornecido aos investidores pela abordagem deste trabalho. Voto esse que vai ser fundamental para o andamento da campanha. Com ele os investidores passam a ter “poder” de decisão dentro da campanha que participam. O gerente da campanha precisa deixar claro o motivo e para onde pretende enviar parte dos fundos arrecadados. Neste cenário, os investidores que investiram em uma determinada campanha, e por isso fazem parte do time de aprovadores, podem opinar sobre as requisições criadas pelo gerente da campanha. Com isso, este cenário se torna restrito aos usuários que fazem parte da campanha na posição de investidor.

5.3 Resultados

5.3.1 Cenário 1 - Criação de Campanha

O primeiro cenário, que testa criações de campanhas, foi executado no dia 25 de Junho de 2022. A Tabela 6 mostra o cenário no momento dos testes em relação aos valores do dólar e ether em real. A primeira bateria de testes, ou seja as primeiras trinta campanhas criadas, tiveram início pela manhã às 10:53. Neste momento o valor do ether em reais era de R$ 6.287,32 reais, o dólar estava cotado em R$ 5,24 reais. A segunda bateria foi iniciada no começo da noite no mesmo dia às 19:40, o valor do ether nesse momento era de R$ 6.533,40 reais e o dólar se mantinha em R$ 5,24 reais. A terceira e última bateria de testes teve seu início ao final da noite às 23:52 do mesmo dia, o valor do ether R$ 6.439,33 reais e o dólar ainda mantido em R$ 5,24 reais.

Tabela 6 – Valores no Momento dos Testes - Cenário 1.

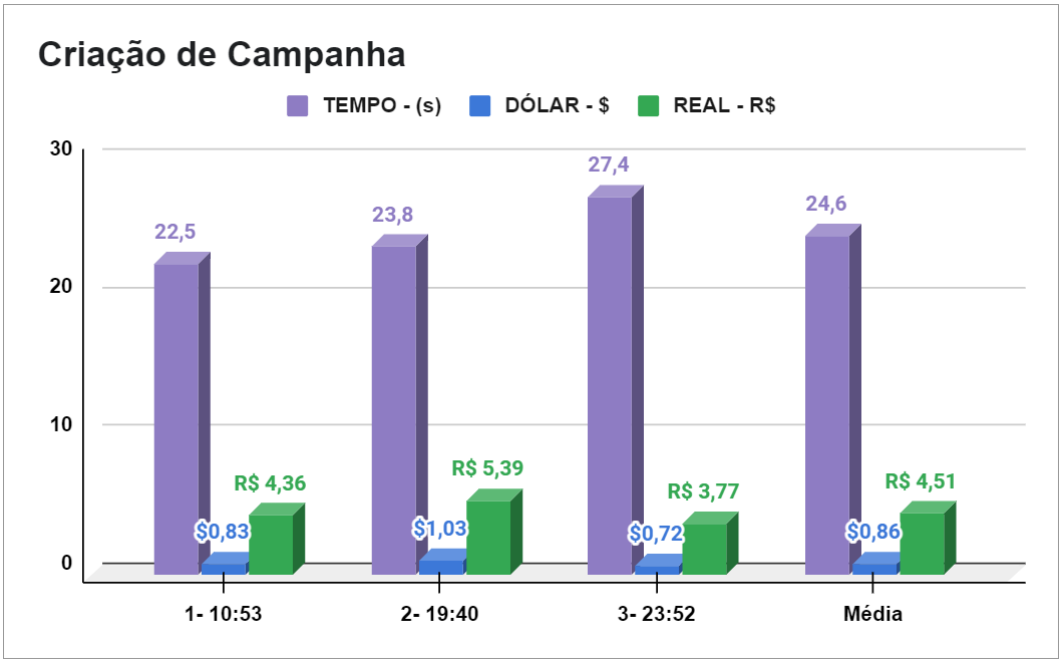
	Hora	**Data**	**Dólar em Real**	**Ether em Real**
1º	10:53	25/06/2022	R$ 5,24	R$ 6.287,32
2º	19:40	25/06/2022	R$ 5,24	R$ 6.533,40
3º	23:52	25/06/2022	R$ 5,24	R$ 6.439,33

Fonte: o autor.

A Figura 41 exibe as médias do tempo, do valor em dólar e do valor em real das transações realizadas durantes os testes. Foi calculada a média de cada uma das três baterias de testes, e uma média foi calculada em cima desses três valores obtidos. O tempo médio para que as transações sejam completamente adicionadas na rede *blockchain* nesse primeiro cenário foi de 24,6 segundos. Os testes mostraram também que durante o período da manhã foi onde as transações eram finalizadas mais rapidamente.

O valor médio gasto em dólar por transação ficou em torno de US$ 0.86 dólares. O período que se mostrou ser menos oneroso em relação às transações foi durante o final da noite entrando na madrugada, a média chegou a US$ 0.72 dólares. O valor médio gasto em reais ficou em torno de R$ 4,51 reais. No dia da realização dos testes o valor do real em relação ao dólar não teve variações e se manteve no mesmo valor nas três baterias de testes.

Figura 41 – Criação de Novas Campanhas.



Fonte: o autor.

5.3.2 Cenário 2 - Investimento dos Usuários

O segundo cenário, que testa o ingresso dos usuários investidores em determinada campanha, foi executado nos dias 26 e 27 de Junho de 2022. A Tabela 7 mostra o cenário daquela data em relação aos valores do dólar e ether em real. A primeira bateria de testes teve início no período da tarde às 13:40 do dia 26. Neste dado momento o valor do ether em reais era de R$ 6.449,03 reais, o dólar estava cotado em R$ 5,24 reais. A segunda bateria foi iniciada no final da noite no mesmo dia às 23:24, o valor do ether nesse momento era de R$ 6.371,49 reais e o dólar se mantinha em R$ 5,24 reais. A terceira e última bateria de testes teve seu início no dia seguinte no começo da tarde às 13:54, o valor do ether R$ 6.189,93 reais e o dólar teve sua primeira variação passando a valer R$ 5,21 reais.

Tabela 7 – Valores no Momento dos Testes - Cenário 2.

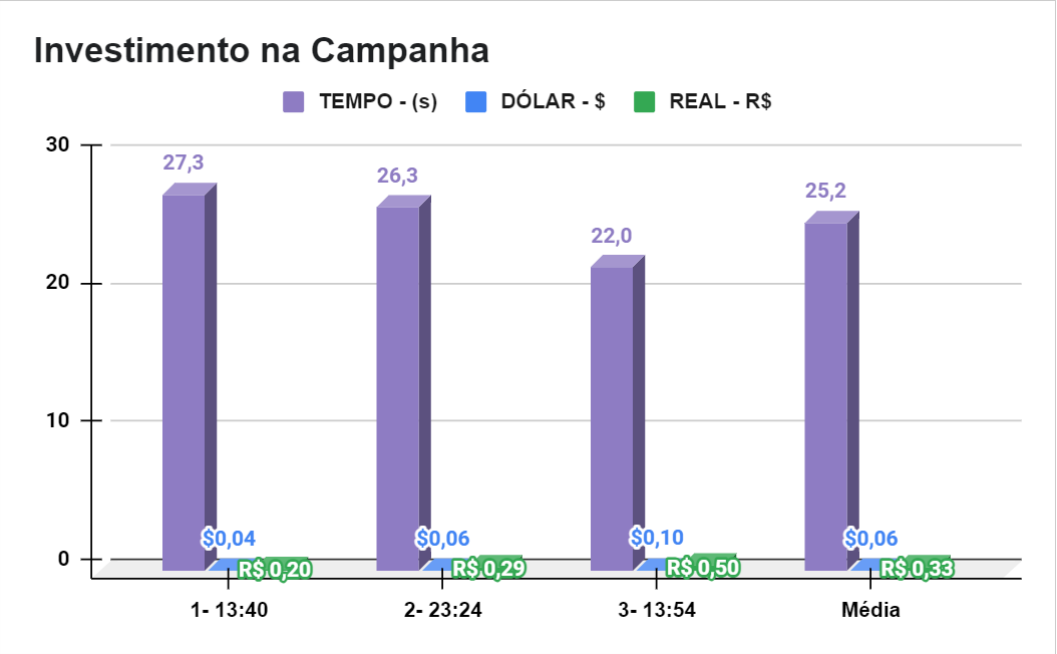
	Hora	**Data**	**Dólar em Real**	**Ether em Real**
1º	13:40	26/06/2022	R$ 5,24	R$ 6.449,03
2º	23:24	26/06/2022	R$ 5,24	R$ 6.371,49
3º	13:54	27/06/2022	R$ 5,21	R$ 6.189,93

Fonte: o autor.

A Figura 42 mostra as médias do tempo, do valor em dólar e do valor em real das transações realizadas durantes os testes. Foi calculado também uma média sobre as médias das três baterias de teste. O tempo médio para que as transações sejam completamente adicionadas

na rede *blockchain* nesse segundo cenário foi de 25,2 segundos.

Figura 42 – Investimento na Campanha.



Fonte: o autor.

Os testes apontam que o mesmo horário em dias diferentes podem ter variações. Isso é notado ao observar que a primeira e terceira bateria foram realizadas praticamente no mesmo horário um dia após o outro e mesmo assim obteve uma variação considerável, mais de 5 segundos na média de tempo das transações. Ficando a primeira bateria definida como a mais demorada, com uma média de 27,3 segundos e a terceira como a mais rápida que teve suas transações confirmadas com uma média de 22 segundos.

O valor médio gasto em dólar por transação ficou em torno de US$ 0.06 dólares. Foi observado que mesmo com a queda do valor do ether e do dólar, a média do valor pago pelas transações teve um aumento considerável acima de 100%. As mesmas transações executadas em dias diferentes, praticamente nos mesmos horários, saíram de uma média de US$ 0.04 dólares para US$ 0.10 dólares. O valor médio gasto em reais ficou em torno de R$ 0,33 reais. Nos dias da realização dos testes o valor do real em relação ao dólar teve uma pequena variação de R$ 0,03 reais do início ao fim dos testes.

5.3.3 Cenário 3 - Campanha com Quantidade de Ether

O terceiro cenário, que testa a criação de requisições para uso do dinheiro arrecadado em determinada campanha, foi executado nos dias 27 e 28 de Junho de 2022. A Tabela 8 mostra

o cenário daquela data em relação aos valores do dólar e ether em real. A primeira bateria de testes teve início no período da noite às 22:04 do dia 27. Neste dado momento o valor do ether em reais era de R$ 6.206,72 reais, o dólar estava cotado em R$ 5,24 reais. A segunda bateria foi iniciada no início do dia seguinte às 09:16, o valor do ether nesse momento era de R$ 6.406,81 reais e o dólar se mantinha em R$ 5,24 reais. A terceira e última bateria de testes teve seu início no meio da tarde do dia 28 às 16:06, o valor do ether R$ 6.119,32 reais e o dólar teve uma nova variação passando a valer R$ 5,27 reais.

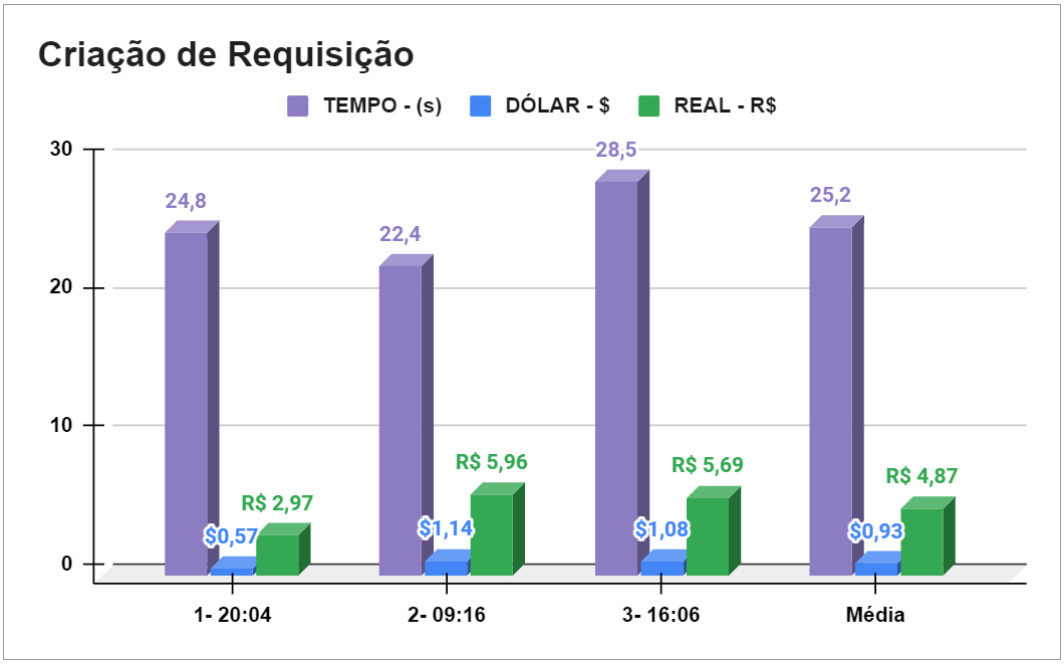
Tabela 8 – Valores no Momento dos Testes - Cenário 3.

	Hora	**Data**	**Dólar em Real**	**Ether em Real**
1º	22:04	27/06/2022	R$ 5,24	R$ 6.206,72
2º	09:16	28/06/2022	R$ 5,24	R$ 6.406,81
3º	16:06	28/06/2022	R$ 5,27	R$ 6.119,32

Fonte: o autor.

A Figura 43 exibe as médias do tempo, do valor em dólar e do valor em real das transações realizadas durantes os testes. Foi calculada uma média sobre as médias das três baterias de testes. O tempo médio para que as transações sejam completamente adicionadas na rede *blockchain* nesse terceiro cenário foi de 25,2 segundos se igualando a média do cenário anterior.

Figura 43 – Criação de Requisição.



Fonte: o autor.

Neste cenário os testes apontam que as transações executadas no início da manhã

são adicionadas mais rapidamente na rede *blockchain*. A diferença entre os períodos distintos chegou a ser superior a 5 segundos na média dos tempos coletados. Com isso as transações realizadas na terceira bateria foram as que tiveram uma menor demora em sua confirmação com um tempo médio de 22 segundos.

O valor médio gasto em dólar por transação ficou em torno de US$ 0.93 dólares. Foi observado que no período da manhã, apesar de ser o que confirmou mais rápido suas transações, também foi o período em que a média do valor pago pelas transações foi mais elevado. Também foi o período em que o ether se tornou mais caro dentre as três baterias de teste. O valor médio pago em dólar das mesmas transações efetuadas em dias diferentes teve um aumento de 100%. Primeira bateira o valor médio US$ 0.57 dólares e já na segunda esse valor dobrou para US$ 1.14 dólares. O valor médio gasto em reais ficou em torno de R$ 4,87 reais. Nos dias da realização dos testes o valor do real em relação ao dólar teve uma pequena variação de R$ 0,03 reais do início ao fim dos testes.

5.3.4 Cenário 4 - Poder de Voto

O quarto e último cenário, que testa a aprovação por parte dos investidores para uso do dinheiro arrecadado em determinada campanha, foi executado nos dias 28 e 29 de Junho de 2022. A Tabela 9 mostra o cenário atual no momento dos testes em relação aos valores do dólar e ether em real. A primeira bateria de testes teve início no período da noite às 20:46 do dia 28. Neste dado momento o valor do ether em reais era de R$ 6.054,70 reais, o dólar estava cotado em R$ 5,27 reais. A segunda bateria foi iniciada no final da noite no mesmo dia às 23:04, o valor do ether nesse momento era de R$ 6.056,54 reais e o dólar se mantinha em R$ 5,27 reais. A terceira e última bateria de testes teve seu início no dia seguinte no final da manhã às 11:26, o valor do ether R$ 5.797,67 reais e o dólar teve uma variação passando a valer R$ 5,23 reais.

Tabela 9 – Valores no Momento dos Testes - Cenário 4.

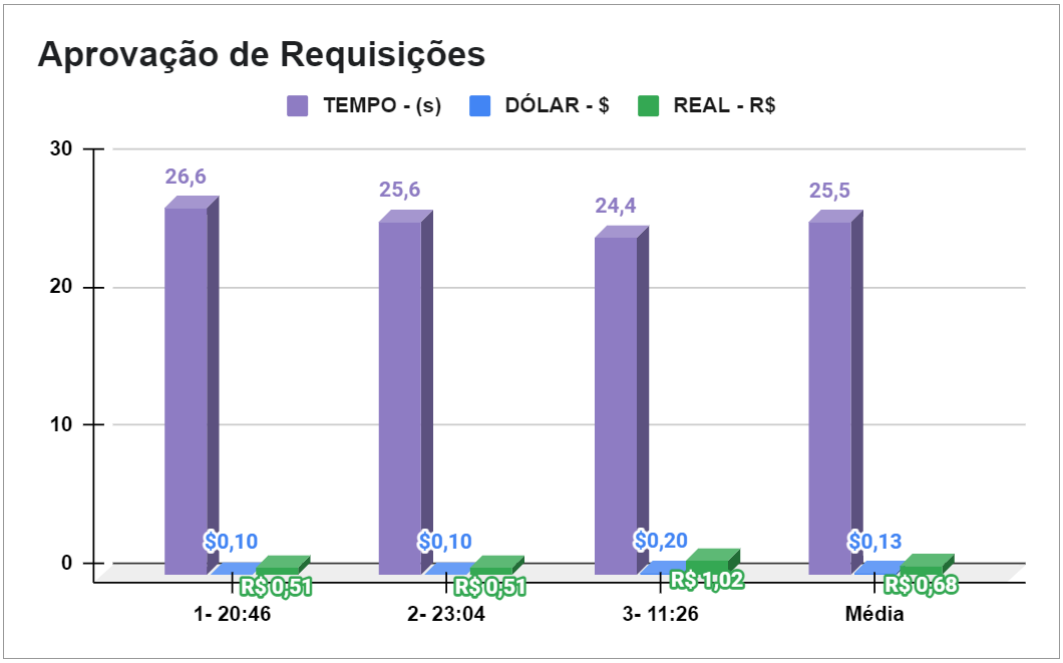
	Hora	**Data**	**Dólar em Real**	**Ether em Real**
1º	20:46	28/06/2022	R$ 5,27	R$ 6.054,70
2º	23:04	28/06/2022	R$ 5,27	R$ 6.056,54
3º	11:26	29/06/2022	R$ 5,23	R$ 5.797,67

Fonte: o autor.

A Figura 44 exibe as médias do tempo, do valor em dólar e do valor em real das transações realizadas durantes os testes. Assim como nos outros cenários, foi calculada a média

sobre as médias obtidas nas três baterias de testes. O tempo médio para que as transações sejam completamente adicionadas na rede *blockchain* nesse quarto cenário foi de 25,5 segundos.

Figura 44 – Aprovação de Requisição.



Fonte: o autor.

Neste cenário as médias dos tempos de transações ficaram mais equilibrados apesar de terem sidas executadas em períodos distintos e até em dias diferentes. A variação das médias ficou em torno de 1 segundo para mais e para menos. Mais uma vez os testes realizados no período da manhã é o que atingiram uma menor demora em confirmar suas transações, com o tempo médio de 24,4 segundos.

O valor médio gasto em dólar por transação ficou em torno de US$ 0.13 dólares. Também foi observado que mesmo com a queda do valor do ether e do dólar, a média do valor pago pelas transações teve um aumento de 100% em relação aos aos outros testes deste cenário. As mesmas transações executadas em dias diferentes, saíram de uma média de US$ 0.10 dólares para US$ 0.20 dólares. O valor médio gasto em reais ficou em torno de R$ 0,68 reais. Nos dias da realização dos testes o valor do real em relação ao dólar teve sua maior variação de R$ 0,04 reais para menos, do início ao fim dos testes.

5.4 Análises

Para uma análise mais completa dos dados foram calculados a mediana, o desvio padrão e os quartis. A mediana é o valor que separa a metade maior e a metade menor de uma

amostra, uma população ou uma distribuição de probabilidade. O desvio padrão é uma medida de dispersão, ou seja, qual a distância dos dados de uma amostra com relação à média. Um baixo desvio padrão indica que os pontos dos dados tendem a estar próximos da média ou do valor esperado. Um alto desvio padrão indica que os pontos dos dados estão espalhados por uma ampla gama de valores. Em relação aos quartis, o primeiro quartil representa o valor do conjunto que delimita os 25% dos valores menores e o terceiro quartil representa o valor do conjunto que delimita os 75% dos valores menores de uma amostra.

A seguir são apresentados os histogramas consolidando os resultados de todos os cenários somados, com a intenção de possibilitar uma visão global dos resultados, de forma a apresentar um cenário mais realista onde várias operações diferentes são exibidas. Eles correspondem a todos os quatro cenários juntos.

Todas as figuras de *boxplot* a seguir possuem alguns losangos coloridos. O losango vermelho indica a média, o azul a mediana, e o verde o desvio padrão. Esses valores estão disponibilizados também nas tabelas. Adicionalmente, alguns valores estatísticos foram calculados para complementar as análises, que foram valor mínimo, valor máximo, média, mediana, quartis e desvio padrão. Todos os valores de ether foram informados somente até a quarta casa decimal após a vírgula, para facilitar a visualização dos dados. Os valores de tempo também foram informados apenas até a segunda casa decimal após a vírgula.

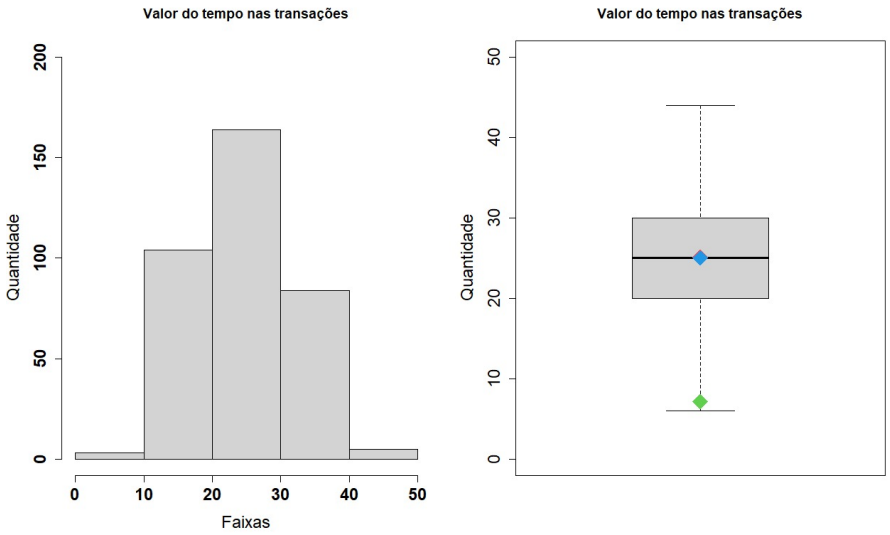
O Apêndice A conta com os Quadros 3 e 4 que mostram os detalhes de todos os cenários do ponto de vista estatístico. Neles são exibidas as seguintes medidas: média, mediana, valor mínimo, valor máximo, variância, desvio padrão, primeiro quartil, segundo quartil, terceiro quartil e alcance.

5.4.1 Análise do Tempo

A Figura 45 exibe o histograma e *boxplot* para os valores totais do tempo de cada cenário, todos somados. O menor valor coletado foi 6,000 e o maior foi 44,000, ou seja, os valores do tempo nesse tipo de transação estão entre esse intervalo. A mediana foi 25,000 segundos, ou seja, metade das transações ocorreu com um valor menor que 25,000 segundos e a outra metade ocorreu com valor maior que 25,000 segundos. O primeiro quartil do *boxplot* possui o valor de 20,000 segundos, ou seja, um quarto das transações foi com um valor menor que 20,000 segundos. Já o terceiro quartil do *boxplot* tem valor de 30,000 segundos, ou seja, 75% das transações ocorreram com valor menor que 30,000 segundos. Neste cenário, pode-se afirmar

que o alcance, variação, da transação com maior valor e a de menor valor (44,000 - 6,000) foi de 38,000 segundos. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de segundos gasto nas transações.

Figura 45 – Análise do Tempo

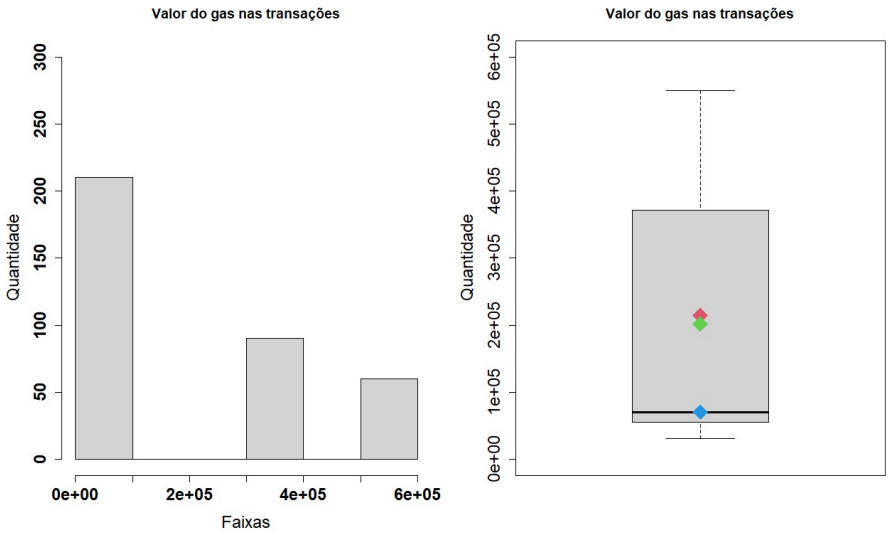


Fonte: o autor.

5.4.2 Análise do Gas

A Figura 46 exibe o histograma e *boxplot* para os valores totais do gas em cada cenário, todos somados. O menor valor coletado foi 30809 e o maior foi 550051, ou seja, os valores do gas nesse tipo de transação estão entre esse intervalo. A mediana foi 70516 wei, ou seja, metade das transações ocorreu com um valor menor que 70516 wei e a outra metade ocorreu com valor maior que 70516 wei. O primeiro quartil do *boxplot* possui o valor de 55039,75 wei, ou seja, um quarto das transações foram com um valor menor que 55039,75 wei. Já o terceiro quartil do *boxplot* tem valor de 371275 wei, ou seja, 75% das transações ocorreram com valor menor que 371275 wei. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (30809 - 550051) foi de 519242 wei. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de gas gasto nas transações.

Figura 46 – Análise do Gas



Fonte: o autor.

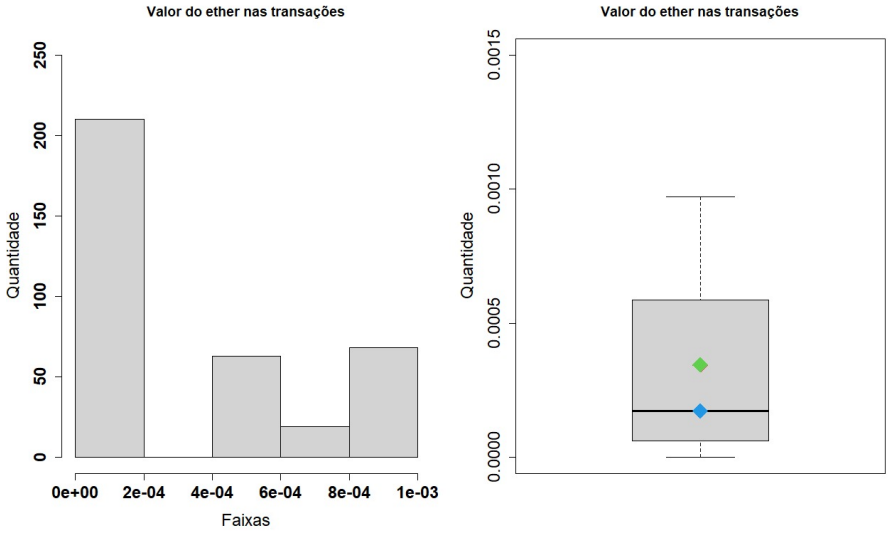
5.4.3 Análise do Ether

A Figura 47 exibe o histograma e *boxplot* para os valores totais em ether de cada cenário, todos somados. O menor valor coletado foi 0,00000000150 e o maior foi 0,00097093751, ou seja, os valores em ether nesse tipo de transação estão entre esse intervalo. A mediana foi 0,00017289125 ether, ou seja, metade das transações ocorreu com um valor menor que 0,00017289125 ether e a outra metade ocorreu com valor maior que 0,00017289125 ether. O primeiro quartil do *boxplot* possui o valor de 0,00006932025 ether, ou seja, um quarto das transações foram com um valor menor que 0,00006932025 ether. Já o terceiro quartil do *boxplot* tem valor de 0,00058620154 ether, ou seja, 75% das transações ocorreram com valor menor que 0,00058620154 ether. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (0,00000000150 - 0,00097093751) foi de 0,00097093601 ether. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de ether gasto nas transações.

5.4.4 Análise do Dólar

A Figura 48 exibe o histograma e *boxplot* para os valores totais em dólar de cada cenário, todos somados. O menor valor coletado foi US$ 0,037874807 dólares e o maior foi US$ 1,187184709 dólares, ou seja, os valores do tempo nesse tipo de transação estão entre esse intervalo. A mediana foi US$ 0,384452261 dólares, ou seja, metade das transações ocorreu com um valor menor que US$ 0,384452261 dólares e a outra metade ocorreu com valor maior que US$

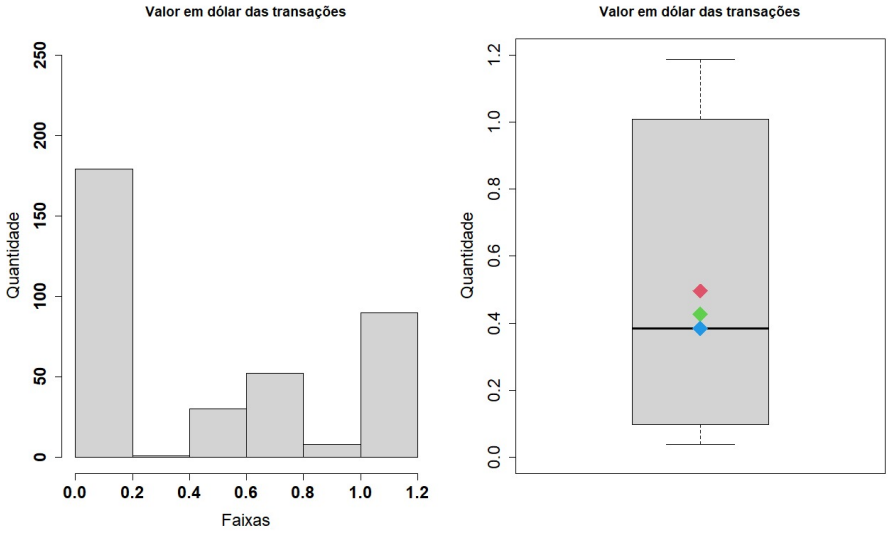
Figura 47 – Análise do Valor em Ether



Fonte: o autor.

0,384452261 dólares. O primeiro quartil do *boxplot* possui o valor de US$ 0,097219105 dólares, ou seja, um quarto das transações foram com um valor menor que US$ 0,097219105 dólares. Já o terceiro quartil do *boxplot* tem valor de US$ 0,999499741 dólares, ou seja, 75% das transações ocorreram com valor menor que US$ 0,999499741 dólares. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (0,037874807 - 1,187184709) foi de US$ 1,149309902 dólares. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor de dólar gasto nas transações.

Figura 48 – Análise do Valor em Dólar

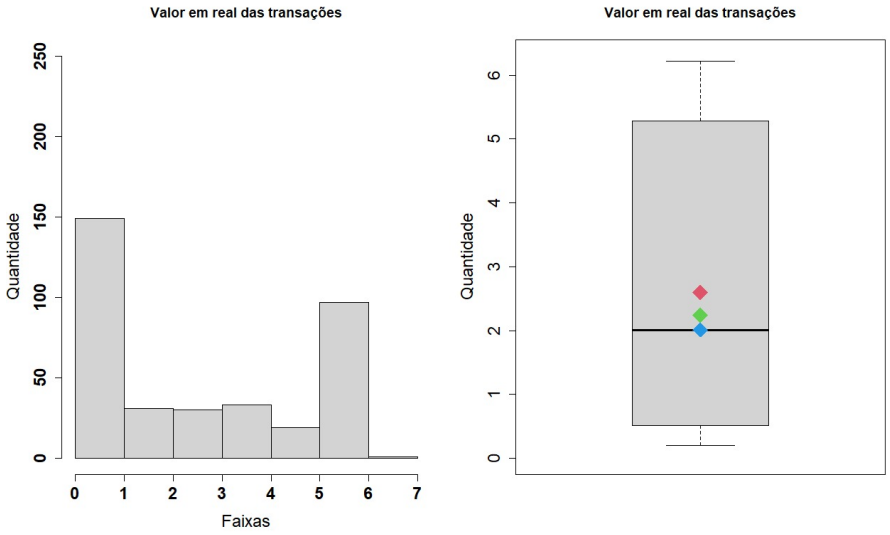


Fonte: o autor.

5.4.5 Análise do Real

A Figura 49 exibe o histograma e *boxplot* para os valores totais em real brasileiro de cada cenário, todos somados. O menor valor coletado foi R$ 0,198463987 reais e o maior foi R$ 6,220847873 reais, ou seja, os valores do tempo nesse tipo de transação estão entre esse intervalo. A mediana foi R$ 2,011508446 reais, ou seja, metade das transações ocorreu com um valor menor que R$ 2,011508446 reais e a outra metade ocorreu com valor maior que R$ 2,011508446 reais. O primeiro quartil do *boxplot* possui o valor de R$ 0,51 reais, ou seja, um quarto das transações foram com um valor menor que R$ 0,51 reais. Já o terceiro quartil do *boxplot* tem valor de R$ 5,237378643 reais, ou seja, 75% das transações ocorreram com valor menor que R$ 5,237378643 reais. Neste cenário, pode-se afirmar que o alcance da transação com maior valor e a de menor valor (0,198463987 - 6,220847873) foi de R$ 6,022383886 reais. No histograma também é possível visualizar as quantidades desse tipo de transação que foram realizadas por intervalo do valor em reais gasto nas transações.

Figura 49 – Análise do Valor em Real



Fonte: o autor.

5.5 Modelo Analítico de Gas

Diante dos dados obtidos nos experimentos que foram realizados com a aplicação, desenvolveu-se um modelo analítico. Este modelo considera apenas o valor pago de gas sobre as transações enviadas para a rede *blockchain*, e sua intenção é estimar o valor de gas para os quatro métodos do contrato inteligente desenvolvido, possibilitando expandir as análises com

cenários projetados com muitos acessos.

Os dados de gas são exibidos no Apêndice A nos Quadros 3 e 4 divididos por cenário de teste. Os cenários de teste são os mesmos apresentados na Seção 5.3, e foram: Criação de Campanha, Investimento dos Usuários, Campanha com Quantidade de Ether e Poder de Voto.

A Figura 50 exibe os valores que foram coletados, gasto com gas, nos quatro cenários de teste e também a variação desse valor para cada um deles. Alguns dos cenários apresentaram mais de um valor para o seu gasto de gas. Os métodos executados nas transações em cada cenário são elencados a seguir:

- ***CreateCampain*:** representa a criação de uma nova campanha;
- ***Contribute*:** representando a entrada de um investidor em uma campanha, enviando ether para determinado projeto;
- ***CreateRequest*:** usado pelo gerente de projeto visando utilizar o dinheiro arrecadado criando uma requisição;
- ***AproveRequest*:** utilizado por aqueles que fazem parte da campanha como investidor aprovando as requisições criadas pelo gerente do projeto.

Figura 50 – Valores de Gas por Método

Métodos	Qtd de Vezes x Gas
CreateCampaign	1 x 55006 29 x 55051 60 x 550051
Contribute	1 x 67809 89 x 30809
CreateRequest	2 x 388375 88 x 371275
AproveRequest	90 x 70516

Fonte: o autor.

Para o modelo analítico considerou-se que o valor de gas com mais repetições seria definido como o valor padrão para o gasto de gas em cada cenário. A Figura 51 exibe os valores padrão encontrados durante os testes para representar o gasto de gas de cada tipo de transação testada. Destaca-se que esses valores são apenas para os resultados apresentados nesse trabalho, e em uma rede de testes, podendo ter valores bem diferentes em uma rede *blockchain* real.

Figura 51 – Valores de Gas por Método

Métodos	Gas
CreateCampaign	550051
Contribute	30809
CreateRequest	371275
AproveRequest	70516

Fonte: o autor.

Com esses valores definidos foi possível propor a Equação 5.1 para o modelo analítico de análise de gas, onde cada nome do método corresponde a uma variável a ser substituída pela quantidade de chamadas ou requisições a esse método. Essa equação considera todos os métodos e seus respectivos valores de gas, formando assim a equação que define a quantidade estimada de gas. Uma vantagem é que ela pode ser utilizada para os mais diversos cenários, e com quantidades variadas e grandes de requisições, permitindo simular a quantidade de usuários da aplicação, por exemplo.

$$\begin{aligned} ModeloDeGas = {} & (CreateCampaign * 55051) + (Contribute * 30809) \\ & + (CreateRequest * 371275) + (AproveRequest * 70516) \end{aligned} \tag{5.1}$$

Diante da equação definida, tornou-se possível estimar a quantidade de gas que seria gasto em cenários diversos. Para exemplificar seu uso, três cenários foram definidos, variando o número de vezes em que cada método é executado. Para uma melhor visualização monetária dos cenários foi utilizado o valor do ether, coletado no dia do ultimo experimento 26 de junho de 2022. Um ether estava valendo US$ 1.107,27 dólares e um dólar estava cotado a R$ 5,23 reais.

O valor médio da taxa cobrada pelo gas coletado nos experimentos foi de de 1,67 Gwei como exibido no Apêndice A - Quadro 4, com ele foi calculado os valores em ether, dólar e real nos cenários analisados com o modelo analítico.

5.5.1 Cenário 1 - Modelo Analítico

O primeiro cenário simula criação de 10 campanhas, 1.000 contribuições, 50 requisições e foi indicado que cada requisição teria que ser votada por todos os investidores, totalizando em 50.000 aprovações. Utilizando a equação definida no modelo analítico, chegou-se ao valor de 3.575.723.260 a ser pago pelo gas de todas as transações desse cenário, apresentado a seguir:

$$\begin{aligned} ModeloDeGas = \quad & (CreateCampaign * 55051) + (Contribute * 30809) \\ & + (CreateRequest * 371275) + (AproveRequest * 70516) \\ ModeloDeGas = \quad & (10 * 55051) + (1.000 * 30809) \\ & + (50 * 371275) + (50.000 * 70516) \\ ModeloDeGas = \quad & (550.510) + (30.809.000) + (18.563.750) + (3.525.800.000) \\ & ModeloDeGas = 3.575.723.260 \end{aligned}$$

Para obter o valor estimado a ser pago pelo gas de todas as 51.060 transações realizadas neste cenário em gwei, é preciso multiplicar a quantidade de gas estimado pelo valor de sua taxa. Ao obter o valor em gwei é possível valorar em unidades de ether, dólar ou reais. Com isso, a realização desse primeiro cenário gastaria em gas o equivalente a 5.971.457.844,2 gwei, ou 11,37 ether. Transformando para dólares ficaria assim US$ 12.589,65 dólares, equivalente à R$ 65.843,86 reais aproximadamente.

5.5.2 Cenário 2 - Modelo Analítico

Este cenário simula criação de 25 campanhas, 500 contribuições, 100 requisições e foi indicado que todas as requisições deveriam ser votadas por pelo menos mais de 50% dos investidores, com isso 25.100 aprovações. Utilizando então a equação definida no modelo analítico, pode-se chegar ao valor de 1.887.324.275 a ser pago pelo gas de todas as transações desse cenário, como é demonstrado a seguir:

$$\begin{aligned} ModeloDeGas = \quad & (CreateCampaign * 55051) + (Contribute * 30809) \\ & + (CreateRequest * 371275) + (AproveRequest * 70516) \\ ModeloDeGas = \quad & (25 * 55051) + (500 * 30809) \\ & + (100 * 371275) + (26.000 * 70516) \\ ModeloDeGas = \quad & (1.376.275) + (15.404.500) + (37.127.500) + (1.833.416.000) \\ & ModeloDeGas = 1.887.324.275 \end{aligned}$$

Para obter o valor estimado a ser pago pelo gas de todas as 26.625 transações realizadas neste cenário em gwei, é preciso multiplicar a quantidade de gas estimado pelo valor de sua taxa. Ao obter o valor em gwei é possível valorar em unidades de ether, dólar ou reais. Com isso, a realização desse segundo cenário gastaria em gas o equivalente a 3.151.831.539,25 gwei, ou 5,9471 ether. Transformando para dólares ficaria assim US$ 6.585,04 dólares, equivalente à R$ 34.439,75 reais aproximadamente.

5.5.3 Cenário 3 - Modelo Analítico

Este cenário simula criação de 50 campanhas, 10.000 contribuições, 250 requisições e foi indicado que menos de 50% das requisições receberiam voto suficientes para sua aprovação pelos investidores, com isso 1.000.000 aprovações. Utilizando então a equação definida no modelo analítico, pode-se chegar ao valor de 70.919.661.300 a ser pago pelo gas de todas as transações desse cenário, como é demonstrado a seguir:

$$\begin{aligned} ModeloDeGas = \quad & (CreateCampaign * 55051) + (Contribute * 30809) \\ & + (CreateRequest * 371275) + (AproveRequest * 70516) \\ ModeloDeGas = \quad & (50 * 55051) + (10.000 * 30809) \\ & + (250 * 371275) + (1.000.000 * 70516) \\ ModeloDeGas = \quad & (2.752.550) + (308.090.000) + (92.818.750) + (70.516.000.000) \\ & ModeloDeGas = 70.919.661.300 \end{aligned}$$

Para obter o valor estimado a ser pago pelo gas de todas as 2.010.300 transações realizadas neste cenário em gwei, é preciso multiplicar a quantidade de gas estimado pelo valor de

sua taxa. Ao obter o valor em gwei é possível valorar em unidades de ether, dólar ou reais. Com isso, a realização desse terceiro cenário gastaria em gas o equivalente a 118.435.834.371 gwei, ou 224,28 ether. Transformando para dólares ficaria assim US$ 248.338,51 dólares, equivalente à R$ 1.298.810,40 reais aproximadamente.

5.6 Discussões Gerais

Esta seção faz uma discussão geral sobre os dados coletados nos testes da aplicação. Adicionalmente, também é comentado a respeito das limitações encontradas durante o processo de desenvolvimento e aplicação da proposta, além das ameaças identificadas à validação deste trabalho.

Diante dos dados coletados nos testes, foi observado que o valor médio pago por transação foi de R$ 2,60 reais, não foi considerado um valor alto para poder obter os benefícios que os contratos inteligentes oferecem. Um valor baixo pago para obtenção da rastreabilidade, imutabilidade dos dados e outras características viabilizando o uso da abordagem, que são características de uma *blockchain*.

O tempo entre o envio da transação para a rede e o recebimento da sua resposta com sucesso ou não, pode impactar em alguns tipos de aplicação, um sistema de banco por exemplo, ao escolher o uso de uma solução *blockchain* pode sofrer com os atrasos gerados pela validação dos blocos. Como foi exibido, o tempo de resposta médio fica em torno de 25,1 segundos. Em alguns casos pode não ser muita coisa, mas em outros, como o exemplo do banco, esse tempo pode gerar danos irreparáveis, tornando o uso da solução inviável neste caso.

Com o uso da *blockchain* foi possível acessar dados de todas as transações analisadas, sendo possível visualizar posteriormente suas execuções. Informações como *hash* de origem - pode representar uma carteira de um usuário ou um contrato inteligente; *hash* de destino - representa qual carteira recebeu determinada quantidade de ether; data e hora da confirmação das transação na rede de maneira precisa. Todos esses dados podem ajudar na auditoria de um projeto, seja por parte dos investidores ou parte dos criadores.

O usuário interessado em verificar todas as transações ocorridas em uma determinada campanha pode fazer uso da ferramenta Etherscan e com o *hash* do contrato inteligente conseguir de maneira rápida e pratica todas as informações de transações do contrato. Isso se deve a transparência oferecida pela rede *blockchain*. Os dados além de imutáveis são acessíveis por qualquer usuário que tenho conhecimento do *hash* do contrato da campanha. Com uma maior

transparência no processo do *crowdfunding*, os seus investidores podem se sentir mais seguros para investir e assim aumentar as chances dos projetos saírem do papel. Destaca-se que essa análise é mais do ponto de vista técnico. Uma análise de uso mais adequada para o usuário final, que pode não entender nada de *blockchain*, deve ser projetada considerando requisitos funcionais, usabilidade e a experiência do usuário.

Para o usuário final, uma das principais diferenças entre sites tradicionais de *crowdfunding* e a aplicação proposta identificada durante os testes é o fato de existir um *plugin* para autorização das transações. O tempo para validação de uma transação também foi identificado como uma das possíveis diferenças. O fato dos investidores passarem a ter poder de julgar gastos feitos para o desenvolvimento dos projetos, pode ajudar na confiança dos investidores. Outra diferença é a existência de uma espécie de extrato contendo todos os gastos, desde a criação do contrato inteligente até o momento desejado, gerando transparência nos gastos.

As tecnologias utilizadas na abordagem deste trabalho se mostraram simples de implementação, não necessitando de um estudo mais elaborado no desenvolvimento de uma aplicação de teste. Em uma busca rápida foi possível encontrar tutoriais com aplicações de exemplo que ajudam no desenvolvimento de aplicações mais elaboradas. A documentação da linguagem Solidity[12] é bem completa, o que facilita a do contrato inteligente. No entanto, para desenvolvimento do *front-end* foi necessário um maior conhecimento da biblioteca React[13]. O *plugin* Metamask oferece uma grande ajuda no envio das transações para a rede. Ele torna transparente o comportamento da aplicação ao enviar moedas de um lugar para outro na rede *blockchain*.

O algoritmo de consenso tem seu impacto percebido na aplicação ao ter a necessidade de aguardar um pouco mais que em sistemas convencionais a confirmação de uma transação. Para cada transação o algoritmo auxilia na validação do novo bloco. Assim, usuários não habituados acabam sentido este impacto.

Este trabalho é uma pesquisa que pode impactar na escolha da utilização de uma rede *blockchain*. Possibilitando a pessoa que nunca teve contato ou experiência com o assunto pode obter informações de como funciona e também ver como ela se comporta na prática em comparação com aplicações comuns.

Com o uso de uma solução *blockchain*, os custos com infraestrutura são reduzidos devido a não necessidade de uma infraestrutura robusta com alto poder de processamento para

[12] https://docs.soliditylang.org/en/v0.8.16/ Acesso em: 08 ago. 2022
[13] https://pt-br.reactjs.org/docs/getting-started.html Acesso em: 08 ago. 2022

a aplicação. O processo utilizado para execução dos métodos da aplicação fica a cargo dos mineradores. A aplicação passa a fazer apenas consultas na rede para obter as informações dos contratos inteligentes. A consulta aos dados do contrato não gera custos aos usuários.

Durante o processo de desenvolvimento deste trabalho existiram alguns obstáculos. Um desses obstáculos, foi o entendimento de como funcionava a comunicação entre uma aplicação *desktop* e a rede *blockchain*. Foi preciso buscar conhecimento sobre quais componentes seriam necessários para uma interação direta, feita pela aplicação. Essa busca foi feita tentando alterar o mínimo possível do processo já conhecido por usuários de sites *crowdfunding* convencionais.

Este trabalho contribui com uma análise de viabilização de uma aplicação que gera mais segurança aos usuários de sites *crowdfunding*. Nele é possível ter uma ideia de quais valores a ser pago durante a utilização da aplicação em uma rede *blockchain*. É fornecida também uma análise geral do tempo de espera para a realização de ações na rede. Nos dias atuais, onde os usuários medem a qualidade de um sistema por sua rapidez de resposta, um usuário desavisado ou sem conhecimento prévio, pode sentir desconforto ao ter que esperar de 15 a 30 segundos em média para ver a confirmação de sua ação. Este trabalho oferece como contribuição científica uma revisão sistemática a respeito do uso de *blockchain* para *crowdfunding*, apontando o estado da arte diante do cenário acadêmico e identificando o crescimento dos estudos voltados ao uso da tecnologia *blockchain* com foco no *crowdfunding*. Esta pesquisa contribui para a comunidade *blockchain* no desenvolvimento de uma aplicação que utiliza uma rede disponibilizada pela Ethereum para testes. Ajuda também na validação dos conceitos inerentes à tecnologia, oferecendo uma visão da integração de uma *blockchain* com outras tecnologias e ferramentas.

Como aspectos sociais, este trabalho ajuda no entendimento do financiamento coletivo *crowdfunding* e da tecnologia *blockchain* com uso de contratos inteligentes. Também exibe as vantagens de sua utilização em relação a transparência e imutabilidade dos dados. Também é possível mensurar valores gastos em sua utilização. O uso de uma aplicação como a proposta neste trabalho pode melhorar a vida dos usuários de *crowdfunding* gerando mais confiança e facilitando a prestação de contas dos projetos junto aos investidores, o que pode ocasionar a atração de mais investidores devido a maior transparência. Com esse aumento de investidores, cada vez mais projetos podem alcançar seu desenvolvimento.

Utilizando a tecnologia *blockchain* neste trabalho foi possível identificar a existência

de um impacto para pessoas que irão utilizar tal solução. Para existir o uso correto da aplicação faz-se necessário o conhecimento prévio sobre *plugins*, carteiras digitais, redes *blockchain* e seus conceitos. Diferente das aplicações comuns onde o usuário apenas navega no site onde a campanha foi hospedada e faz suas escolhas.

Percebeu-se que é necessário conduzir um estudo mais detalhado voltado ao público-alvo, aqueles que utilizam sites *crowdfunding* convencionais, buscando respostas, barreiras e impedimentos no uso da *blockchain*. Com esse estudo realizado e juntamente com o desenvolvido neste trabalho é possível obter uma melhor visão a respeito da solução.

Como impactos sobre aplicações e sistemas, foi identificado o problema do tempo de resposta para uma transação ser finalizada e adicionada na rede *blockchain*. Existem aplicações que dependendo da ação que se deseja realizar, sua resposta com a confirmação necessita ser processada com rapidamente.

5.6.1 Limitações do Trabalho e Ameaças à Validade

Uma observação importante é que na solução apresentada não se levou em consideração a inserção de outros dados que descrevam melhor as campanhas em si. Vídeos, gráficos, imagens e outras forma de recursos digitais poderiam ter sido enviados para a rede. Isso devido ao escopo da pesquisa se atentar em buscar respostas a respeito do valor a ser pago ao utilizar uma solução *blockchain*, assim como o impacto do tempo de atraso em transações.

Além da não utilização de alguns recursos digitais na descrição das campanhas, como acontece em sites de *crowdfunding*, não foram implementadas todas as regras de negócio presentes nos sites tradicionais de *crowdfunding*. Funções como estabelecimento de metas de arrecadação, o que fazer com o dinheiro arrecadado caso a meta não seja atingida, dentre outras funcionalidades.

Não foi possível a automatização das transações, ou seja, cada transação foi executada individualmente. Com isso não foi possível medir e observar o comportamento da solução com transações simultâneas. Testes com usuários utilizadores de sites de *crowdfunding* convencionais não foram realizados. Não foram devido à dificuldade de encontrar pessoas que possuam esse perfil. Esses testes são importantes na obtenção de dados como dificuldades encontradas na utilização da nova solução. Com esses dados seria possível obter uma visão mais ampla, melhorando o entendimento a respeito da viabilidade da proposta.

Alguns pontos foram observados como ameaça à validade deste trabalho, um deles

é o fato do uso de uma aplicação externa, o Metamask, *plugin* indispensável para utilização da solução desenvolvida. A integração da aplicação com a rede *blockchain* tem uma grande dependência do uso do *plugin* Metamask. Ele desempenha um papel muito importante na arquitetura proposta. Nele é feita toda a autorização de gastos. Para um teste mais automatizado essa solução teria problemas, pois cada transação feita, tem a intervenção humana para permitir que a transação seja enviada para a rede, isso da maneira que foi abordada neste trabalho.

Uma outra observação importante a ser levada em consideração é que o valor do ether tem variações ao longo do tempo. O valor do ether em 01 Abril de 2021 aproximadamente às 20:00 da noite era de R$ 11.306,89 reais. Esse valor foi coletado durante os testes preliminares feitos no desenvolvimento da aplicação deste trabalho. Nos dias em que os testes finais foram realizados, o valor médio do ether ficou em R$ 6.242,69 reais. O fato do valor aumentar ou diminuir bastante deve ser levado em consideração ao escolher utilizar a solução com *blockchain*. No dia 08 de novembro do ano de 2021 o ether chegou a valer R$ 26.719,26 reais.

Com isso, configura-se uma ameaça à validade dos testes realizados, pois o valor das transações podem variar junto com o valor do ether. Com essas variações, as transações podem ficar mais custosas a ponto de inviabilizar o uso desta solução e alterar bastante os valores dos dados coletados.

6 CONCLUSÕES

Com o avanço nos estudos a respeito da tecnologia *blockchain*, uma variedade de aplicações está surgindo rapidamente. No campo do financiamento coletivo ela se encontra num estágio inicial, onde algumas organizações e a academia buscam os benefícios dessa tecnologia para a área do *crowdfunding*.

De acordo com os resultados apresentados nos cenários de avaliação, a solução proposta baseada na tecnologia *blockchain* poderia sim proporcionar uma alternativa viável na obtenção de poderes sobre os projetos e também na auditoria dentro do processo de *crowdfunding*. Isso devido a utilização de uma plataforma segura para financiadores enviarem suas contribuições e votarem a respeito dos gastos, aumentando a confiança e transparência no uso do dinheiro arrecadado.

Ao utilizar a tecnologia *blockchain* desafios inerentes a seu uso surgem, portanto ao buscar uma avaliação de praticidade em uma solução com base em *blockchain*, os profissionais devem fazer uma análise cuidadosa da viabilidade das soluções capazes de cobrir os diferentes requisitos de negócios. Por conta disso, existe uma crescente exploração sobre os potenciais usos da tecnologia *blockchain*.

Foram apontadas como as principais vantagens encontradas na solução proposta: ajudar os investidores terem mais controle sobre o gasto do dinheiro arrecadado nas campanhas, ajudar também na obtenção de informações sobre os gastos envolvendo o projeto, aumentando a confiança e dispondo de uma maior transparência. A qualquer momento é possível verificar informações sobre todas as transações realizadas em determinada campanha.

6.1 Considerações Finais

Neste trabalho foi proposto um modelo de arquitetura que utiliza a tecnologia *blockchain*, no qual foi elaborada e desenvolvida uma aplicação para fornecer um ambiente mais democrático e seguro para investidores da modalidade *crowdfunding*. O objetivo geral deste trabalho foi gerar uma solução *crowdfunding* juntamente com uma rede *blockchain* aumentando a confiança no processo de investimentos em projetos de financiamento coletivo. Por fim, foi realizado um estudo sobre a viabilidade e o desempenho da aplicação criada.

Uma padronização no desenvolvimento de aplicações similares que integram serviços diversos, de diferentes tecnologias (*web*, microsserviços, etc), com *blockchain* é possibilitada

com a implementação da arquitetura de referência. Fazendo isso, os benefícios alcançados com o uso de *blockchain* podem ser compartilhados com variados serviços. Uma das funções da arquitetura de referência é possibilitar a identificação das camadas mais utilizadas, fazer a organização delas, melhorando a compreensão.

Seguindo no mesmo contexto, um problema relevante e oportuno foi abordado ao se propor e instanciar uma arquitetura de referência aproveitando a tecnologia moderna *blockchain*. Diante do desenvolvimento e a experiência adquirida nesta pesquisa, buscou-se encontrar respostas para algumas questões relevantes de pesquisa.

Considerando a primeira questão elencada no trabalho "*Quais os principais desafios tecnológicos que os investidores e os criadores de projeto podem enfrentar para alterar a forma que o crowdfunding possui em gestão financeira utilizando a tecnologia blockchain?*", destaca-se por meio do aprendizado adquirido durante a pesquisa e as percepções durante os testes que é importante ter um conhecimento prévio a respeito do funcionamento das transações em uma rede *blockchain*, principalmente a respeito de seus custos e tempo que leva para suas validações.

Analisando a segunda questão de pesquisa "*É possível desenvolver uma solução baseada em blockchain que contemple confiabilidade, transparência e segurança, buscando um maior número de investidores para projetos inovadores?*", como apontado neste trabalho é sim possível a criação de uma solução baseada no uso dessa tecnologia. Dessa maneira, acredita-se que a tecnologia *blockchain* apresenta um potencial para suprir problemas de confiança e segurança em razão dos dados tratados serem imutáveis. Também em relação a transparência, os gastos realizados por uma campanha ficam disponíveis a qualquer usuário interessado, bastando ter conhecimento do *hash* do contrato inteligente dessa campanha. Tendo isso em vista, acredita-se na possibilidade de aumento no número de investidores.

6.2 Publicações

Alguns artigos foram elaborados e submetidos durante a construção desta pesquisa, sendo trabalhos que se relacionam com o tema *blockchain*. O processo de escrita desses artigos auxiliou a fornecer um melhor entendimento a respeito da tecnologia, ampliando o conhecimento a seu respeito. O Quadro 2 apresenta em forma de lista os artigos publicados, seja em conferência ou em periódicos.

Quadro 2 – Artigos publicados em conferências e periódicos

Artigo	**Veículo de Publicação**
Um Estudo Preliminar das Relações entre Características de Blockchain e a Aplicação na Sociedade	V Workshop Sobre Aspectos Sociais, Humanos e Econômicos de Software (WASHES 2020) (COUTINHO *et al.*, 2020)
Uma Análise Inicial sobre a Aplicação de Blockchain na Sociedade	II Workshop Sobre as Implicações da Computação na Sociedade (WICS 2021) (COUTINHO *et al.*, 2021)
Avaliando o Custo de Contratos Inteligentes em Aplicações Blockchain por meio de Ambientes de Simulação	II Workshop de Modelagem e Simulação de sistemas intensivos em Software (MSSiS 2020) (COUTINHO *et al.*, 2020)
Oportunidades de Pesquisa em Blockchain em Tempos de Pandemia	Revista Sistemas e Mídias Digitais (RSMD 2020) (BEZERRA *et al.*, 2020)
A Blockchain Solution for Crowdfunding and Cost Analysis	Euro American Conference on Telematics and Information Systems (EATIS 2022) (MAIA; COUTINHO, 2022)
Aplicações e Impactos da Blockchain na Sociedade	Colóquio Blockchain e Web Descentralizada (CSBC 2022/WBCI 2022) (COUTINHO *et al.*, 2022)
Analyzing a Blockchain Application for the Educational Domain from the Perspective of a Software Ecosystem	III Workshop Sobre as Implicações da Computação na Sociedade (WICS 2022) (ABREU *et al.*, 2022)

Fonte: o autor.

6.3 Trabalhos Futuros

Nesta seção os potenciais trabalhos futuros que podem ser gerados a partir dessa pesquisa serão descritos. Alguns são mais orientados à aplicação em si e outros para a infraestrutura.

Como trabalhos futuros, pretende-se explorar a linguagem Solidity para que a aplicação não dependa do uso do Metamask para utilização da carteira digital da Ethereum. Assim seria possível executar novos testes com transações simultâneas, visualizar o comportamento de simulações com uma escala maior e analisar o desempenho da aplicação.

Também como trabalhos futuros, pretende-se fazer um cadastro completo de campanhas, com a possibilidade de *upload* de arquivos como fotos e vídeos, tornando assim mais parecido com os sites convencionais. Observou-se que o tamanho do bloco a ser minerado é de muita importância, com isso, como trabalhos futuros pretende-se fazer o uso de um banco de dados convencional tentando ajudar a reduzir custos, guardando os dados menos sensíveis nele. No caso das informações nas descrições das campanha e também nas descrições das requisição, elas poderiam ser guardadas diretamente em um banco de dados como o MongoDB ou até mesmo num relacional PostgresSQL. Com esses ajustes, seria possível que o valor pago pela validação dessas transações diminuísse consideravelmente, ajudando ainda mais na viabilização do projeto.

Para buscar ampliar a análise de custos gerados com a utilização de uma rede *blockchain* em uma solução para *crowdfunding*, pretende-se fazer testes da mesma aplicação, mas utilizando uma ou mais redes diferentes da Ethereum que também dão suporte aos contratos inteligentes, como por exemplo as redes Hyperledger, Counterparty e Polkadot. Com os testes realizados é possível fazer comparações como qual rede oferece as melhores vantagens para a proposta deste trabalho.

Um outro trabalho futuro seria analisar o comportamento da rede *blockchain* e da aplicação com o aumento de usuários utilizando a aplicação. Neste trabalho foi explorado testes com apenas um usuário. Com essa análise, a aplicação vai se aproximar mais da realidade onde podem existir diversos usuários ao mesmo tempo utilizando a aplicação. Desta maneira auxiliando no estudo da viabilidade da solução.

Ainda como trabalho futuro, resta conduzir uma avaliação da aplicação com usuários de sites convencionais de *crowdfunding*. A avaliação da aplicação com o público-alvo pode ajudar a entender dúvidas que podem surgir em sua utilização e assim melhorar a aplicação. A própria aplicação pode ser avaliada do ponto de vista de usabilidade e utilidade por parte dos usuários.

REFERÊNCIAS

ABREU, A.; COUTINHO, E.; BEZERRA, W.; MAIA, D.; GOMES, A.; SANTOS, I. Analyzing a blockchain application for the educational domain from the perspective of a software ecosystem. In: III WORKSHOP SOBRE AS IMPLICAÇÕES DA COMPUTAÇÃO NA SOCIEDADE. Porto Alegre, RS **Anais** [...]: SBC, 2022. p. 85–92. ISSN 2763-8707. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/20734. Acesso em: 10 ago. 2022.

ABREU, A. W. d. S. **Uma abordagem baseada em blockchain para armazenamento e controle de acesso aos dados de certificados de alunos do ensino superior**. 2020. Dissertação (Mestre em Computação) – Universidade Federal do Ceará, Quixadá, 2020, Disponível em: https://repositorio.ufc.br/handle/riufc/55477. Acesso em: 10 ago. 2022.

ABREU, A. W. S.; COUTINHO, E. F.; BEZERRA, C. I. A blockchain-based architecture for query and registration of student degree certificates. In: 14TH BRAZILIAN SYMPOSIUM ON SOFTWARE COMPONENTS, ARCHITECTURES, AND REUSE. Natal, RN **Proceedings** [...], 2020. p. 151–160. Disponível em: https://dl.acm.org/doi/abs/10.1145/3425269.3425285?casa_token=MC0QHUp7EB4AAAAA:R2vP041YQtOxznzNqlwZynssv4E3-iEsTHr5dyTUeCoHAyqgk6U8-sbZVl9JYjgQ5VilS-2-7c_TNMs. Acesso em: 10 ago. 2022.

AHMAD, N. A. N.; RAHMAN, S. A. H. S. A. Applying ethereum smart contracts to blockchain-based crowdfunding system to increase trust and information symmetry. In: 7TH INTERNATIONAL CONFERENCE ON COMPUTER TECHNOLOGY APPLICATIONS. Vienna, Austria **Proceedings** [...], 2021. p. 53–59. Disponível em: https://dl.acm.org/doi/fullHtml/10.1145/3477911.3477920?casa_token=-2ao6rX3WsMAAAAA:xYE2x6E-zjb2N9zRIAwTc69nc1yPGyPcSvcstumxdUo8ShhWVE6J0L7eD7us01BRsOedU469bO_oVTA. Acesso em: 10 ago. 2022.

AITZHAN, N. Z.; SVETINOVIC, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. **IEEE Transactions on Dependable and Secure Computing**, IEEE, v. 15, n. 5, p. 840–852, 2016. Disponível em: https://ieeexplore.ieee.org/abstract/document/7589035/. Acesso em: 10 ago. 2022.

ALAMMARY, A.; ALHAZMI, S.; ALMASRI, M.; GILLANI, S. Blockchain-based applications in education: A systematic review. **Applied Sciences**, Multidisciplinary Digital Publishing Institute, v. 9, n. 12, p. 2400, 2019. Disponível em: https://www.mdpi.com/2076-3417/9/12/2400. Acesso em: 10 ago. 2022.

ALBERT, E.; CORREAS, J.; GORDILLO, P.; ROMÁN-DÍEZ, G.; RUBIO, A. Gasol: Gas analysis and optimization for ethereum smart contracts. In: BIERE, A.; PARKER, D. (Ed.). **Tools and Algorithms for the Construction and Analysis of Systems**. Cham: Springer International Publishing, 2020. p. 118–125. ISBN 978-3-030-45237-7. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-45237-7_7. Acesso em: 10 ago. 2022.

ALHARBY, M.; MOORSEL, A. van. Blockchain-based smart contracts: A systematic mapping study. **arXiv preprint arXiv:1710.06372**, 2017. Disponível em: https://arxiv.org/abs/1710.06372. Acesso em: 10 ago. 2022.

ALI, N. S.; SHIBGHATULLAH, A. Protection web applications using real-time technique to detect structured query language injection attacks. **International Journal of Computer**

Applications, Foundation of Computer Science, v. 149, n. 6, p. 26–32, 2016. Disponível em: https://portal.arid.my/Publications/e54ca493-857f-47.pdf. Acesso em: 10 ago. 2022.

ALIAGA, Y. E. M.; HENRIQUES, M. A. A. Uma comparação de mecanismos de consenso em blockchains. In: ENCONTRO DOS ALUNOS E DOCENTES DO DEPARTAMENTO DE ENGENHARIA DE COMPUTAÇÃO E AUTOMAÇÃO INDUSTRIAL. Campinas, SP **Proceedings**: [*S. n.*], 2017. p. 26–27. Disponível em: https://www.escavador.com/sobre/377860042/yoshitomi-eduardo-maehara-aliaga. Acesso em: 10 ago. 2022.

ALIAGA, Y. E. M.; MARTINS, D. F. G.; HENRIQUES, M. A. A. Proof-of-stake baseado em tempo discreto. In: II WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIA E APLICAÇÕES. Gramado, RS **Anais** [...], 2019. Disponível em: https://sol.sbc.org.br/index.php/wblockchain/article/view/7487. Acesso em: 10 ago. 2022.

ANBIMA. **CVM edita regras para crowdfunding**. 2017. Disponível em: https://www.anbima.com.br/pt_br/informar/regulacao/informe-de-legislacao/cvm-edita-regras-para-crowdfunding.htm. Acesso em: 09 ago. 2022.

ARAUJO, V. S. de; FREITAS, M. G. de; MARTIN, M. V. A. Blockchain e o futuro dos contratos administrativos. **Revista Quaestio Iuris**, v. 14, n. 01, p. 481–503, 2021. Disponível em: https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/48956. Acesso em: 10 ago. 2022.

ASHARI, F.; CATONSUKMORO, T.; BAD, W. M.; SFENRANTO, W. *et al.* Smart contract and blockchain for crowdfunding platform. **International Journal of Advanced Trends in Computer Science and Engineering**, p. 3036–3041, 2020. Disponível em: https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-822263. Acesso em: 10 ago. 2022.

ASSIS, C. V. S. R. d. **Análise e detecção de Ponzi schemes em contratos inteligentes na rede Ethereum**. 2021. Monografia (TCC) – Faculdade de Engenharia - Universidade Federal de Mato Grosso, Cuiabá, MT, 2021, Disponível em: https://bdm.ufmt.br/handle/1/2001. Acesso em: 10 ago. 2022.

ASTE, T.; TASCA, P.; MATTEO, T. D. Blockchain technologies: The foreseeable impact on society and industry. **Computer**, IEEE COMPUTER SOC, v. 50, n. 9, p. 18–28, 2017. Disponível em: https://kclpure.kcl.ac.uk/portal/files/82188755/Blockchain_Technologies_ASTE_Accepted_5_May_17_GREEN_AAM.pdf. Acesso em: 10 ago. 2022.

BACH, L. M.; MIHALJEVIC, B.; ZAGAR, M. Comparative analysis of blockchain consensus algorithms. In: 41ST INTERNATIONAL CONVENTION ON INFORMATION AND COMMUNICATION TECHNOLOGY, ELECTRONICS AND MICROELECTRONICS (MIPRO). New York, NY, USA **Conference** [...]: IEEE, 2018. p. 1545–1550. Disponível em: https://ieeexplore.ieee.org/abstract/document/8400278. Acesso em: 10 ago. 2022.

BARBER, S.; BOYEN, X.; SHI, E.; UZUN, E. Bitter to better—how to make bitcoin a better currency. In: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY. Berlin, Heidelberg **Conference** [...], 2012. p. 399–414. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-32946-3_29. Acesso em: 10 ago. 2022.

BARCELOS, F. A.; MARTINS, J. V. d. L. **Aplicabilidade da blockchain no sistema de eleição departamental da UTFPR campus Ponta Grossa**. 2020. Monografia (TCC) – Universidade Tecnológica Federal do Paraná, Ponta Grossa - Paraná, PR, 2020, Disponível em: http://riut.utfpr.edu.br/jspui/handle/1/26445. Acesso em: 10 ago. 2022.

BATUBARA, F. R.; UBACHT, J.; JANSSEN, M. Challenges of blockchain technology adoption for e-government: a systematic literature review. In: 19TH ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH: GOVERNANCE IN THE DATA AGE. Gramado, RS **Proceedings** [...], 2018. p. 1–9. Disponível em: https://dl.acm.org/doi/abs/10.1145/3209281.3209317. Acesso em: 10 ago. 2022.

BEGINNERS, E. **What is Ethereum?** 2021. Disponível em: https://ethereum.org/en/what-is-ethereum/. Acesso em: 09 ago. 2022.

BEZERRA, W. L. B.; MAIA, D. J. H.; ABREU, A. W.; COUTINHO, E. F. Oportunidades de pesquisa em blockchain em tempos de pandemia. **Revista Sistemas e Mídias Digitais (RSMD)**, v. 5, n. 1, julho 2020. ISSN 2525-9555. Disponível em: http://revistasmd.virtual.ufc.br/arquivos/volume-5/numero-1/rsmd-v5-n1-1.pdf. Acesso em: 10 ago. 2022.

BILLERT, M. Yes, we can! blockchain based crowdfunding and crowdworking. In: PRE-ICIS SIGBPS WORKSHOP ON BLOCKCHAIN AND SMART CONTRACT (PRE-ICIS). Munique, Alemanha **Proceedings** [...], 2019. Disponível em: https://www.alexandria.unisg.ch/258635/. Acesso em: 10 ago. 2022.

BITCOIN.ORG. **O que é mineração de Bitcoin?** 2022. Disponível em: https://bitcoin.org/pt_BR/faq#o-que-significa-sincronizando-e-porque-demora-tanto. Acesso em: 23 mar. 2022.

BITFURY, G. Proof of stake versus proof of work. **White paper, Sep**, v. 810, 2015. Disponível em: bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf. Acesso em: 10 ago. 2022.

BOGUSZ, C. I.; LAURELL, C.; SANDSTRÖM, C. Tracking the digital evolution of entrepreneurial finance: the interplay between crowdfunding, blockchain technologies, cryptocurrencies, and initial coin offerings. **IEEE Transactions on Engineering Management**, IEEE, v. 67, n. 4, p. 1099–1108, 2020. Disponível em: https://ieeexplore.ieee.org/abstract/document/9115055/. Acesso em: 10 ago. 2022.

BOSU, A.; IQBAL, A.; SHAHRIYAR, R.; CHAKRABORTY, P. Understanding the motivations, challenges and needs of blockchain software developers: A survey. **Empirical Software Engineering**, Springer, v. 24, n. 4, p. 2636–2673, 2019. ISSN 1573-7616. Disponível em: https://doi.org/10.1007/s10664-019-09708-7. Acesso em: 09 ago. 2022.

BOVÉRIO, M. A.; SILVA, V. A. F. da. Blockchain: uma tecnologia além da criptomoeda virtual. **Revista Interface Tecnológica**, v. 15, n. 1, p. 109–121, 2018. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/326. Acesso em: 10 ago. 2022.

BRAGA, A.; MARINO, F.; SANTOS, R. dos. Segurança de aplicaçoes blockchain além das criptomoedas. In: XVII SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS — SBSEG 2017. Braísilia, DF **Simpósio** [...], 2017. p. 99–148. Disponível em: https://www.researchgate.net/publication/327894518_Seguranca_de_Aplicacoes_Blockchain_Alem_das_Criptomoedas. Acesso em: 10 ago. 2022.

BURGOS, A.; ALCHIERI, E. Um estudo sobre o uso de replicação máquina de estados paralelas na implementação de blockchains. In: XXII WORKSHOP DE TESTES E TOLERÂNCIA A FALHAS. Uberlândia, MG **Anais** [...], 2021. p. 57–70. Disponível em: https://sol.sbc.org.br/index.php/wtf/article/view/17204. Acesso em: 10 ago. 2022.

BURLE, L. M. **Um estudo de caso em cadeias de blocos**: principais mecanismos de consenso e a plataforma hyperledger fabric. 2019. Monografia (TCC) – Universidade Federal Fluminense, Niterói, RJ, 2019, Disponível em: https://app.uff.br/riuff/handle/1/12585. Acesso em: 10 ago. 2022.

BUTERIN, V. *et al.* A next-generation smart contract and decentralized application platform. **white paper**, v. 3, n. 37, 2014. Disponível em: https://nft2x.com/wp-content/uploads/2021/03/EthereumWP.pdf. Acesso em: 10 ago. 2022.

BUYSERE, K. D.; GAJDA, O.; KLEVERLAAN, R.; MAROM, D.; KLAES, M. **A framework for European crowdfunding**. [*S. n.*], 2012. Disponível em: https://www.fundraisingschool.it/wp-content/uploads/2013/02/European-Crowdfunding-Framework-Oct-2012.pdf. Acesso em: 10 ago. 2022.

CARDOSO, B. **Contratos inteligentes**: descubra o que são e como funcionam. 2018. Disponível em: https://brunonc.jusbrasil.com.br/artigos/569694569/contratos-inteligentes-descubra-o-que-sao-e-como-funcionam. Acesso em: 21 mar. 2022.

CARVALHO, C. A. de; ÁVILA, L. V. A tecnologia blockchain aplicada aos contratos inteligentes. **Revista Em Tempo**, v. 18, n. 01, p. 156–176, 2019. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3210. Acesso em: 10 ago. 2022.

CATARSE. **Quem Somos**. 2022. Disponível em: https://crowdfunding.catarse.me/quem-somos?ref=ctrse_footer/. Acesso em: 08 abr. 2022.

CHICARINO, V.; JESUS, E. F.; ALBUQUERQUE, C.; ROCHA, A. A. Uso de blockchain para privacidade e segurança em internet das coisas. In: VII SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS. Rio de Janeiro, RJ **Simpósio** [...]: SBC, 2017. v. 28. Disponível em: https://www.researchgate.net/publication/321966650_Uso_de_Blockchain_para_Privacidade_e_Seguranca_em_Internet_das_Coisas. Acesso em: 10 ago. 2022.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. **IEEE Access**, v. 4, p. 2292–2303, 2016. ISSN 2169-3536. Disponível em: https://ieeexplore.ieee.org/abstract/document/7467408. Acesso em: 10 ago. 2022.

COLLINS, L.; PIERRAKIS, Y. The venture crowd: crowdfunding equity investments into business. Nesta, 2012. Disponível em: https://eprints.kingston.ac.uk/id/eprint/29089/. Acesso em: 10 ago. 2022.

COMÉRCIO, J. do. **Investimento agora é colaborativo**. 2018. Disponível em: https://www.jornaldocomercio.com/_conteudo/cadernos/empresas_e_negocios/2018/08/644641-investimento-agora-e-colaborativo.html. Acesso em: 18 fev. 2021.

CONCEIÇÃO, V. M. R. Arlindo F. da; PAULA, R. F. de. Blockchain e aplicações em saúde. In: XIX - SIMPÓSIO BRASILEIRO DE COMPUTAÇÃO APLICADA À SAÚDE 2019. Niteroí, RJ **Simpósio** [...]: Sociedade Brasileira de Computação – SBC, 2019. p. 43–92.

ISBN 978-85-7669-472-4. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/29/94/244-1?inline=1. Acesso em: 10 ago. 2022.

CORREA, O. A. **Estudo da aplicaçao de estrutura blockchain com proof of stake para arquivamento de documentos com registro no tempo**. 2018. Monografia (TCC) – Universidade Federal de Santa Catarina, Florianópolis, SC, 2018, Disponível em: https://repositorio.ufsc.br/handle/123456789/187862. Acesso em: 10 ago. 2022.

COSH, A.; CUMMING, D.; HUGHES, A. Outside enterpreneurial capital. **The Economic Journal**, Oxford University Press Oxford, UK, v. 119, n. 540, p. 1494–1533, 2009. Disponível em: https://academic.oup.com/ej/article-abstract/119/540/1494/5089592?login=true. Acesso em: 10 ago. 2022.

COUTINHO, E.; BEZERRA, W.; MAIA, D. Um estudo preliminar das relações entre características de blockchain e a aplicação na sociedade. In: V WORKSHOP SOBRE ASPECTOS SOCIAIS, HUMANOS E ECONÔMICOS DE SOFTWARE. Porto Alegre, RS **Anais** [...]: SBC, 2020. p. 116–120. ISSN 2763-874X. Disponível em: https://sol.sbc.org.br/index.php/washes/article/view/11205. Acesso em: 10 ago. 2022.

COUTINHO, E.; BEZERRA, W.; MAIA, D. Uma análise inicial sobre a aplicação de blockchain na sociedade. In: II WORKSHOP SOBRE AS IMPLICAÇÕES DA COMPUTAÇÃO NA SOCIEDADE. Porto Alegre, RS **Anais** [...]: SBC, 2021. p. 45–56. ISSN 2763-8707. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/15963. Acesso em: 10 ago. 2022.

COUTINHO, E.; MAIA, D.; BEZERRA, W.; ABREU, A. Avaliando o custo de contratos inteligentes em aplicações blockchain por meio de ambientes de simulação. In: II WORKSHOP EM MODELAGEM E SIMULAÇÃO DE SISTEMAS INTENSIVOS EM SOFTWARE. Porto Alegre, RS **Anais** [...]: SBC, 2020. p. 56–65. ISSN 0000-0000. Disponível em: https://sol.sbc.org.br/index.php/mssis/article/view/12495. Acesso em: 10 ago. 2022.

COUTINHO, E. F.; FREITAS, H. P. de; SANTOS, I. B. dos; TEMOTEO, P. G. R. L.; MAIA, D. J. H.; BEZERRA, W. L. B. Aplicaçções e impactos da blockchain na sociedade. In: COLÓQUIO EM BLOCKCHAIN E WEB DESCENTRALIZADA. Niterói, RJ **Colóquio** [...], 2022. p. 85–92. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/20734. Acesso em: 10 ago. 2022.

CRETA, F.; TENCA, F. Tokenomics: A new opportunity in the real estate business? a qualitative approach to crowdfunding and blockchain interaction. **First Monday**, v. 26, n. 10, 2021. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/10699. Acesso em: 10 ago. 2022.

CUNHA, S. K. D.; BULGACOV, Y. L.; MEZA, M. L. F.; BALBINOT, Z. O sistema nacional de inovação e a ação empreendedora no brasil. **Base - Revista de Administração e Contabilidade da UNISINOS**, Universidade do Vale do Rio dos Sinos, v. 6, n. 2, p. 120–137, 2009. Disponível em: https://www.redalyc.org/pdf/3372/337228638004.pdf. Acesso em: 10 ago. 2022.

DETSCH, A. **Uma arquitetura para incorporação modular de aspectos de segurança em aplicações peer-to-peer.** 2005. Dissertação (Mestre em Computação Aplicada) – Universidade do Vale do Rio do Sinos, São Leopoldo, RS, 2005, Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/2213. Acesso em: 10 ago. 2022.

DRISCOLL, K.; HALL, B.; PAULITSCH, M.; ZUMSTEG, P.; SIVENCRONA, H. The real byzantine generals. In: IEEE. **The 23rd Digital Avionics Systems Conference (IEEE Cat. No. 04CH37576)**. 2004. v. 2, p. 6–D. Disponível em: https://ieeexplore.ieee.org/abstract/document/1390734. Acesso em: 10 ago. 2022.

EPSTEIN, R. A. The political economy of crowdsourcing: Markets for labor, rewards, and securities. **U. Chi. L. Rev. Dialogue**, HeinOnline, v. 82, p. 35, 2015. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/uchidial82&div=4&id=&page=. Acesso em: 10 ago. 2022.

EQSEED. **O que é equity crowdfunding?** 2022. Disponível em: https://eqseed.com/faq/52335-o-que-é-equity-crowdfunding. Acesso em: 13 abr. 2022.

FELINTO, E. Crowdfunding: entre as multidões e as corporações. **Comunicação Mídia e Consumo**, v. 9, n. 26, p. 137–150, 2013. Disponível em: https://revistacmc.espm.br/revistacmc/article/view/347. Acesso em: 10 ago. 2022.

FELIPE, I. Shared value creation and crowdfunding in brazil. **Journal of Financial Innovation (JoFI)**, v. 1, n. 3, p. 213–230, 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2956089. Acesso em: 10 ago. 2022.

FERREIRA, J. E.; PINTO, F. G. C.; SANTOS, S. C. dos. Estudo de mapeamento sistemático sobre as tendências e desafios do blockchain. **Gestão. org**, Universidade Federal de Pernambuco, v. 15, n. 6, p. 108–117, 2017. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7328726. Acesso em: 10 ago. 2022.

FIDELIS, M. A. **Um estudo sobre Non-Fungible Token (NFT)**. 2022. Monografia (TCC) – Pontifícia Universidade Católica de Goiás, Goiânia, GO, 2022, Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/4280. Acesso em: 10 ago. 2022.

FOROUZAN BEHROUZ A.; MOSHARRAF, F. **Redes de Computadores**: uma abordagem top-down. Porto Alegre, RS: AMGH, 2013. E–book. ISBN 9788580551693. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788580551693/. Acesso em: 10 ago. 2022.

GEBERT, M. Application of blockchain technology in crowdfunding. **New European**, v. 18, 2017. Disponível em: https://www.researchgate.net/profile/Michael-Gebert-2/publication/318307115_APPLICATION_OF_BLOCKCHAIN_TECHNOLOGY_IN_CROWDFUNDING/links/5961b927a6fdccc9b1298dac/APPLICATION-OF-BLOCKCHAIN-TECHNOLOGY-IN-CROWDFUNDING.pdf. Acesso em: 10 ago. 2022.

GREGÓRIO, E. N. de V.; LINS, F. A. A.; NÓBREGA, O. de O. Transparência de conectividade de serviços blockchain em sistemas iot: uma proposta de arquitetura. **Research, Society and Development**, v. 10, n. 12, p. e239101220273–e239101220273, 2021. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/20273. Acesso em: 10 ago. 2022.

GREVE, F.; SAMPAIO, L.; ABIJAUDE, J.; COUTINHO, A. A.; BRITO, I.; QUEIROZ, S. Blockchain e a revolução do consenso sob demanda. In: MINICURSOS DO SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS. Porto Alegre, RS **Simpósio** [...]: Sociedade Brasileira de Computação, 2018. Acesso em: 10 ago. 2022. Disponível em: http://143.54.25.88/index.php/sbrcminicursos/article/view/1770.

HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. In: MENEZES, A. J.; VANSTONE, S. A. (Ed.). **Advances in Cryptology-CRYPTO' 90**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991. p. 437–455. ISBN 978-3-540-38424-3. Disponível em: https://link.springer.com/chapter/10.1007/3-540-38424-3_32. Acesso em: 10 ago. 2022.

HOWE, J. **Poder Das Multidões, O**. Elsevier Brasil, 2009. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=HMZCHEMiemcC&oi=fnd&pg=PA1&dq=Poder+Das+Multid%C3%B5es,+O&ots=7SpXCa3C00&sig=XYMsa2m-5hgkoKxrlHm_scTnq44#v=onepage&q=Poder%20Das%20Multid%C3%B5es%2C%20O&f=false. Acesso em: 10 ago. 2022.

HU, M.; LI, X.; SHI, M. Product and pricing decisions in crowdfunding. **Marketing Science**, INFORMS, v. 34, n. 3, p. 331–345, 2015. Disponível em: https://pubsonline.informs.org/doi/abs/10.1287/mksc.2014.0900. Acesso em: 10 ago. 2022.

HYPERLEDGER. **Hyperledger.** 2020. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/blockchain.html. Acesso em: 21 mar. 2022.

INVESTIMENTO colaborativo vira opção a pequeno investidor. **ISTO É Dinheiro**, 2016. Disponível em: https://www.istoedinheiro.com.br/investimento-colaborativo-vira-opcao-a-pequeno-investidor/. Acesso em: 29 abr. 2021.

ISHMAEV, G. Blockchain technology as an institution of property. **Metaphilosophy**, v. 48, n. 5, p. 666–686, 2017. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/meta.12277. Acesso em: 10 ago. 2022.

JOSELLI, M. Blockchain e games. **SBGAMES**, v. 17, p. 1–11, 2018. Disponível em: http://sbgames.org/sbgames2018/files/papers/Tutoriais/188591.pdf. Acesso em: 10 ago. 2022.

KAMIENSKI, C.; SOUTO, E.; ROCHA, J.; DOMINGUES, M.; CALLADO, A.; SADOK, D. Colaboraçao na internet e a tecnologia peer-to-peer. In: XXV CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO–SBC2005. São Leopoldo, RS **Proceedings** [...], 2005. v. 25. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/6532817/arq0290-with-cover-page-v2.pdf?Expires=1663360232&Signature=Rpqeyb-gEngrqyWebXQy4B1oHdGs3axyMS-cos6SRSIQL4LXudjJ6Q4BafEjpc4Upw-~bY805aGzx7lm8Y_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 10 ago. 2022.

KHATTER, H.; CHAUHAN, H.; TRIVEDI, I.; AGARWAL, J. Secure and transparent crowdfunding using blockchain. In: 2021 INTERNATIONAL CONFERENCE ON RECENT TRENDS ON ELECTRONICS, INFORMATION, COMMUNICATION & TECHNOLOGY (RTEICT). Bangalore, India **Conference** [...]: IEEE, 2021. p. 76–80. Disponível em: https://ieeexplore.ieee.org/abstract/document/9573956. Acesso em: 10 ago. 2022.

KORPELA, K.; HALLIKAS, J.; DAHLBERG, T. Digital supply chain transformation toward blockchain integration. In: 50TH HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (HICSS). Honolulu, HI **Conference** [...]: ScholarSpace, 2017. Disponível em: https://scholarspace.manoa.hawaii.edu/handle/10125/41666. Acesso em: 10 ago. 2022.

LAWTON, K.; MAROM, D. **The crowdfunding revolution**: Social networking meets venture financing. Thecrowdfundingrevolution.com, 2010. Disponível em: https://vdoc.pub/documents/the-crowdfunding-revolution-social-networking-meets-venture-financing-76u3h12ns7l0. Acesso em: 10 ago. 2022.

LEE, W.; RAHIM, N. Decentralized application for charity organization crowdfunding using smart contract and blockchain. **Applied Information Technology And Computer Science**, v. 2, n. 2, p. 236–248, 2021. Disponível em: https://publisher.uthm.edu.my/periodicals/index.php/aitcs/article/view/2202. Acesso em: 10 ago. 2022.

LEWIS, A. **The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them**. Mango Media Inc., 2018. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=5pUREAAAQBAJ&oi=fnd&pg=PT11&dq=The+basics+of+bitcoins+and+blockchains:+an+introduction+to+cryptocurrencies+and+the+technology+that+powers+them&ots=FsJDs5NpaA&sig=h4w1zjk9nRB6fFt5WtdK4ewrxbM#v=onepage&q=The%20basics%20of%20bitcoins%20and%20blockchains%3A%20an%20introduction%20to%20cryptocurrencies%20and%20the%20technology%20that%20powers%20them&f=false. Acesso em: 10 ago. 2022.

LI, X.; JIANG, P.; CHEN, T.; LUO, X.; WEN, Q. A survey on the security of blockchain systems. **Future Generation Computer Systems**, Elsevier, v. 107, p. 841–853, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X17318332. Acesso em: 10 ago. 2022.

LIMA, F. Q. **Crowdfunding**: renovando o financiamento à inovação. 2013. Monografia (TCC) – Faculdade de Economia, Administração e Contabilidade, Brasília, DF, 2013, Disponível em: https://bdm.unb.br/handle/10483/6759. Acesso em: 10 ago. 2022.

LIMA, L. **A tecnologia blockchain aplicada à rastreabilidade de alimentos**. 2018. Disponível em: https://www.paripassu.com.br/blog/blockchain-rastreabilidade-de-alimentos/. Acesso em: 07 abr. 2022.

LUCAS, R. A. F.; ANDREA, C. M. **A regulamentação das criptomoedas como meio garantidor de segurança jurídica**. 2019. Disponível em: https://repositorio.uniube.br/handle/123456789/1294. Acesso em: 10 ago. 2022.

LUCENA, A. U. de; HENRIQUES, M. A. A. Estudo de arquiteturas dos blockchains de bitcoin e ethereum. In: IX ENCONTRO DE ALUNOS E DOCENTES DO DCA/FEEC/UNICAMP (EADCA). Campinas, SP **Encontro** [...], 2016. Disponível em: https://diegoazziufabc.files.wordpress.com/2017/08/estudo-de-arquiteturas-dos-blockchains.pdf. Acesso em: 10 ago. 2022.

LYRA, J. G. d. M.; MEIRINO, M. J. Bitcoin e blockchain: aplicações além da moeda virtual. 2017. In: XIII CONGRESSO NACIONAL DE EXCELÊNCIA EM GESTÃO IV INOVARSE 2017. Rio de Janeiro, RJ **Anais** [...], 2017. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/producaoIntelectual/viewProducaoIntelectual.xhtml;jsessionid=C-Lo7IdtAliphGdY9vlevBwV.sucupira-205?popup=true&id_producao=5341592. Acesso em: 10 ago. 2022.

MAIA, D. J. H.; COUTINHO, E. F. A blockchain solution for crowdfunding and cost analysis. In: 11TH EURO AMERICAN CONFERENCE ON TELEMATICS AND INFORMATION SYSTEMS. New York, NY, USA **Proceedings** [...]: Association for Computing Machinery, 2022. (EATIS '22). ISBN 9781450397384. Disponível em: https://doi.org/10.1145/3544538.3544650. Acesso em: 10 ago. 2022.

MARTINO, P.; BELLAVITIS, C.; DASILVA, C. M. Blockchain and initial coin offerings (icos): A new way of crowdfunding. **Available at SSRN 3414238**, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3414238. Acesso em: 10 ago. 2022.

MASCARENHAS, J. Z.; VIEIRA, A. B.; ZIVIANI, A. Análise da rede de transações do ethereum. In: I WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES. Campos do Jordão, SP **Anais** [...], 2018. Disponível em: https://sol.sbc.org.br/index.php/wblockchain/article/view/2352. Acesso em: 10 ago. 2022.

MATSUMINE, V. S. M. **Uma implementação do esquema de multi-assinaturas MuSig no cenário m-de-n com árvores de Merkle e suas aplicações ao bitcoin**. 2019. Monografia (TCC) – Universidade de Brasília, Brasília, DF, 2021, Disponível em: https://bdm.unb.br/handle/10483/28926. Acesso em: 10 ago. 2022.

MATTILA, J. The blockchain phenomenon. **Berkeley Roundtable of the International Economy**, p. 16, 2016. Disponível em: https://brie.berkeley.edu/sites/default/files/juri-mattila-.pdf. Acesso em: 10 ago. 2022.

MENDONÇA, R. D.; GOMES, O. S.; PEREIRA, P. C.; VIEIRA, A. B.; NACIF, J. A. Utilização de blockchain na rastreabilidade da cadeia produtiva do leite. In: III WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIA E APLICAÇÕES. Uberlândia, MG **Anais** [...], 2020. p. 55–60. Disponível em: https://sol.sbc.org.br/index.php/wblockchain/article/view/12433. Acesso em: 10 ago. 2022.

MENDONÇA, R. D.; GOMES, O. S.; VIEIRA, A. B.; NACIF, J. A. Tratamento de concessão e revogação de acesso a registros eletrônicos de saúde em blockchain. In: IV WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES. Uberlândia, MG **Anais** [...]: SBC, 2021. p. 100–113. Disponível em: https://sol.sbc.org.br/index.php/wblockchain/article/view/17133. Acesso em: 10 ago. 2022.

MGHAZLI, Y.-S. B.; MAIA, V. M.; CAVALCANTI, F. O. S. Mineração de dados: um investimento viável. In: VIII CONGRESSO NACIONAL DE ADMINISTRAÇÃO E CONTABILIDADE-ADCONT 2017. Rio de Janeiro, RJ **Congresso** [...], 2017. Disponível em: http://adcont.net/index.php/adcont/AdCont2017/paper/view/2456. Acesso em: 10 ago. 2022.

MOLLICK, E. The dynamics of crowdfunding: An exploratory study. **Journal of business venturing**, Elsevier, v. 29, n. 1, p. 1–16, 2014. Disponível em: https://www.sciencedirect.com/science/article/pii/S088390261300058X. Acesso em: 10 ago. 2022.

MOLLICK, E.; ROBB, A. Democratizing innovation and capital access: The role of crowdfunding. **California management review**, SAGE Publications Sage CA: Los Angeles, CA, v. 58, n. 2, p. 72–87, 2016. Disponível em: https://journals.sagepub.com/doi/abs/10.1525/cmr.2016.58.2.72. Acesso em: 10 ago. 2022.

MOLLICK, E. R.; KUPPUSWAMY, V. After the campaign: Outcomes of crowdfunding. **UNC Kenan-Flagler Research Paper**, n. 2376997, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376997. Acesso em: 10 ago. 2022.

MOREIRA, K. B. **Blockchain**: tecnologia, arquitetura e aplicações. 2019. Monografia (TCC) – Faculdade UnB Gama, Universidade de Brasília - UnB, Brasília, DF, 2019, Disponível em: https://bdm.unb.br/handle/10483/26357. Acesso em: 10 ago. 2022.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, v. 4, p. 21260, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 10 ago. 2022.

NAUMOVA, O.; SVETKINA, I.; NAUMOV, D. The main limitations of applying blockchain technology in the field of education. In: 2019 INTERNATIONAL SCIENCE AND TECHNOLOGY CONFERENCE "EASTCONF". Vladivostok, Russia **Conference** [...], 2019. p. 1–4. ISSN null. Disponível em: https://ieeexplore.ieee.org/abstract/document/8725411. Acesso em: 10 ago. 2022.

NOFER, M.; GOMBER, P.; HINZ, O.; SCHIERECK, D. Blockchain. **Business & Information Systems Engineering**, v. 59, n. 3, p. 183–187, Jun 2017. ISSN 1867-0202. Disponível em: https://doi.org/10.1007/s12599-017-0467-3. Acesso em: 08 ago. 2022.

NORDIN, N.; SUMB, R. M.; ZAINUDDINC, Z. Crowdfunding: Threat or opportunity? In: TOWARDS LIVABLE, RESILIENT COMPETITIVE CITIES INTERNATIONAL CONFERENCE 2018. Kuala Lumpur, Malaysia **Conference** [...]. Disponível em: https://www.researchgate.net/profile/Rabihah-Mdsum/publication/329962288_Crowdfunding_Threat_or_Opportunity/links/5c259ae092851c22a34a452a/Crowdfunding-Threat-or-Opportunity.pdf. Acesso em: 10 ago. 2022.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital [Revista online]**, v. 31, p. 11–15, 2012. Disponível em: http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf. Acesso em: 10 ago. 2022.

PEASTER, W. M. **Ethereum Gas Explained**. 2020. Disponível em: https://defiprime.com/gas. Acesso em: 09 ago. 2022.

PEREIRA, R. R. Estudo de caso sobre a tecnologia blockchain, projeto ethereum e viabilidade de métodos de mineração. **Ciência da Computação-Tubarão**, 2018. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/8469. Acesso em: 10 ago. 2022.

PETRONI, B. C. A.; FRANCO, G. R. Smart contracts baseados em blockchain na cadeia de custódia digital: uma proposta de arquitetura. In: TENTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE AND CYBER LAW. São Paulo, SP **Conference** [...], 2018. p. 23–30. Disponível em: http://icofcs.org/2018/ICoFCS-2018-003.pdf. Acesso em: 10 ago. 2022.

PORTO, A. M.; JUNIOR, J. M. de L.; SILVA, G. B. Tecnologia blockchain e direito societário: aplicações práticas e desafios para a regulação. **Revista de Informação Legislativa**, Senado Federal, v. 56, n. 223, p. 11–30, 2019. Disponível em: https://www12.senado.leg.br/ril/edicoes/56/223/ril_v56_n223_p11. Acesso em: 10 ago. 2022.

POTENZA, G. P.; OLIVEIRA, A. E. D. d. Regulando a inovação: o crowdfunding e o empreendedorismo brasileiro. **Revista de Direito Empresarial**, v. 15, p. 69–107, 2016. Disponível em: https://edisciplinas.usp.br/pluginfile.php/1898797/mod_resource/content/1/REGULANDO%20A%20INOVAC%CC%A7A%CC%83O%20-%20O%20CROWDFUNDING%20E%20O%20EMPREENDEDORISMO%20BRASILEIRO.pdf. Acesso em: 10 ago. 2022.

PRIMECOIN, K. S. **Cryptocurrency with Prime Number Proof-of-Work**. 2013. Disponível em: https://academictorrents.com/details/d0f9accaec8ac9d538fdf9d675105ae1392ea32b. Acesso em: 10 ago. 2022.

QIN, R.; YUAN, Y.; WANG, F. Research on the selection strategies of blockchain mining pools. **IEEE Transactions on Computational Social Systems**, v. 5, n. 3, p. 748–757, 2018. ISSN 2329-924X. Disponível em: https://ieeexplore.ieee.org/abstract/document/8444975. Acesso em: 10 ago. 2022.

RIFI, N.; RACHKIDI, E.; AGOULMINE, N.; TAHER, N. C. Towards using blockchain technology for ehealth data access management. In: 2017 FOURTH INTERNATIONAL CONFERENCE ON ADVANCES IN BIOMEDICAL ENGINEERING (ICABME). New York, NY, USA **Conference** [...]: IEEE, 2017. p. 1–4. Disponível em: https://ieeexplore.ieee.org/abstract/document/8167555. Acesso em: 10 ago. 2022.

ROCHA, J.; DOMINGUES, M.; CALLADO, A.; SOUTO, E.; SILVESTRE, G.; KAMIENSKI, C.; SADOK, D. Peer-to-peer: Computaçao colaborativa na internet. In: MINICURSOS DO XXII SIMPOSIO BRASILEIRO DE REDES DE COMPUTADORES (SBRC 2004). Gramado, RS **Proceedings** [...], 2004. Disponível em: https://www.cin.ufpe.br/~cak/publications/sbrc2004_minicurso_p2p.pdf. Acesso em: 10 ago. 2022.

ROLIM, C. O.; FREITAS, L. W. de. Demochain-framework destinado a criação de redes blockchain híbridas para dispositivos iot. In: II WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIA E APLICAÇÕES. Três de Maio, RS **Anais** [...]: SBC, 2019. Disponível em: https://sol.sbc.org.br/index.php/eradrs/article/view/7034. Acesso em: 10 ago. 2022.

ROMAGNOLO, C. A. **O que é Criptografia?** 2017. Disponível em: https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia. Acesso em: 23 fev. 2022.

ROUHANI, S.; DETERS, R. Performance analysis of ethereum transactions in private blockchain. In: 2017 8TH IEEE INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING AND SERVICE SCIENCE (ICSESS). Beijing, China **Conference** [...]: IEEE, 2017. p. 70–74. Disponível em: https://ieeexplore.ieee.org/abstract/document/8342866. Acesso em: 10 ago. 2022.

RUBINSTEINN, G. **Projeto social em blockchain distribui R$ 2 mi em criptomoedas no Brasil**. 2021. Disponível em: https://exame.com/dinheiro-tendencias/projeto-social-em-blockchain-distribui-r-2-mi-em-criptomoedas-no-brasil/. Acesso em: 07 abr. 2022.

SBEGHEN, B. M. **A multidão do crowdfunding na economia do virtual**: um estudo do site catarse. 2012. Monografia (TCC) – Faculdade de Biblioteconomia e Comunicação - Universidade Federal do Rio Grande do Sul, Porto Alegre, RS, 2012, Disponível em: https://www.lume.ufrgs.br/handle/10183/54321. Acesso em: 10 ago. 2022.

SERPRO. **Serpro desenvolve rede BlockChain para a Receita Federal**. 2019. Disponível em: https://www.serpro.gov.br/menu/imprensa/Releases/serpro-desenvolve-rede-blockchain-para-a-receita-federal. Acesso em: 3 ago. 2020.

SHARPLES, M.; DOMINGUE, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In: VERBERT, K.; SHARPLES, M.; KLOBUČAR, T. (Ed.). **Adaptive and Adaptable Learning**. Cham: Springer

International Publishing, 2016. p. 490–496. ISBN 978-3-319-45153-4. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-45153-4_48. Acesso em: 10 ago. 2022.

SHINGH, S.; KAMALVANSHI, V.; GHIMIRE, S.; BASYAL, S. Dairy supply chain system based on blockchain technology. **Asian J. Econ. Bus. Account**, v. 14, p. 13–19, 2020. Disponível em: https://www.researchgate.net/profile/Shuvam-Shingh/publication/339658540_Dairy_Supply_Chain_System_Based_on_Blockchain_Technology/links/5e5e5efaa6fdccbeba14d6d3/Dairy-Supply-Chain-System-Based-on-Blockchain-Technology.pdf. Acesso em: 10 ago. 2022.

SILVA, M. P. A segurança da democracia e a blockchain (securing democracy through blockchain). **Revista Projeção, Direito e Sociedade**, v. 9, n. 1, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3321706. Acesso em: 10 ago. 2022.

SOUSA, T. M. P. d. **Votechain, uma solução mais segura, acessível e inovadora para as eleições, implementada com a tecnologia Blockchain**. 2019. Monografia (TCC) – Universidade Federal do Rio Grande do Norte, Natal, RN 2019, Disponível em: https://repositorio.ufrn.br/handle/123456789/43646. Acesso em: 10 ago. 2022.

STEFFEN, C. Economia criativa, design e crowdfunding: uma exploração das plataformas brasileiras de financiamento coletivo. In: XII CONGRESSO LATINOAMERICANO DE INVESTIGADORES DE LA COMUNICACIÓN. Lima, Perú **Proceedings** [...], 2014. Disponível em: https://congreso.pucp.edu.pe/alaic2014/wp-content/uploads/2013/09/GT10-C\%C3\%A9sar-Steffen.pdf. Acesso em: 10 ago. 2022.

STEFFEN, C. Meios digitais participativos e economia criativa: uma exploração das plataformas brasileiras de crowdfunding. **Intexto**, n. 32, p. 156–171, 2015. Disponível em: https://www.seer.ufrgs.br/intexto/article/view/47816. Acesso em: 10 ago. 2022.

SZABO, N. **Smart Contracts**. 1994. Disponível em: http://bit.ly/2Yc9vjb. Acesso em: 21 mar. 2022.

ULLAH, N. **Crowdfunding, Crypto-Currency, Blockchain, Financial Dealings**: Review of business planning, challenges and issues. 2021. Disponível em: https://mpra.ub.uni-muenchen.de/108666/. Acesso em: 10 ago. 2022.

ULRICH, F. **Bitcoin:** a moeda na era digital. São Paulo: Instituto Mises Brasil, 2014. Disponível em: https://produtos.infomoney.com.br/hubfs/ebook-bitcoin.pdf. Acesso em: 10 ago. 2022.

USINA GRANELLI. **Tecnologia Blockchain para a rastreabilidade da cadeia produtiva sucroalcooleira**. 2022. Disponível em: https://usinagranelli.com.br/tecnologia-blockchain-para-a-rastreabilidade-da-cadeia-produtiva-sucroalcooleira/. Acesso em: 07 abr. 2022.

VEUGER, J. Trust in a viable real estate economy with disruption and blockchain. **Facilities**, Emerald Publishing Limited, 2018. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/F-11-2017-0106/full/html?fullSc=1&mbSc=1. Acesso em: 10 ago. 2022.

VIANA, C.; BRANDAO, A.; DIAS, D.; CASTELLANO, G.; GUIMARAES, M. de P. Blockchain para gerenciamento de prontuários eletrônicos. **Revista ibérica de sistemas e tecnologias de informação**, Associação Ibérica de Sistemas e Tecnologias de Informacao, n. E28, p. 177–187, 2020. Disponível em: https://www.researchgate.net/profile/Diego-Roberto-Dias/publication/339795838_Blockchain_para_gerenciamento_de_prontuarios_eletronicos/links/

5e6645e792851c7ce0537a3b/Blockchain-para-gerenciamento-de-prontuarios-eletronicos.pdf. Acesso em: 10 ago. 2022.

WANG, W.; HOANG, D. T.; HU, P.; XIONG, Z.; NIYATO, D.; WANG, P.; WEN, Y.; KIM, D. I. A survey on consensus mechanisms and mining strategy management in blockchain networks. **IEEE Access**, v. 7, p. 22328–22370, 2019. ISSN 2169-3536. Disponível em: https://ieeexplore.ieee.org/abstract/document/8629877. Acesso em: 10 ago. 2022.

WANG, X.; FENG, Q.; CHAI, J. The research of consortium blockchain dynamic consensus based on data transaction evaluation. In: 2018 11TH INTERNATIONAL SYMPOSIUM ON COMPUTATIONAL INTELLIGENCE AND DESIGN (ISCID). Hangzhou, China **Proceedings** [...]: IEEE, 2018. v. 2, p. 214–217. Disponível em: https://ieeexplore.ieee.org/abstract/document/8695561. Acesso em: 10 ago. 2022.

WILL, A.; BRÜNTJE, D.; GOSSEL, B. Entrepreneurial venturing and media management. In: **Managing media firms and industries**. Springer, 2016. p. 189–206. Acesso em: 10 ago. 2022. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-08515-9_11.

WOOD, G. **Ethereum**: A secure decentralised generalised transaction ledger. 2019. Disponível em: https://gavwood.com/paper.pdf. Acesso em: 09 ago. 2022.

WOOD, G. *et al.* Ethereum: A secure decentralised generalised transaction ledger. **Ethereum project yellow paper**, v. 151, n. 2014, p. 1–32, 2014. Disponível em: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf. Acesso em: 10 ago. 2022.

XIAO, Y.; ZHANG, N.; LOU, W.; HOU, Y. T. A survey of distributed consensus protocols for blockchain networks. **IEEE Communications Surveys Tutorials**, v. 22, n. 2, p. 1432–1465, Secondquarter 2020. ISSN 1553-877X. Disponível em: https://ieeexplore.ieee.org/abstract/document/8972381. Acesso em: 10 ago. 2022.

XIE, J.; TANG, H.; HUANG, T.; YU, F. R.; XIE, R.; LIU, J.; LIU, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. **IEEE Communications Surveys & Tutorials**, IEEE, v. 21, n. 3, p. 2794–2830, 2019. Disponível em: https://ieeexplore.ieee.org/abstract/document/8642861. Acesso em: 10 ago. 2022.

XU, X.; WEBER, I.; STAPLES, M. Blockchain in software architecture. 2019. In: Springer Cham. 2019. p. 83—-92. Disponível em: https://doi.org/10.1007/978-3-030-03035-3_5. Acesso em: 10 ago. 2022.

XU, X.; WEBER, I.; STAPLES, M.; ZHU, L.; BOSCH, J.; BASS, L.; PAUTASSO, C.; RIMBA, P. A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE INTERNATIONAL CONFERENCE ON SOFTWARE ARCHITECTURE (ICSA). New York, NY, USA **Conference** [...]: IEEE, 2017. p. 243–252. Disponível em: https://ieeexplore.ieee.org/abstract/document/7930224. Acesso em: 10 ago. 2022.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, X.; WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE INTERNATIONAL CONGRESS ON BIG DATA (BIGDATA CONGRESS). Honolulu, HI, USA **Proceedings** [...]: IEEE, 2017. p. 557–564. Disponível em: https://ieeexplore.ieee.org/abstract/document/8029379. Acesso em: 10 ago. 2022.

ZHENG, Z.; XIE, S.; DAI, H.-N.; CHEN, X.; WANG, H. Blockchain challenges and opportunities: A survey. **International Journal of Web and Grid Services**, Inderscience Publishers (IEL), v. 14, n. 4, p. 352–375, 2018. Disponível em: https://allquantor.at/blockchainbib/pdf/zheng2018blockchain.pdf. Acesso em: 10 ago. 2022.

ZHU, H.; ZHOU, Z. Z. Analysis and outlook of applications of blockchain technology to equity crowdfunding in china. **Financial innovation**, Springer, v. 2, n. 1, p. 1–11, 2016. Disponível em: https://link.springer.com/article/10.1186/s40854-016-0044-7. Acesso em: 10 ago. 2022.

APÊNDICE A – QUADROS COM DADOS DOS EXPERIMENTOS

Quadro 3 – Detalhes dos cenários com medidas de média, mediana, mínimo, máximo e alcance

cenários	medidas	média	mediana	mínimo	máximo	alcance
cenário 1.1	**tempo**	22,533	22,500	12,000	35,000	23,000
	gas	55049,5	55051	55006	55051	45
	taxa gas	1,26	1,20	1,00	1,50	0,50
	ether	0,0006930647	0,0006600612	0,0005500510	0,0008250765	0,0002750255
cenário 1.2	**tempo**	23,767	24,000	6,000	41,000	35,000
	gas	550051	550051	550051	550051	0
	taxa gas	1,50	1,50	1,50	1,50	0,00
	ether	0,0000000015	0,0000000015	0,0000000015	0,0000000015	0,0000000000
cenário 1.3	**tempo**	27,400	27,500	15,000	40,000	25,000
	gas	550051	550051	550051	550051	0
	taxa gas	1,07	1,07	1,07	1,07	0,00
	ether	0,0005862015	0,0005862015	0,0005862015	0,0005862015	0,0000000000
cenário 2.1	**tempo**	27,267	29,000	11,000	44,000	33,000
	gas	30809	30809	30809	30809	0
	taxa gas	1,00	1,00	1,00	1,00	0,00
	ether	0,0000308093	0,0000308093	0,0000308093	0,0000308093	0,0000000000
cenário 2.2	**tempo**	26,333	26,000	11,000	38,000	27,000
	gas	30809	30809	30809	30809	0
	taxa gas	1,50	1,50	1,50	1,50	0,00
	ether	0,0000462135	0,0000462135	0,0000462135	0,0000462135	0,0000000000
cenário 2.3	**tempo**	22,000	19,000	12,000	37,000	25,000
	gas	32042,33333	30809	30809	67809	37000
	taxa gas	2,50	2,50	2,50	2,50	0,00
	ether	0,0000801058	0,0000770225	0,0000770225	0,0001695225	0,0000925000
cenário 3.1	**tempo**	24,767	25,000	13,000	38,000	25,000
	gas	371275	371275	371275	371275	0
	taxa gas	1,29	1,29	1,29	1,29	0,00
	ether	0,0004789449	0,0004789449	0,0004789449	0,0004789449	0,0000000000
cenário 3.2	**tempo**	22,367	22,000	9,000	35,000	26,000
	gas	371845	371275	371275	388375	17100
	taxa gas	2,50	2,50	2,50	2,50	0,00
	ether	0,0009296125	0,0009281875	0,0009281875	0,0009709375	0,0000427500
cenário 3.3	**tempo**	28,467	28,500	19,000	41,000	22,000
	gas	371845	371275	371275	388375	17100
	taxa gas	2,50	2,50	2,50	2,50	0,00
	ether	0,0009296125	0,0009281875	0,0009281875	0,0009709375	0,0000427500
cenário 4.1	**tempo**	26,567	26,500	11,000	41,000	30,000
	gas	70516	70516	70516	70516	0
	taxa gas	1,20	1,20	1,20	1,20	0,00
	ether	0,0000846193	0,0000846193	0,0000846193	0,0000846193	0,0000000000
cenário 4.2	**tempo**	25,600	26,500	12,000	37,000	25,000
	gas	70516	70516	70516	70516	0
	taxa gas	1,20	1,20	1,20	1,20	0,00
	ether	0,0000846188	0,0000846193	0,0000846049	0,0000846193	0,0000000144
cenário 4.3	**tempo**	24,433	25,000	10,000	35,000	25,000
	gas	70516	70516	70516	70516	0
	taxa gas	2,50	2,50	2,50	2,50	0,00
	ether	0,0001762890	0,0001762900	0,0001762600	0,0001762900	0,0000000300
cenários	**medidas**	**média**	**mediana**	**mínimo**	**máximo**	**alcance**

Fonte: o autor.

Quadro 4 – Detalhes dos cenários com medidas de média, mediana, mínimo, máximo e alcance

cenários	**medidas**	**média**	**mediana**	**mínimo**	**máximo**	**alcance**
cenário 1	**tempo**	24,567	24,000	6,000	41,000	35,000
	gas	385050,5	550051	55006	550051	495045
	taxa gas	1,28	1,20	1,00	1,50	0,50
	ether	0,0004264226	0,0005862015	0,0000000015	0,0008250765	0,0008250750
cenário 2	**tempo**	25,200	25,000	11,000	44,000	33,000
	gas	31220,11111	30809	30809	67809	37000
	taxa gas	1,67	1,50	1,00	2,50	1,50
	ether	0,0000523762	0,0000462135	0,0000308093	0,0001695225	0,0001387132
cenário 3	**tempo**	25,200	25,000	9,000	41,000	32,000
	gas	371655	371275	371275	388375	17100
	taxa gas	2,10	2,50	1,29	2,50	1,21
	ether	0,0007793900	0,0009281875	0,0004789449	0,0009709375	0,0004919926
cenário 4	**tempo**	25,533	25,500	10,000	41,000	31,000
	gas	70516	70516	70516	70516	0
	taxa gas	1,63	1,20	1,20	2,50	1,30
	ether	0,0001151757	0,0000846193	0,0000846049	0,0001762900	0,0000916851
Total	**tempo**	25,125	25,000	6,000	44,000	38,000
	gas	214610,4028	70516	30809	550051	519242
	taxa gas	1,67	1,50	1,00	2,50	1,50
	ether	0,0003433411	0,0001728913	0,0000000015	0,0009709375	0,0009709360
cenários	**medidas**	**média**	**mediana**	**mínimo**	**máximo**	**alcance**

Fonte: o autor.

Quadro 5 – Detalhes dos cenários com medidas de variância, desvio padrão, 1o. quartil, 2o. quartil e 3o. quartil

cenários	medidas	variância	desvio padrão	1o. quartil	2o. quartil	3o. quartil
cenário 1.1	**tempo**	23,361	4,833	20,250	22,500	24,000
	gas	67,5	8,215838363	55051	55051	55051
	taxa gas	0,02	0,15	1,20	1,20	1,45
	ether	0,0000000076	0,0000873894	0,0006600612	0,0006600612	0,0007838263
cenário 1.2	**tempo**	68,047	8,249	19,000	24,000	27,000
	gas	0	0	550051	550051	550051
	taxa gas	0,00	0,00	1,50	1,50	1,50
	ether	0,0000000000	0,0000000000	0,0000000015	0,0000000015	0,0000000015
cenário 1.3	**tempo**	46,110	6,790	24,000	27,500	31,000
	gas	0	0	550051	550051	550051
	taxa gas	0,00	0,00	1,06	1,06	1,06
	ether	0,0000000000	0,0000000000	0,0005862015	0,0005862015	0,0005862015
cenário 2.1	**tempo**	71,720	8,469	20,750	29,000	32,000
	gas	0	0	30809	30809	30809
	taxa gas	0,00	0,00	1,00	1,00	1,00
	ether	0,0000000000	0,0000000000	0,0000308093	0,0000308093	0,0000308093
cenário 2.2	**tempo**	34,506	5,874	24,000	26,000	30,000
	gas	0	0	30809	30809	30809
	taxa gas	0,00	0,00	1,50	1,50	1,50
	ether	0,0000000000	0,0000000000	0,0000462135	0,0000462135	0,0000462135
cenário 2.3	**tempo**	60,000	7,746	17,250	19,000	28,750
	gas	45633333,33	6755,244876	30809	30809	30809
	taxa gas	0,00	0,00	2,50	2,50	2,50
	ether	0,0000000003	0,0000168881	0,0000770225	0,0000770225	0,0000770225
cenário 3.1	**tempo**	41,220	6,420	19,500	25,000	28,000
	gas	0	0	371275	371275	371275
	taxa gas	0,00	0,00	1,29	1,29	1,29
	ether	0,0000000000	0,0000000000	0,0004789449	0,0004789449	0,0004789449
cenário 3.2	**tempo**	49,826	7,059	18,000	22,000	26,000
	gas	9747000	3122,018578	371275	371275	371275
	taxa gas	0,00	0,00	2,50	2,50	2,50
	ether	0,0000000001	0,0000078050	0,0009281875	0,0009281875	0,0009281875
cenário 3.3	**tempo**	43,775	6,616	22,250	28,500	33,750
	gas	9747000	3122,018578	371275	371275	371275
	taxa gas	0,00	0,00	2,50	2,50	2,50
	ether	0,0000000001	0,0000078050	0,0009281875	0,0009281875	0,0009281875
cenário 4.1	**tempo**	56,323	7,505	23,250	26,500	32,000
	gas	0	0	70516	70516	70516
	taxa gas	0,00	0,00	1,20	1,20	1,20
	ether	0,0000000000	0,0000000000	0,0000846193	0,0000846193	0,0000846193
cenário 4.2	**tempo**	46,938	6,851	24,000	26,500	30,000
	gas	0	0	70516	70516	70516
	taxa gas	0,00	0,00	1,20	1,20	1,20
	ether	0,0000000000	0,0000000026	0,0000846193	0,0000846193	0,0000846193
cenário 4.3	**tempo**	42,737	6,537	19,000	25,000	30,750
	gas	0	0	70516	70516	70516
	taxa gas	0,00	0,00	2,50	2,50	2,50
	ether	0,0000000000	0,0000000055	0,0001762900	0,0001762900	0,0001762900

Fonte: o autor.

Quadro 6 – Detalhes dos cenários com medidas de variância, desvio padrão, 1o. quartil, 2o. quartil e 3o. quartil

cenários	**medidas**	**variância**	**desvio padrão**	**1o. quartil**	**2o. quartil**	**3o. quartil**
cenário 1	**tempo**	49,125	7,009	20,250	24,000	28,000
	gas	55062131483	234653,2154	55051	550051	550051
	taxa gas	0,04	0,20	1,06	1,20	1,50
	ether	0,0000000964	0,0003104064	0,0000000015	0,0005862015	0,0006600612
cenário 2	**tempo**	59,488	7,713	19,000	25,000	31,750
	gas	15211111,11	3900,142448	30809	30809	30809
	taxa gas	0,39	0,62	1,00	1,50	2,50
	ether	0,0000000005	0,0000228410	0,0000308093	0,0000462135	0,0000770225
cenário 3	**tempo**	50,297	7,092	20,000	25,000	29,750
	gas	6424988,764	2534,756155	371275	371275	371275
	taxa gas	0,32	0,57	1,29	2,50	2,50
	ether	0,0000000457	0,0002137298	0,0004789449	0,0009281875	0,0009281875
cenário 4	**tempo**	48,342	6,953	20,000	25,500	31,000
	gas	0	0	70516	70516	70516
	taxa gas	0,37	0,61	1,20	1,20	2,50
	ether	0,0000000019	0,0000434557	0,0000846193	0,0000846193	0,0001762900
Total	**tempo**	51,502	7,177	20,000	25,000	30,000
	gas	40758155591	201886,4918	55039,75	70516	371275
	taxa gas	0,36	0,60	1,20	1,5 0	2,50
	ether	0,0000001195	0,0003456611	0,0000693203	0,0001728913	0,0005862015
cenários	**medidas**	**variância**	**desvio padrão**	**1o. quartil**	**2o. quartil**	**3o. quartil**

Fonte: o autor.